System Administration

ZENworks® Mobile Management 2.5.x

July 2012

Novell®

Legal Notices

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

Table of Contents

Accessing the Dashboard

Requirements

ZENworks Mobile Management dashboard requirements:

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

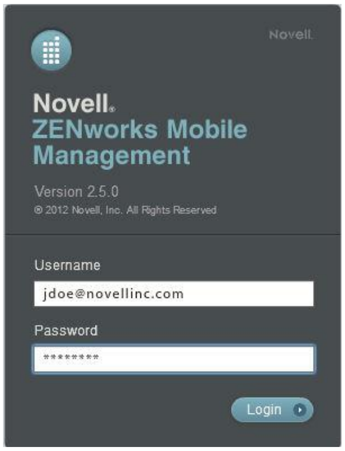
In your Web browser, enter the server address of the *ZENworks Mobile Management* server, followed by ***/dashboard***

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

Login

Log in to the *ZENworks Mobile Management* dashboard by using the email address and password you designated as administrative login credentials when installing the *ZENworks Mobile Management Web/Http Server Component*.

You 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.


Novell.
Novell.
ZENworks Mobile Management
Version 2.5.0
© 2012 Novell, Inc. All Rights Reserved
Username
Password
Login

Username: jdoe@novellinc.com

Password: ********

Organization Administration

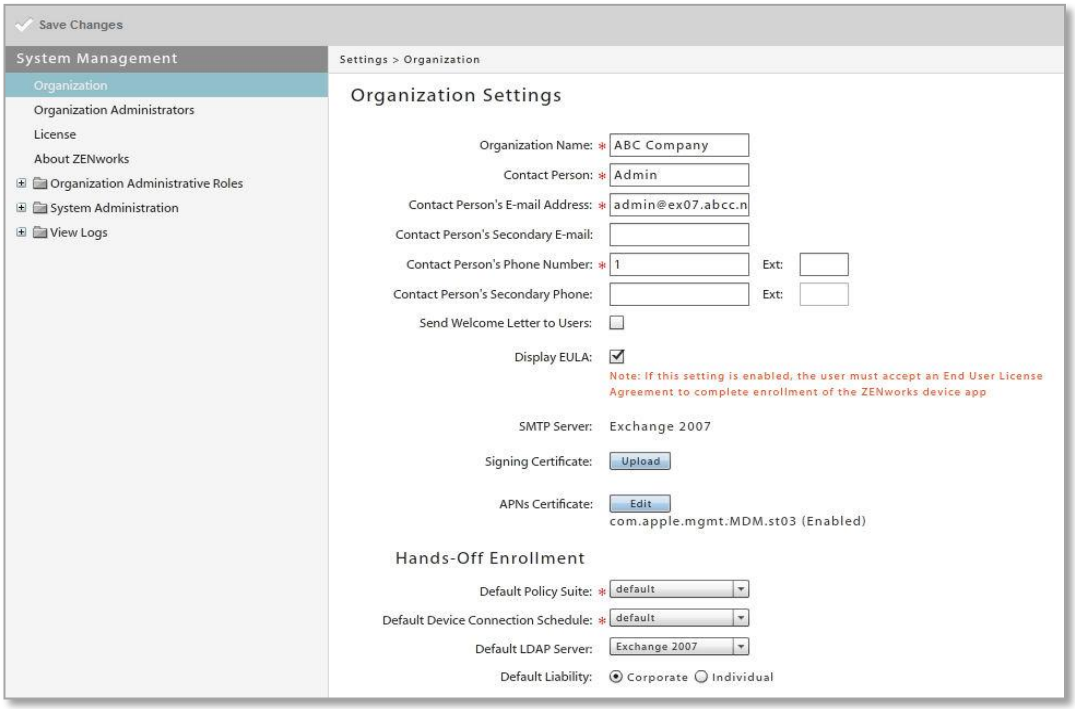
This section of the guide documents topics related to managing a single organization. See Managing Multiple Organizations for information regarding management of a *ZENworks Mobile Management* server with multiple organizations.

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
- EULA enablement - when this option is enabled, users must accept an End User License Agreement to complete *ZENworks Mobile Management* app enrollment
- SMTP server name
- Signing Certificate *Upload* button (see description below)
- APNs Certificate *Upload* button (see description below)
- Hands-Off enrollment configuration
    - Default Policy Suite
    - Default Device Connection Schedule
    - Default (Administrative) LDAP Server
    - Default Liability



Organization Settings

Organization Name: * ABC Company
Contact Person: * Admin
Contact Person's E-mail Address: * admin@ex07.abcc.n
Contact Person's Secondary E-mail:
Contact Person's Phone Number: * 1 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
SMTP Server: Exchange 2007
Signing Certificate:
APNs Certificate:
com.apple.mgmt.MDM.st03 (Enabled)

Hands-Off Enrollment

Default Policy Suite: * default
Default Device Connection Schedule: * default
Default LDAP Server: Exchange 2007
Default Liability: ● Corporate ○ Individual

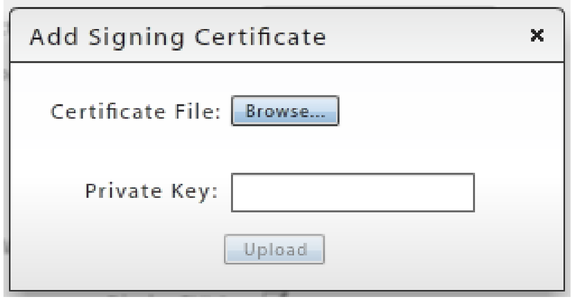
Signing Certificate Upload

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.



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

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:

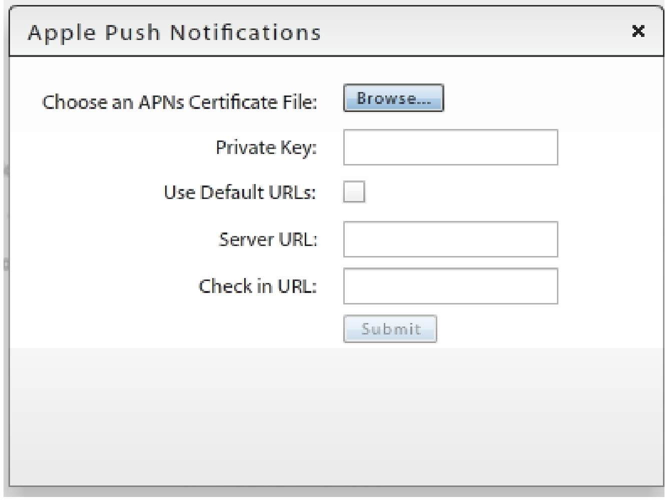
- Devices support Selective Wipe, Lock Device, and Clear Passcode
- Full Wipe and Lock Device commands are applied immediately
- You can record and access installed applications on devices
- You can record and access installed configuration profiles on devices
- You have access to additional device statistics
- 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

1. Select ***System*** > ***Organization***.

2. Click the *Upload* button next to the **APNs Certificate** field.

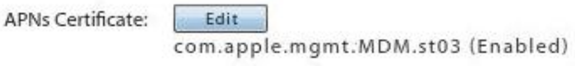


3. Click the ***Browse*** button, then navigate to and select the .pfx file containing the APNs certificate.
4. In the ***Private Key*** field, enter the password you set when exporting the certificate.
5. Select the **Use Default URLs** box to populate the *Server URL* and *Check in URL* fields with **Error! Hyperlink reference not valid.**. 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.

6. Click the ***Submit*** button.

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



APNs Certificate: com.apple.mgmt.MDM.st03 (Enabled)

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

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	• Can add or remove users and perform all the functions in the right-hand *Details* panel, except *Show Recovery Password* • Can email an individual user, but cannot use *Group Emailing* • Can perform most functions in the left-hand panel of *User Profile* • Can view the grids in the *Audit Data* and *Search Text Message Log* options (*User Profile*), but cannot view the body or attachments of a text message • Can choose the Visible Columns	• Restricted from adding or removing users and from all functions in the right *Details* panel • Restricted from sending an email to an individual user or a group • Restricted from the *Location Data, Audit Data, Search Phone Log, Search Text Message Log*, and *File Archive* options in the left panel of *User Profile* • Read-only access to options in the left panel of *User Profile* • Can choose the Visible Columns for the *Users* list

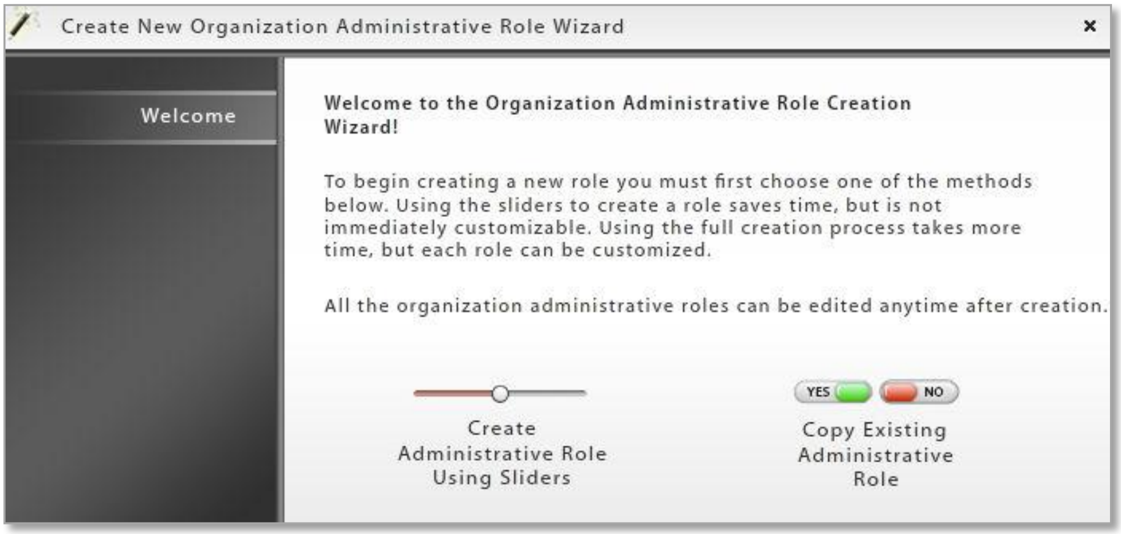
	for the *Users* list	
Organization	Read-only access	Read-only access
Reporting	Full access (view and export)	Full access (view and export)
System	• Read-only access • Restricted from the *System Administration* option in the left panel	• Read-only access • Restricted from the *System Administration* option in the left panel

Customized Organization Administrator Roles

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

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

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



Welcome to the Organization Administrative Role Creation Wizard!

