

# Managing Users, Devices, and Groups

**ZENworks® Mobile Management 2.9.x**

May 2014

**Novell.**

## Legal Notices

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

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

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

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

Novell, Inc.  
1800 South Novell Place  
Provo, UT 84606  
U.S.A.  
[www.novell.com](http://www.novell.com)

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

## Novell Trademarks

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

## Third-Party Materials

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

## Table of Contents

<b>Accessing the Dashboard</b>	<b>4</b>
<b>Managing Users</b>	<b>6</b>
The User Grid.....	6
Customizing and Searching the User Grid .....	7
Assigning Settings and Resources to Groups/Folders from the Grid .....	9
The User Panel .....	11
Exporting Data from the User Grid .....	13
Adding / Removing / Disabling Users .....	13
The User Profile .....	14
User Information .....	14
Device Administration .....	18
Corporate Resource Assignments .....	34
Device Summary.....	42
<b>Local Groups</b>	<b>43</b>
Managing Local Groups .....	44
Add a Group and Assign Users .....	45
Edit a Group Name or Change Group Membership .....	45
Prioritizing Groups .....	46
Configure the Group Settings .....	47
Remove a Group.....	48
<b>Appendix A: Recovering User Information</b>	<b>48</b>

# Accessing the Dashboard

## Access the Dashboard

*ZENworks Mobile Management* dashboard requirements:

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

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

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

## Standard Login

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

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

A system administrator can create additional logins to the dashboard with system administrator, organization administrator, or support administrator privileges. See the [System Administration Guide](#) for details.



## OpenID Login

Use your OpenID credentials to log in.

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

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

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



Admin Setup Pin Code

Enter Admin Setup Pin Code

Zone Name

OpenID Identity

OK



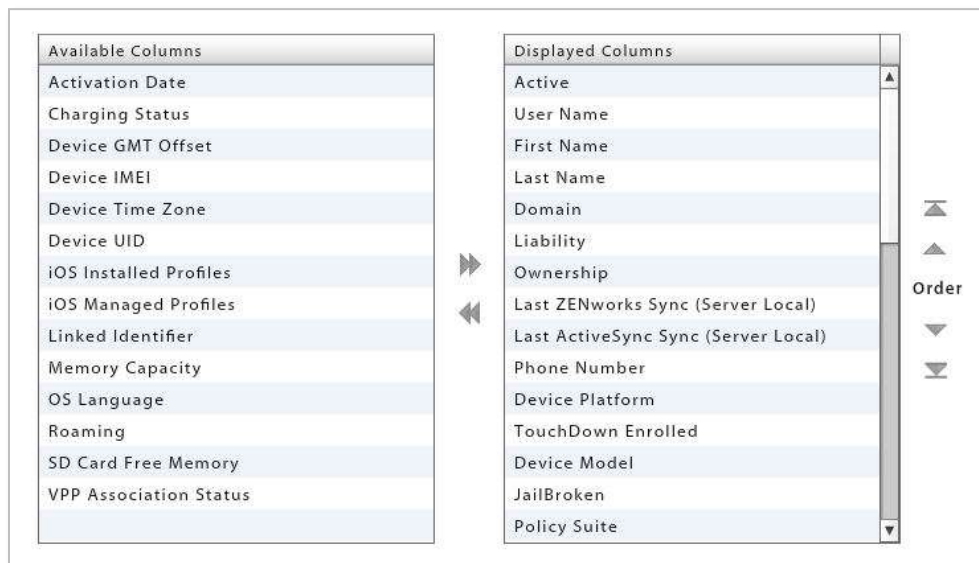


## Customizing and Searching the User Grid

Customize the user list view by:

- Choosing the visible columns
- Rearranging columns
- Sorting columns
- Searching for and displaying a distinct category of users
- Limiting the list to members of an LDAP folder or group

**Choose the visible columns.** Click the *Choose Visible Columns* button in the bottom left corner of the User Grid. Using the forward arrow, move items from the *Available Columns* list to the *Displayed Columns* list so that they will appear in the User Grid. In the *Displayed Columns* list, use the up/down arrows to arrange the columns in the order you want them to appear. The Dashboard saves the columns you choose to view.