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

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

YES
NO
Create Administrative Role Using Sliders
Copy Existing Administrative Role

1. Choose a method for creating an Organization Administrative Role:
    - Use the sliders to determine the role's initial settings. The new role copies the settings of the predefined Organization *Full Admin*, *Support Admin,* or *Restricted Admin*.
    - Copy the settings of an existing role
2. Specify the role permissions to copy.
3. Enter a **Role Name** and **Description**.
4. Click **Finish** to save the new role.
5. Find and select the role in the *Organization Administrative Roles* grid.

6. Set the general permissions for the role:
    - **Prevent role from managing administrator accounts, roles and user privacy protections**
        - Locks the role out of modifying administrator accounts, administrator roles, and user privacy protection.
        - Most roles should be locked, except those for administrators requiring full privileges.
        - If set to YES, this permission overrules the *System Section Permissions,* regardless of how they are set.
        - Defaults to YES when creating a role with the sliders. If you are copying an existing role, the setting of the copied role is the default.
    - **Prevent role from viewing protected data as defined in User Privacy Protection**
        - Blocks administrators assigned this role from viewing the protected data of only the users or policy suites designated in User Privacy Protection. (Automatically places the role in the *Restricted* column of the ***Restrict Organization Administrative Roles*** list. See User Privacy Protection.)
        - Defaults to YES when creating a role with the sliders. If you are copying an existing role, the setting of the copied role is the default.
7. Set the permissions associated with dashboard access. See Appendix A: Role Permissions for a comprehensive list.

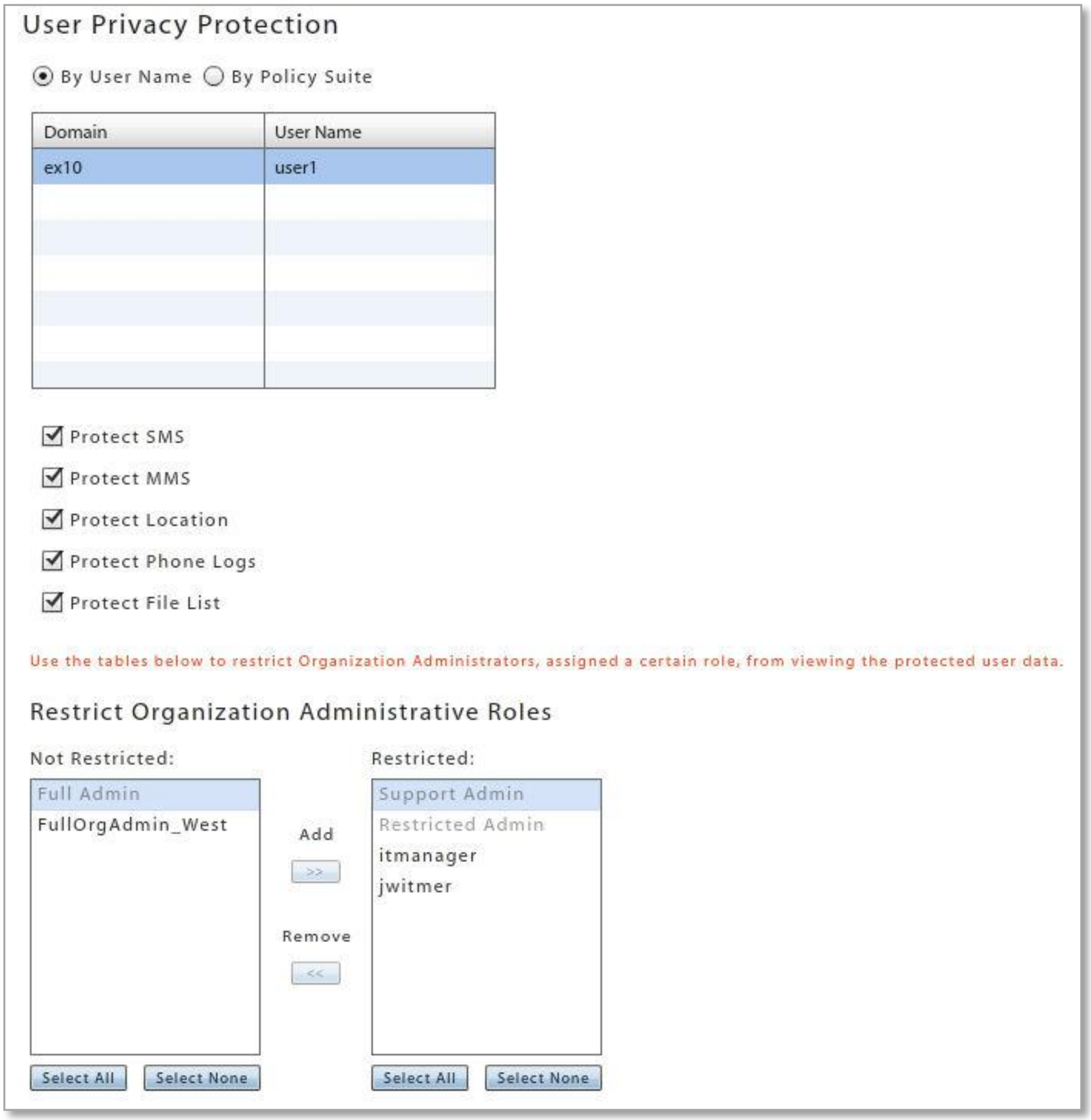
Organization Administrative Roles: User Privacy Protection

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.

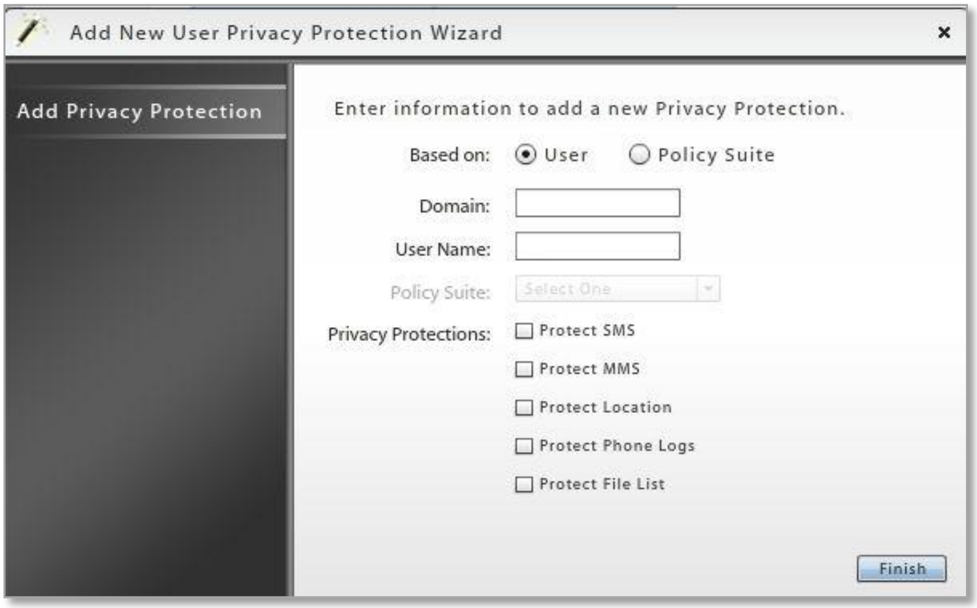
Restrict Organization Administrative Roles

Not Restricted:	Restricted:
Full Admin	Support Admin
FullOrgAdmin_West	Restricted Admin
	itmanager
	jwitmer

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

Adding Users to the Privacy Protection List

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



Add New User Privacy Protection Wizard

Enter information to add a new Privacy Protection.

Based on: ● User ○ Policy Suite

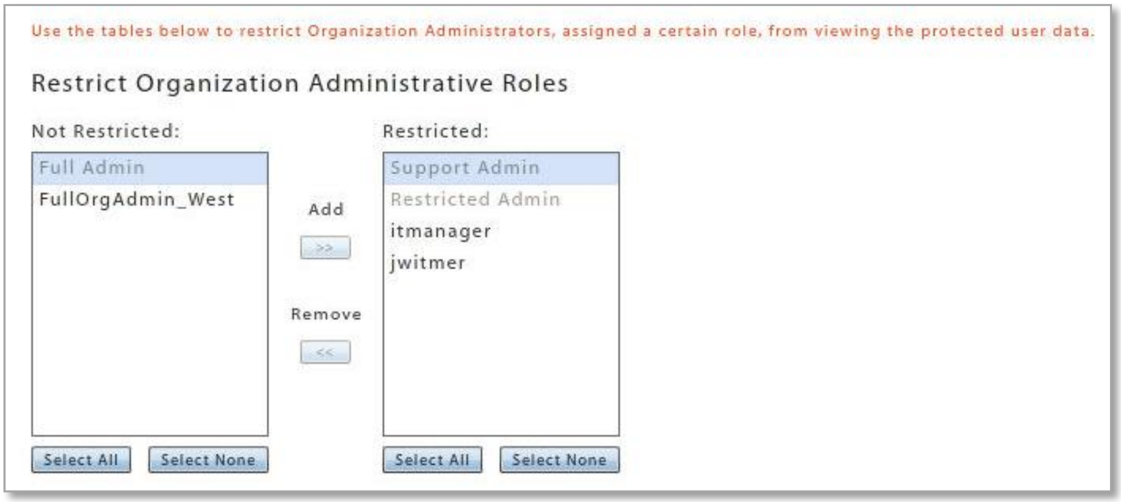
Privacy Protections: ☐ Protect SMS ☐ Protect MMS ☐ Protect Location ☐ Protect Phone Logs ☐ Protect File List

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

Adding Administrator Roles to the Restricted/Not Restricted List

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

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



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

Restrict Organization Administrative Roles

Not Restricted:

Full Admin
FullOrgAdmin_West

Restricted:

Support Admin
Restricted Admin
itmanager
jwitmer

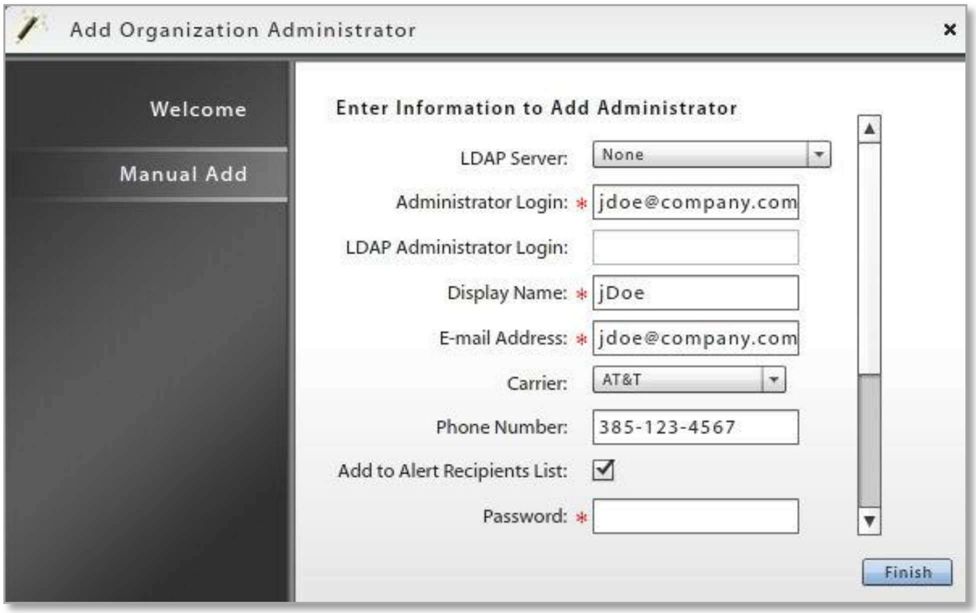
1. Select an administrative role on either side of the list. (Hold the SHIFT or CTRL key to select multiple items; hold the CTRL key to unselect an item).
2. Click **Add** to move a role from *Not Restricted* to *Restricted*.
3. Click **Remove** to move a role from *Restricted* to *Not Restricted*.
4.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

Organization Administrator Logins

See also, System Administrator Logins

Creating Organization Administrator Logins

Select ***System*** > ***Organization Administrators*** > ***Add Administrator***.



Enter Information to Add Administrator

LDAP Server: None
Administrator Login: * jdoe@company.com
LDAP Administrator Login:
Display Name: * jDoe
E-mail Address: * jdoe@company.com
Carrier: AT&T
Phone Number: 385-123-4567
Add to Alert Recipients List: ☑
Password: *

The Add Administrator Wizard steps you through creating login credentials for organization administrators.

The Wizard asks for the following information:

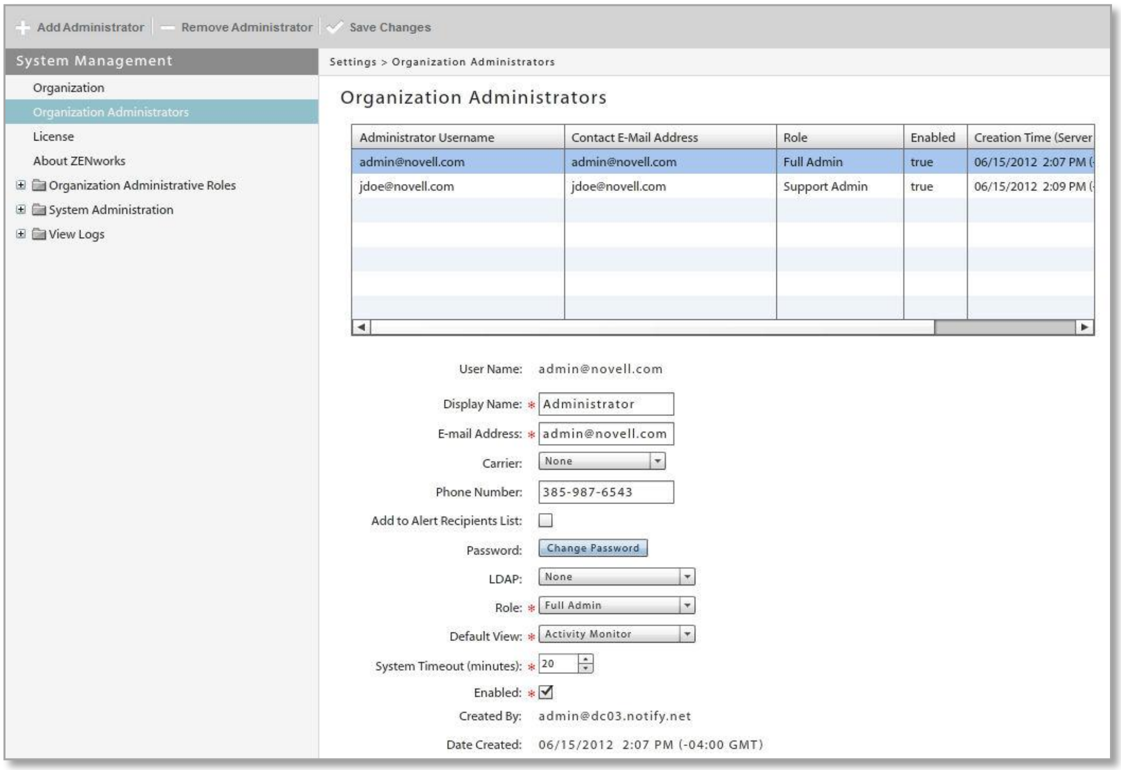
- **LDAP Server** – the server with which this user is associated (optional) if you are creating LDAP authentication logins. (*Administrator Login* and *Password* fields will be disabled if you choose this option.)
- **Administrator Login** – Enter the administrator's email address to be used as a username (if not using LDAP authentication).
- **LDAP Administrator Login** – Enter the administrator's LDAP server user name if using LDAP authentication.
- **Display Name** – Enter the name that will display for this login.
- **Email address** – Enter the contact email address of the user.
- **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).
- **Add to Alert Recipient List** – Check this box to make this administrator a recipient of Compliance Management email or SMS alerts.
- **Password** – Assign a password if you are creating a login that does not use LDAP authentication.
- **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
- ***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.

1. Select ***System*** > ***Organization Administrators***.
2. Select an administrator from the list. Edit the settings and click ***Save Changes***. You can also remove the administrator by clicking ***Remove Administrator***.



Administrator Username	Contact E-Mail Address	Role	Enabled	Creation Time (Server
admin@novell.com	admin@novell.com	Full Admin	true	06/15/2012 2:07 PM
jdoe@novell.com	jdoe@novell.com	Support Admin	true	06/15/2012 2:09 PM

User Name: admin@novell.com
Display Name: * Administrator
E-mail Address: * admin@novell.com
Carrier: None
Phone Number: 385-987-6543
Add to Alert Recipients List: ☐
Password: Change Password
LDAP: None
Role: * Full Admin
Default View: * Activity Monitor
System Timeout (minutes): * 20
Enabled: * ☑
Created By: admin@dc03.notify.net
Date Created: 06/15/2012 2:07 PM (-04:00 GMT)

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.
- **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 **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***, or ***iOS MDM Sync Log***.

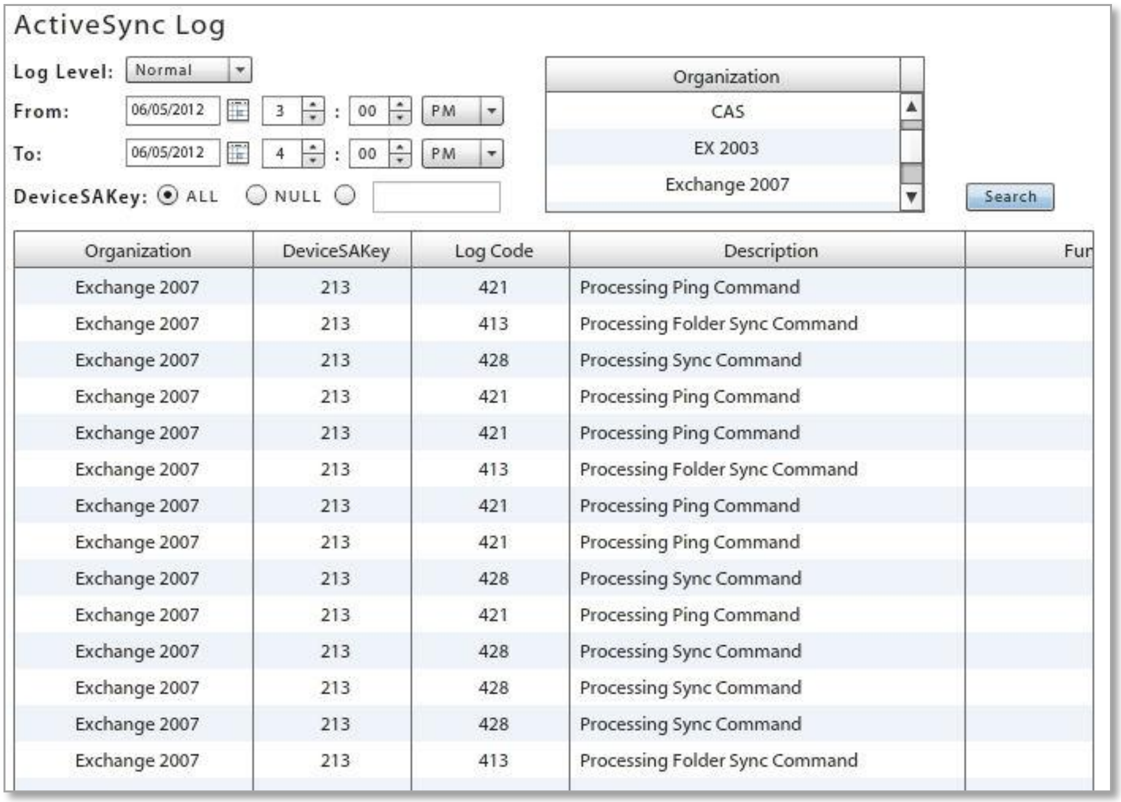
The **Log Level** defaults to **Normal** and the log populates the grid with system-wide data from the past hour. If you change the log level to **Verbose,** click **Search**.

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.



Log Level: Normal

From: 06/05/2012 3 : 00 PM

To: 06/05/2012 4 : 00 PM

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:

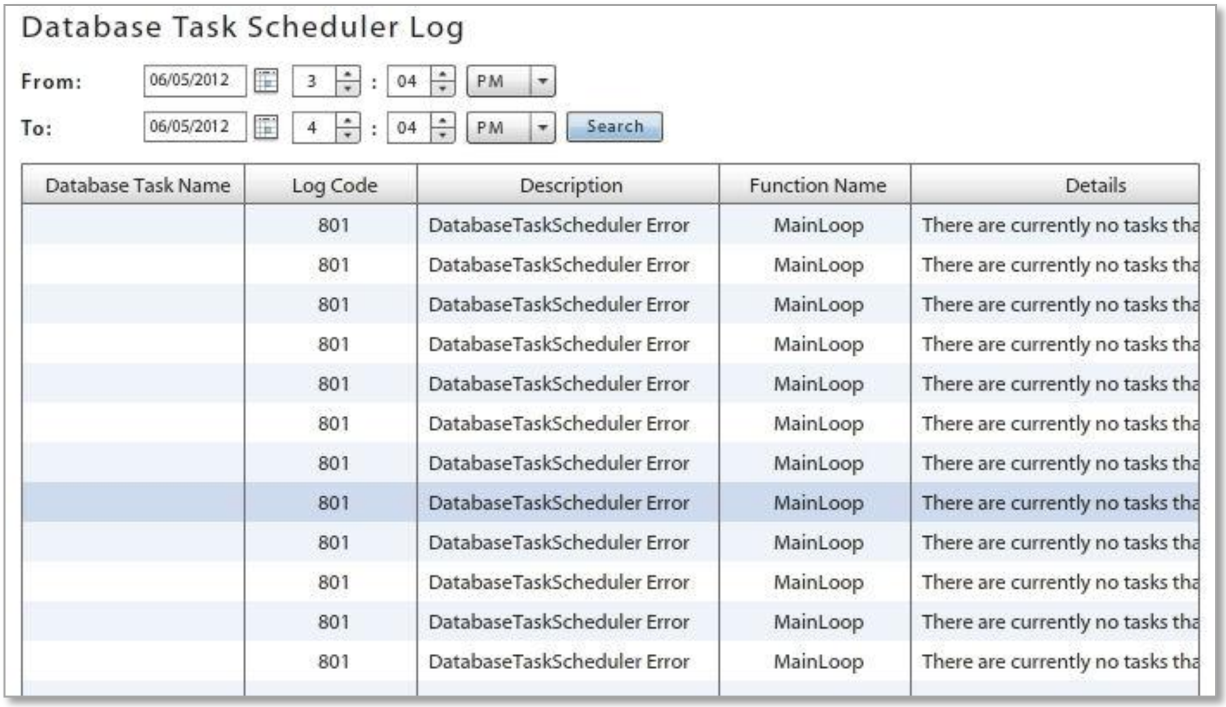
- Database Task Name – Name assigned to the database cleanup task
- Log Code – Code number associated with the logged event
- Description – Description associated with the log code
- Function Name – Displays a returned error; blank when the log event is successful
- Details – Description or reason for 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.



From: 06/05/2012 3 : 04 PM

To: 06/05/2012 4 : 04 PM

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

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***.

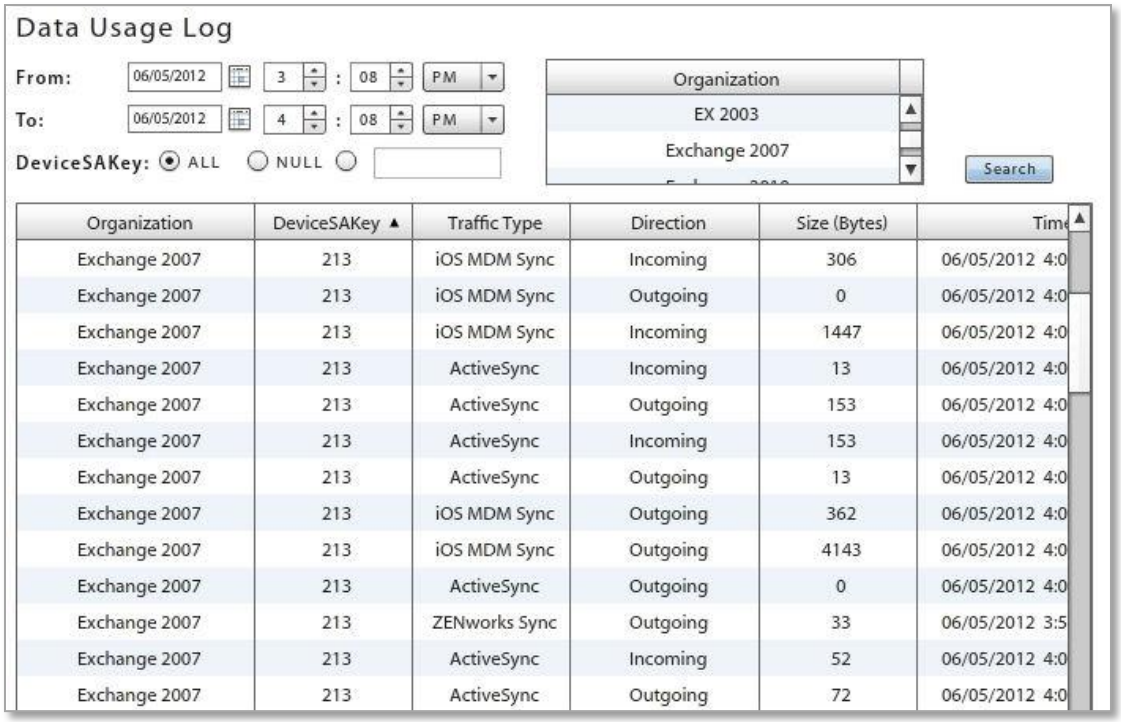
The log populates the grid with system-wide data from the past hour.

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	DeviceSAKey ▲	Traffic Type	Direction	Size (Bytes)	Tim
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

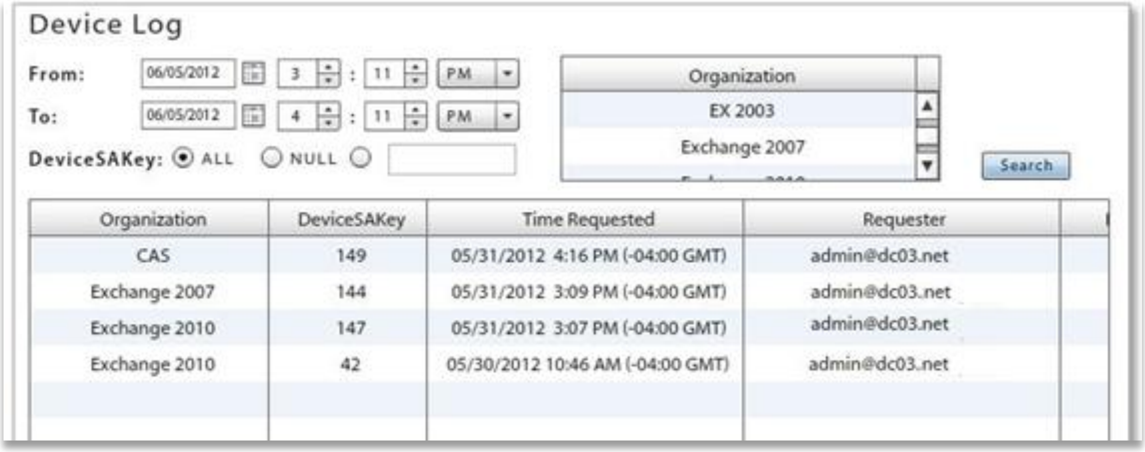
Select ***Device Log***.

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.



Device Log

From: 06/05/2012 3 : 11 PM

To: 06/05/2012 4 : 11 PM

DeviceSAKey: ● ALL ○ NULL ○

Organization
EX 2003
Exchange 2007

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***.

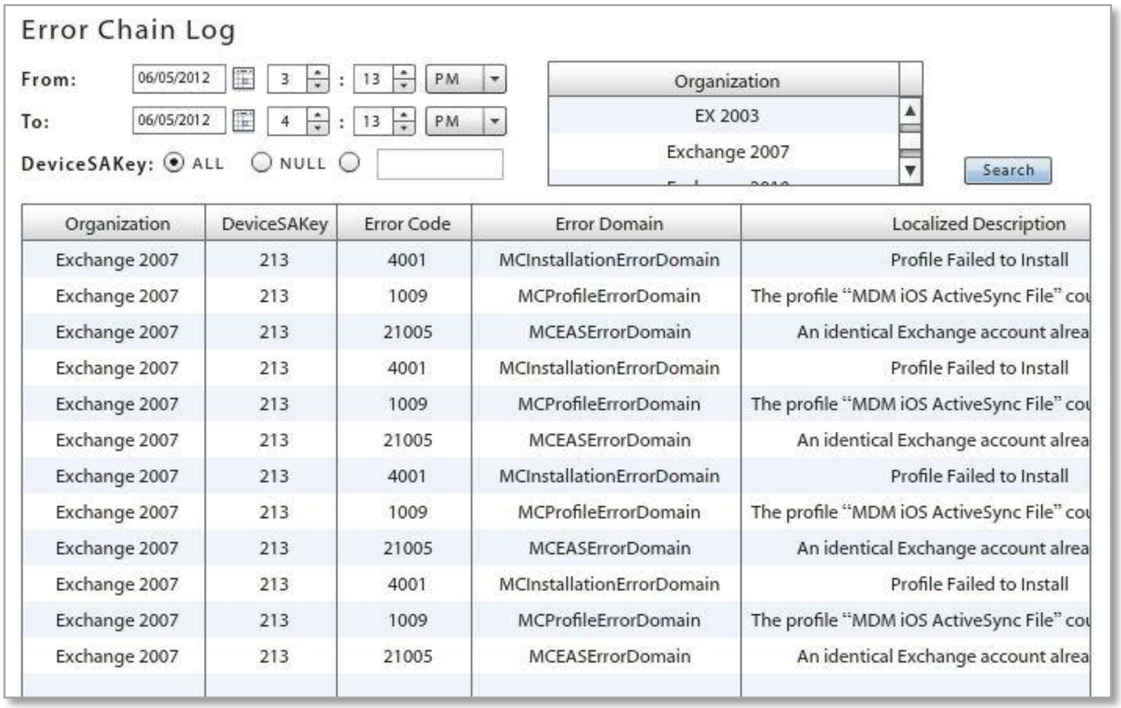
The log populates the grid with system-wide data from the past hour.

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	DeviceSAKey	Error Code	Error Domain	Localized Description
Exchange 2007	213	4001	MCInstallationErrorDomain	Profile Failed to Install
Exchange 2007	213	1009	MCProfileErrorDomain	The profile "MDM iOS ActiveSync File" cou
Exchange 2007	213	21005	MCEASErrorDomain	An identical Exchange account alrea
Exchange 2007	213	4001	MCInstallationErrorDomain	Profile Failed to Install
Exchange 2007	213	1009	MCProfileErrorDomain	The profile "MDM iOS ActiveSync File" cou
Exchange 2007	213	21005	MCEASErrorDomain	An identical Exchange account alrea
Exchange 2007	213	4001	MCInstallationErrorDomain	Profile Failed to Install
Exchange 2007	213	1009	MCProfileErrorDomain	The profile "MDM iOS ActiveSync File" cou
Exchange 2007	213	21005	MCEASErrorDomain	An identical Exchange account alrea
Exchange 2007	213	4001	MCInstallationErrorDomain	Profile Failed to Install
Exchange 2007	213	1009	MCProfileErrorDomain	The profile "MDM iOS ActiveSync File" cou
Exchange 2007	213	21005	MCEASErrorDomain	An identical Exchange account alrea

Licensing Log

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

The log displays:

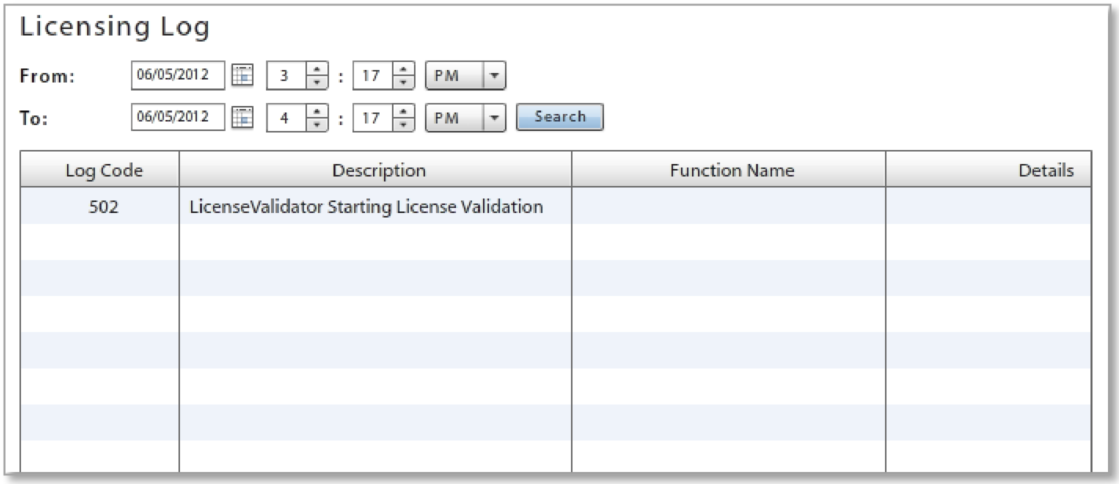
- Log Code – Code number associated with the logged event
- Description – Description associated with the log code
- Function Name – Displays a returned error; blank when log event is successful
- Details – Description or reason for the error; blank when log event is successful
- Time stamp – Date and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



Licensing Log

From: 06/05/2012 3 : 17 PM

To: 06/05/2012 4 : 17 PM

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***.

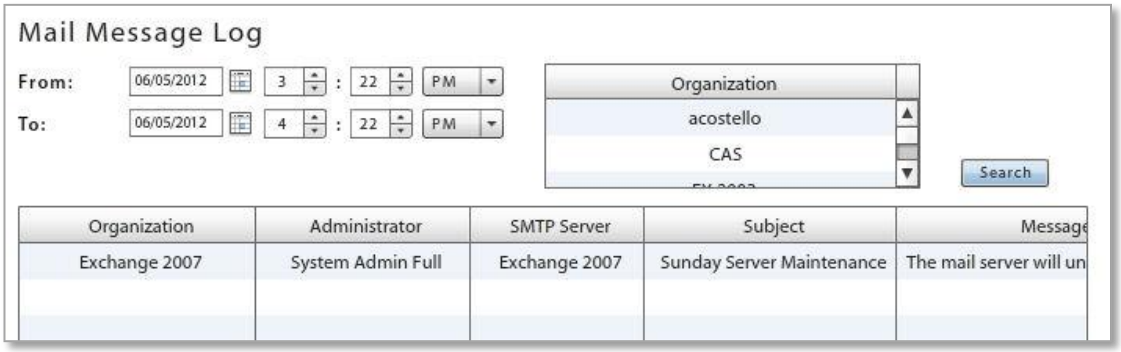
The log populates the grid with system-wide data from the past hour.

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.



From: 06/05/2012 3 : 22 PM

To: 06/05/2012 4 : 22 PM

Organization
acostello
CAS

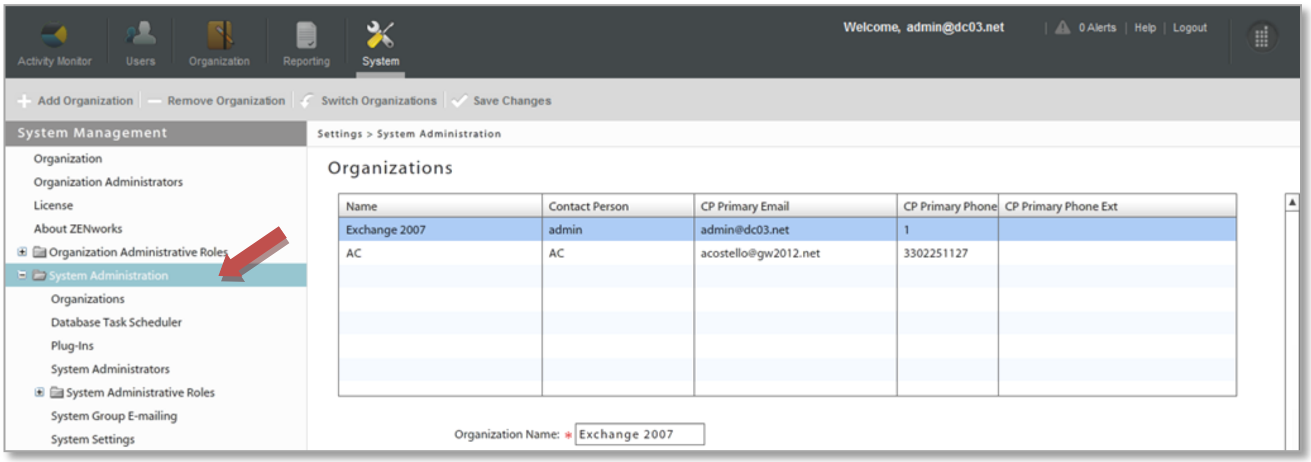
Organization	Administrator	SMTP Server	Subject	Messag
Exchange 2007	System Admin Full	Exchange 2007	Sunday Server Maintenance	The mail server will un

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.



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	

Organization Name: * Exchange 2007

Managing Multiple Organizations

Multi-Tenant ZENworks Mobile Management Systems

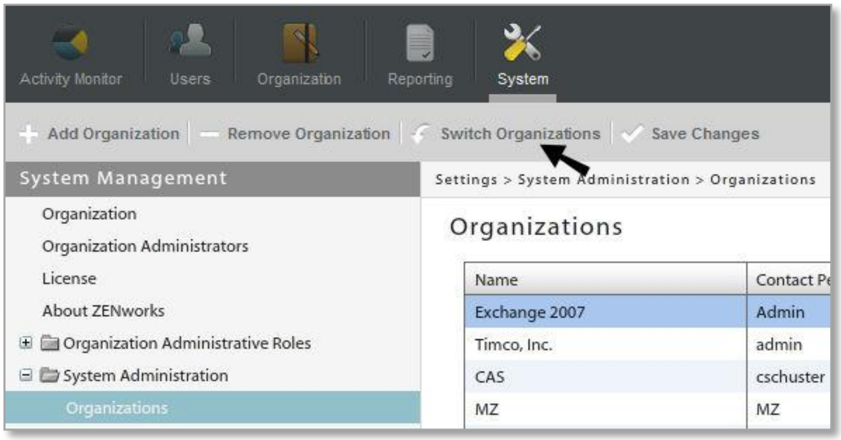
A single instance of the *ZENworks Mobile Management* server application supports a multi-tenant architecture, which allows an enterprise to manage one or multiple organizations.

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.



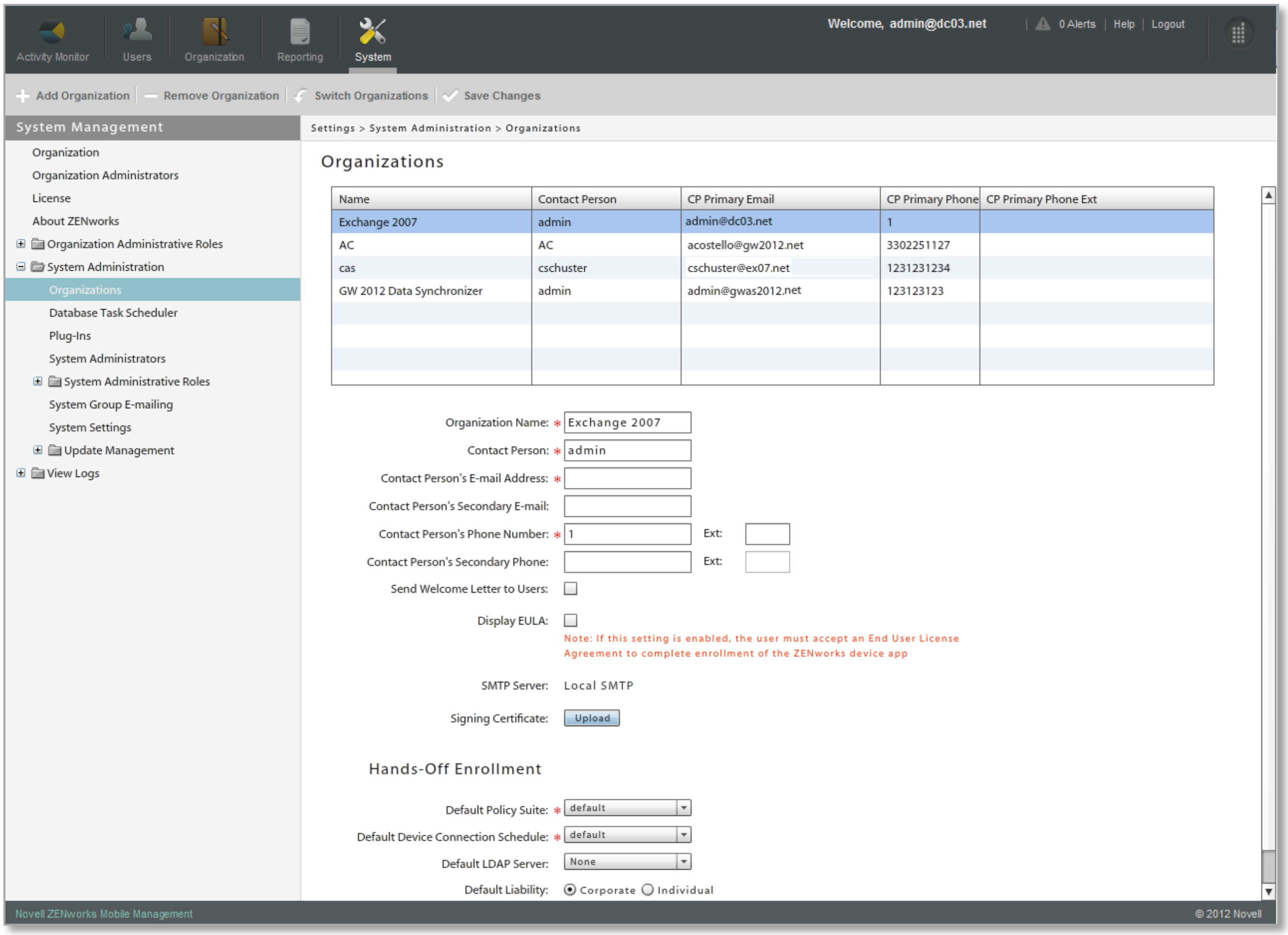
Organizations

Name	Contact Pe
Exchange 2007	Admin
Timco, Inc.	admin
CAS	cschuster
MZ	MZ

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
- EULA enablement - when this option is enabled, users must accept an End User License Agreement to complete ZENworks Mobile Management app enrollment
- SMTP server name
- Signing certificate Upload button (see description below)
- Hands-Off enrollment configuration
    - Default Policy Suite
    - Default Device Connection Schedule
    - Default (*Administrative*) LDAP Server
    - Default Liability



Organizations

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	
cas	cschuster	cschuster@ex07.net	1231231234	
GW 2012 Data Synchronizer	admin	admin@gwas2012.net	123123123	

Organization Name: * Exchange 2007
Contact Person: * admin
Contact Person's E-mail Address: *
Contact Person's Secondary E-mail:
Contact Person's Phone Number: * 1 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
SMTP Server: Local SMTP
Signing Certificate: Upload

Hands-Off Enrollment

Default Policy Suite: * default
Default Device Connection Schedule: * default
Default LDAP Server: None
Default Liability: ● Corporate ○ Individual

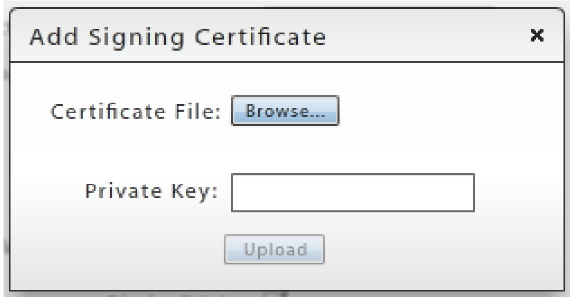
Signing Certificate Upload

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.

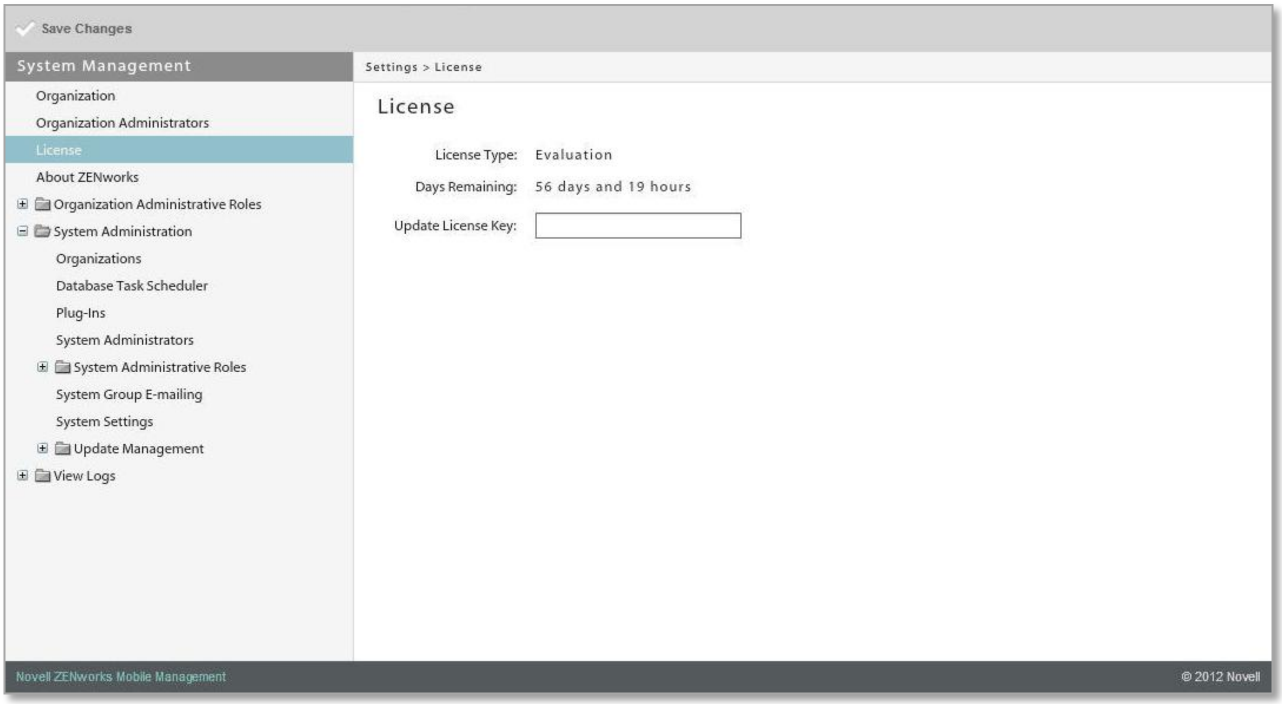


3. Click the ***Browse*** button, then navigate to and select the file containing the certificate.
4. Enter the ***Private Key*** associated with the certificate and click ***Upload***.
5. Click ***Save Changes*** on the gray option bar.

License

If you are extending a *ZENworks Mobile Management* software evaluation license or moving to a license for a purchased copy of the software, you must enter a new license key for the server. Updating the license requires full system admin login credentials.

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 ***Update License Key*** field and select ***Save Changes***.



License Type: Evaluation
Days Remaining: 56 days and 19 hours

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.***

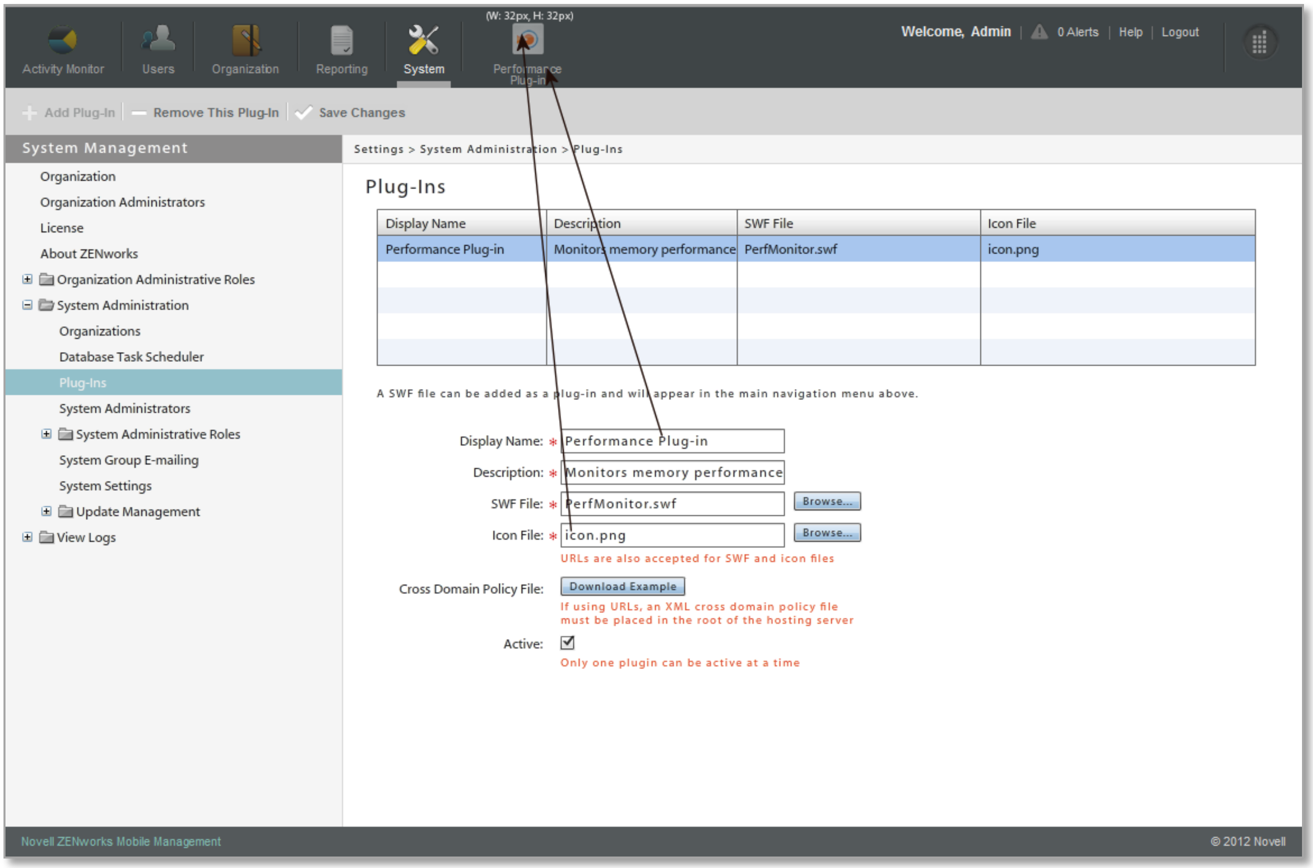
Plug-Ins

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.



Display Name	Description	SWF File	Icon File
Performance Plug-in	Monitors memory performance	PerfMonitor.swf	icon.png

A SWF file can be added as a plug-in and will appear in the main navigation menu above.

Display Name: * Performance Plug-in

Description: * Monitors memory performance

SWF File: * PerfMonitor.swf

Icon File: * icon.png

URLs are also accepted for SWF and icon files

Cross Domain Policy File:

If using URLs, an XML cross domain policy file must be placed in the root of the hosting server

Active: ☑

Only one plugin can be active at a time

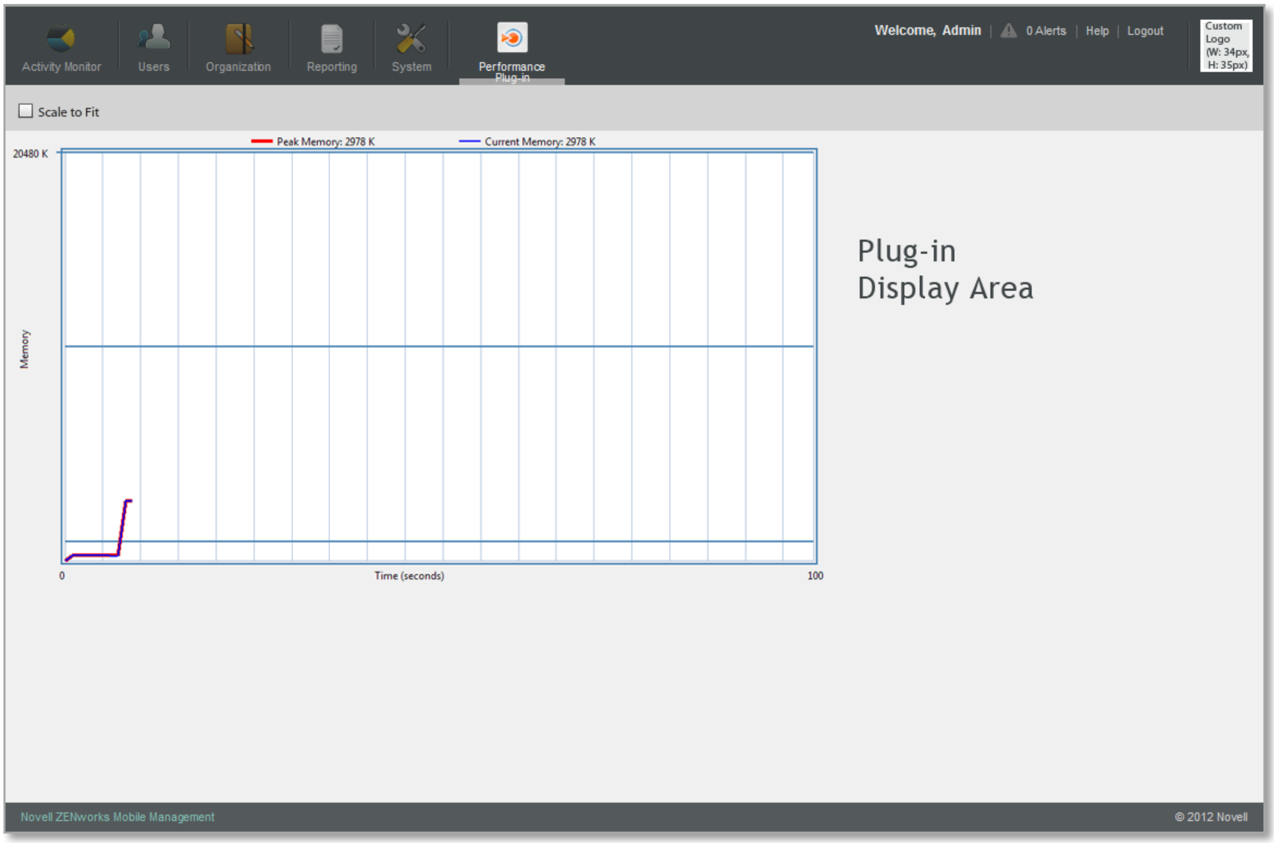
Sample ZENworks Dashboard with SWF Plugged In

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.

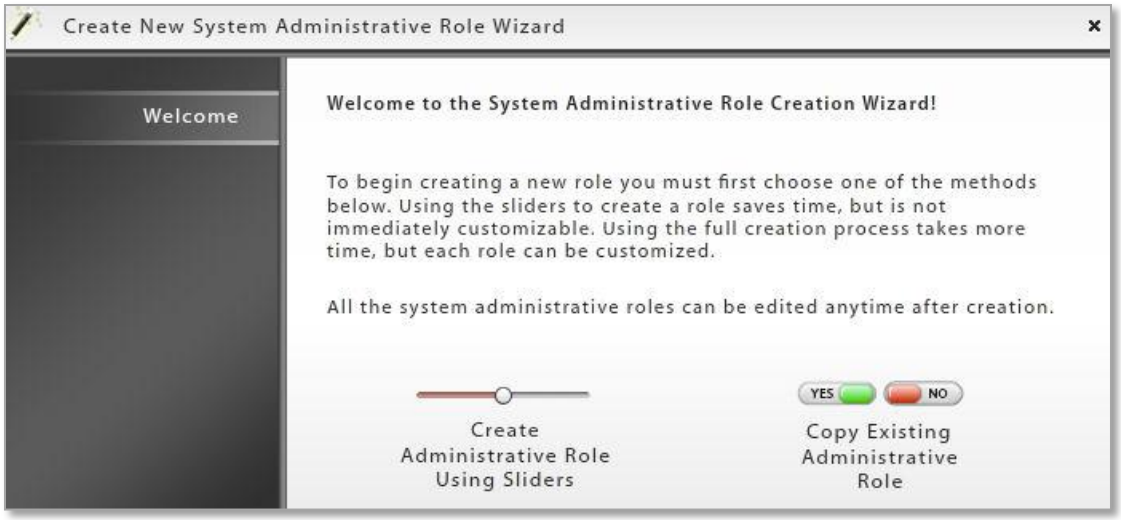
SYSTEM ADMINISTRATOR ROLES		
Dashboard View	**Support System Admin**	**Restricted System Admin**
Activity Monitor	Read-only access; cannot disable or snooze alerts	Read-only access; cannot disable or snooze alerts
Users	• Can add or remove users and perform all the functions in the right-hand *Details*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

Welcome

Welcome to the System Administrative Role Creation Wizard!

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

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

Create Administrative Role Using Sliders
YES
NO
Copy Existing Administrative Role

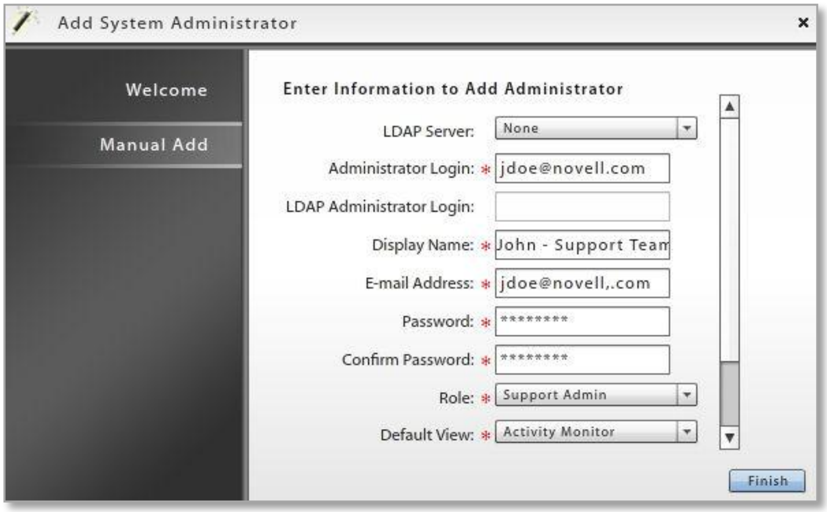
2. Choose a method for creating a System Administrative Role:
   - Use the sliders to determine the role's initial settings. The new role copies the settings of the predefined System *Full Admin*, *Support Admin,* or *Restricted Admin*.
   - Copy the settings of an existing role
3. Specify the role permissions 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.

System Administrator Logins

See also, Organization Administrator Logins

Creating System Administrator Logins

Select ***System*** > ***System Administration*** > ***System Administrators*** > ***Add System Administrator***.



Enter Information to Add Administrator

LDAP Server: None
Administrator Login: * jdoe@novell.com
LDAP Administrator Login:
Display Name: * John - Support Team
E-mail Address: * jdoe@novell,.com
Password: * ********
Confirm Password: * ********
Role: * Support Admin
Default View: * Activity Monitor

The Add Administrator Wizard steps you through creating login credentials for system administrators.

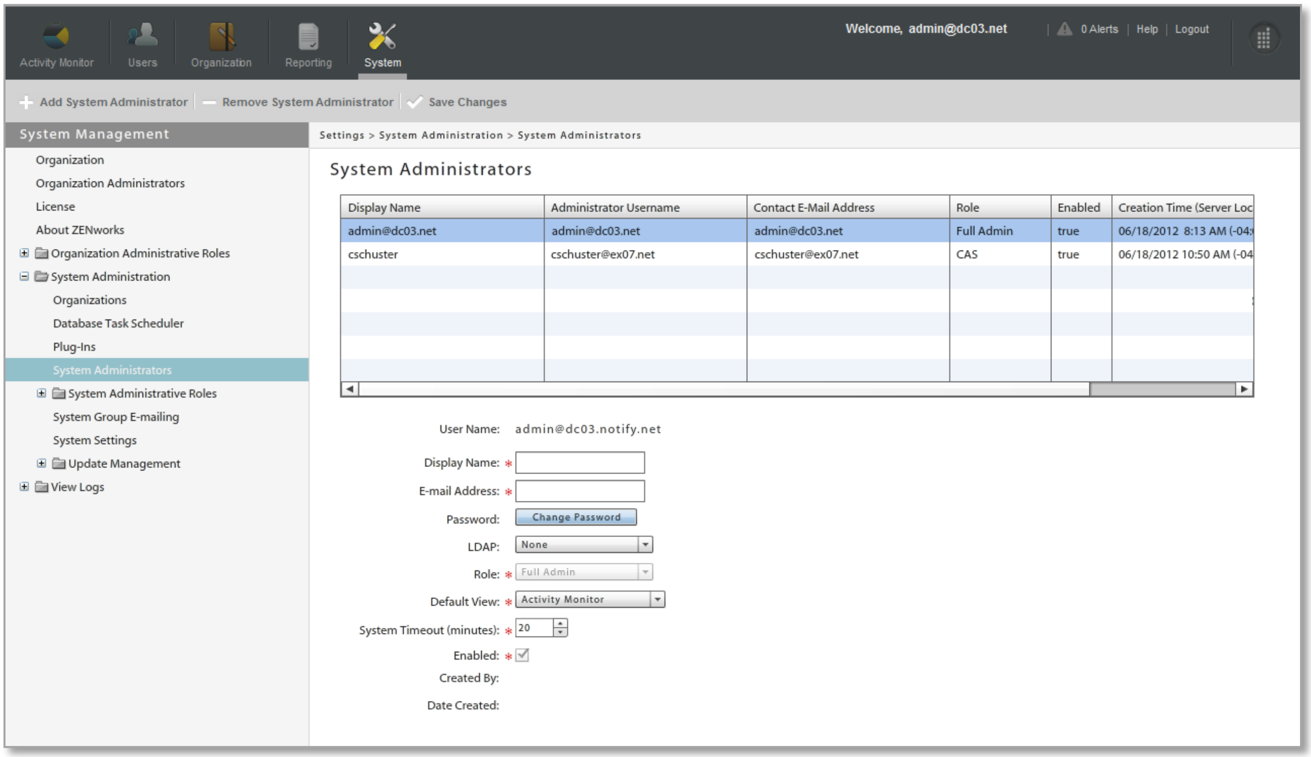
The Wizard asks for the following information:

- **LDAP server** with which this user is associated (optional) if you are creating LDAP authentication logins. (*Administrator Login* and *Password* fields are disabled if you choose this option.)
- **Administrator Login** – Enter the administrator's email address to be used as a username (if the user is not using LDAP authentication).
- **LDAP Administrator Login** – Enter the administrator's LDAP server user name if the user is using LDAP authentication.
- **Display Name** – Enter the name to display for this login.
- **Email address** – Enter the contact email address of the user.
- **Password** – Assign a password if you are creating a login that does not use LDAP authentication.
- **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

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.

1. Select ***System*** > ***System Administration*** > ***System Administrators***.
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***.



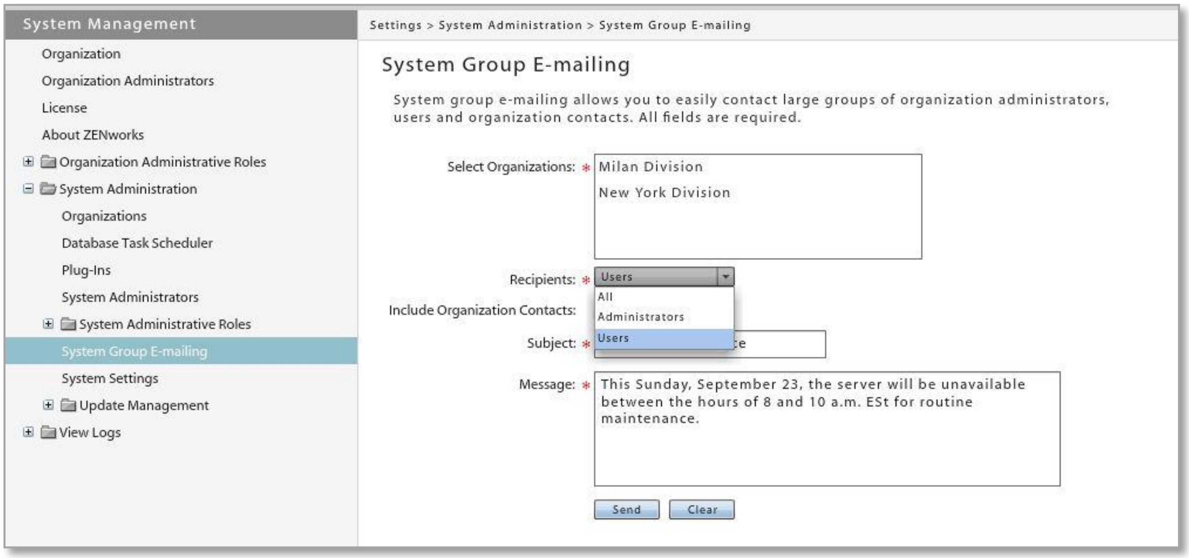
Display Name	Administrator Username	Contact E-Mail Address	Role	Enabled	Creation Time (Server Loc
admin@dc03.net	admin@dc03.net	admin@dc03.net	Full Admin	true	06/18/2012 8:13 AM (-04
cschuster	cschuster@ex07.net	cschuster@ex07.net	CAS	true	06/18/2012 10:50 AM (-04

User Name: admin@dc03.notify.net
Display Name: *
E-mail Address: *
Password:
LDAP: None
Role: * Full Admin
Default View: * Activity Monitor
System Timeout (minutes): * 20
Enabled: * ☑
Created By:
Date Created:

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 Group E-mailing

System group e-mailing allows you to easily contact large groups of organization administrators, users and organization contacts. All fields are required.

Select Organizations: * Milan Division
New York Division

Recipients: * Users

Include Organization Contacts:

Subject: * e

Message: * This Sunday, September 23, the server will be unavailable between the hours of 8 and 10 a.m. ESt for routine maintenance.

System Settings

Custom Dashboard and Login Logos

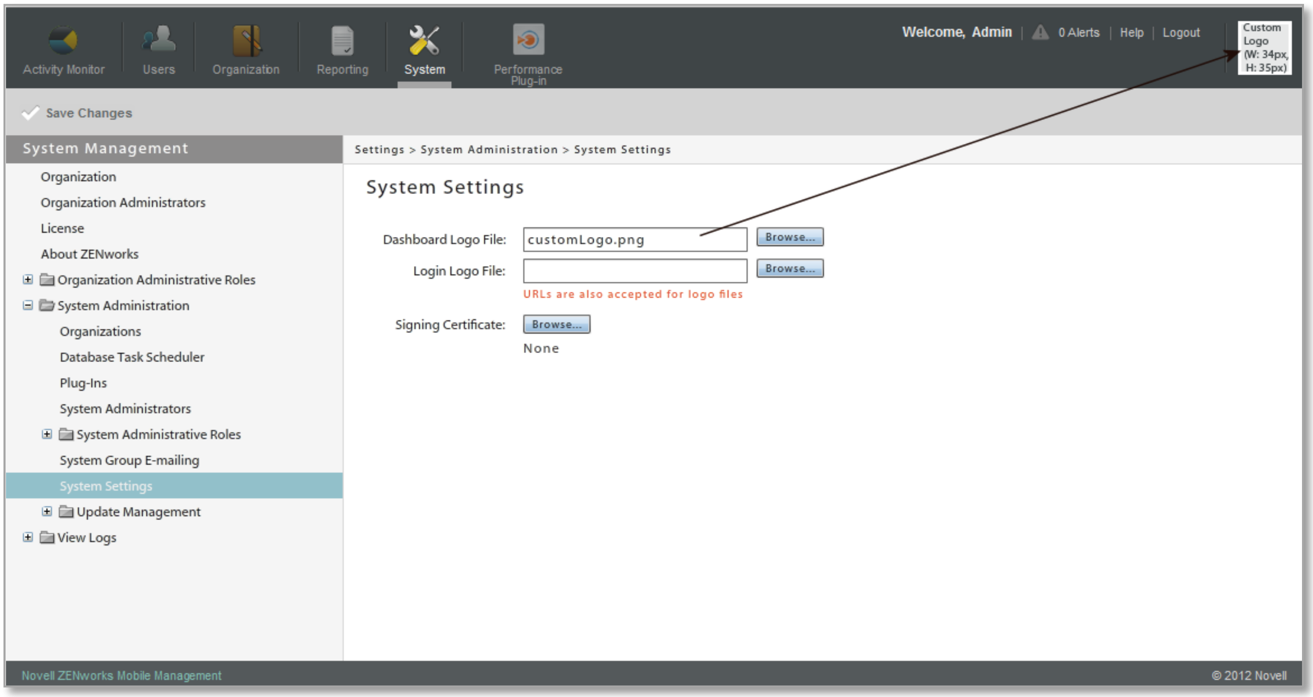
To customize the *ZENworks Mobile Management* server pages, administrators can insert custom logos and icons that appear in *ZENworks Mobile Management*'s dashboard navigation menu and on the *ZENworks Mobile Management* login page.

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



Dashboard Logo File: customLogo.png

Login Logo File:

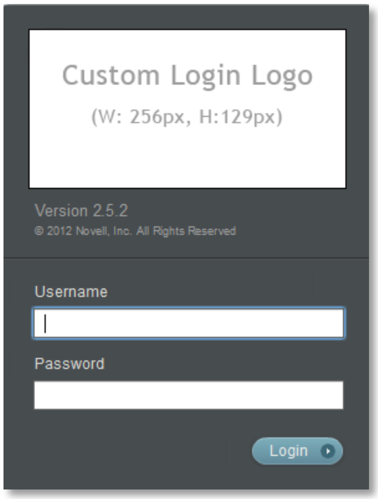
URLs are also accepted for logo files

Signing Certificate: None

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

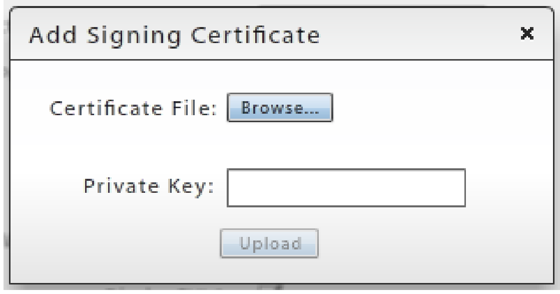
Signing Certificate Upload

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 ***Private Key*** 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

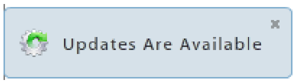
Updates cannot be applied from the dashboard. A system administrator must use the *ZENworks Mobile Management Update Manager* application to install the updates.

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.


Updates Are Available

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. Even though the server automatically checks for updates every 24 hours, you can initiate an on-demand check for updates from this page. You can also download updates from this page in preparation for a scheduled maintenance. Doing this from the dashboard is convenient and allows you to prepare ahead of time for the actual 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.

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 Mobile 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 ***Smart Users and Devices*** 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 Device Enrollment		●	
		Clear Passcode		●	
		Disable Device		●	
		Full Wipe		●	
		Lock Device		●	
		Selective Wipe		●	
		Send Welcome Letter		●	
		Show Recovery Password		●	
		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			●	●
	Location			●	●

Parent Category	First Subset Level	Second Subset Level	Third Subset Level	Full Access	Read Only
	Logging			●	●
	Messaging			●	●
	Remove User			●	
	User Profile			●	●
		Assign CalDAV		●	●
		Assign CardDAV		●	●
		Assign Exchange Servers		●	●
		Assign LDAP Servers		●	●
		Assign Mail Servers		●	●
		Assign SCEP Servers		●	●
		Assign Subscribed Calendars		●	●
		Assign VPN		●	●
		Assign Wi-Fi Networks		●	●
		Audit Data		●	●
		Client Certificates		●	●
		File Archive (File List)		●	●
		iOS MDM Settings		●	●
		Last Sync Data		●	●
		Location Data		●	●
		Search Phone Log		●	●
		Search Text Message Log		●	●
		User Information		●	●
		View Logs		●	●
			ActiveSync Log	●	●
			Data Usage Log	●	●
			Device Log	●	●
			Error Chain Log	●	●
			iOS MDM Sync Log	●	●
			ZENworks Sync Log	●	●
Organization				●	●
	Corporate Resources for iOS Devices			●	●
		CalDAV Servers		●	●
		CardDAV Servers		●	●
		Exchange Servers		●	●

Parent Category	**First Subset Level**	**Second Subset Level**	**Third Subset Level**	**Full Access**	**Read Only**
		LDAP Servers		●	●
		Mail Servers		●	●
		SCEP Servers		●	●
		Subscribed Calendars		●	●
		VPN		●	●
		Wi-Fi Networks		●	●
	Organization Control			●	●
		Compliance Manager		●	●
		File Share		●	●
		Group E-mailing		●	●
		Mobile Apps		●	●
		SMTP Server		●	●
	User Account Settings			●	●
		ActiveSync Servers		●	●
		Administrative LDAP Servers		●	●
		Custom Columns		●	●
		Device Connection 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.