**Rearrange columns.** Drag and drop column headings to reorder the columns. The dashboard saves the order in which you arrange the columns.

Active	User Name	Ownership	Last Sync (GMT/UTC)	Device Type	Device Model	Policy Suite
Yes	broberts	Corporate	12/15/2010 3:32 PM	Android	Nexus One	NotifyTe
Yes	dbadger	Personal	12/20/2010 4:18 PM	BlackBerry	9630	NotifyTe
Yes	hburkett	Corporate	12/17/2010 11:23 PM	Android	ADR6300	NotifyTe
Yes	iOStest	Personal	11/23/2010 6:13 PM	iPhone	iPhone 4	NotifyTe
Yes	jconrad	Personal	12/18/2010 1:49 AM	iPhone	iPhone 3GS	Engineer
Yes	jecker@1007dc	Corporate	12/07/2010 7:59 PM	iPhone	iPhone 3GS	NotifyTe

**Sort columns.** Click the heading of any column to sort the list by the information in that column. Sort in ascending or descending order.


User Name ▲	User Name ▼
bking1	ylu01
groover	tgeorge
jecker@dc03.no	sli2
sli	sli
sli2	jecker@dc03.no
tgeorge	groover
ylu01	bking1

**Search for and display a single user or category of users.** Use the search criteria in the drop-down **Search** panel to search for users by user name, phone number, policy suite, device platform, or custom column name and value. The string entered in the search field returns users that contain the string anywhere in the user name.

The image shows a 'Search' dialog box with the following fields and controls:

- User Name:
- Phone Number:
- Policy Suite: -- Select One --
- Device Platform: -- Select One --
- Custom Column Name: -- Select One --
- Custom Column Value: -- Select One --
- Buttons: Search All, Search Folder, Reset

**Display by User Categories.** Limit the display of users in the grid to those in a specific category. There are three major user categories: *Users by LDAP*, *Users by Local Group*, and *Uncategorized Users*. Browse the user category directory and select a local group or LDAP group/folder. The users listed in the grid will contain only the users belonging to the group or folder you chose.

To refresh the grid so that it displays the entire list of users, click the group again, click the refresh button , or click the *Reset* button in the *Search* option.

The image shows the 'Search' dialog box with the 'Display by User Categories' section expanded. The tree view shows the following structure:

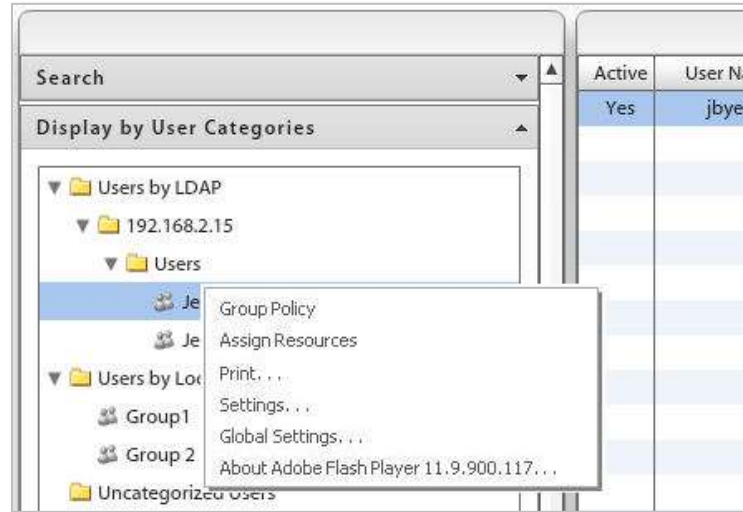
- Users by LDAP
- Users by Local Group (selected)
- Group 1
- Group 2
- Uncategorized Users



## Assigning Settings and Resources to Groups/Folders from the Grid

Settings such as Policy Suite, Connection Schedule, and Liability can be assigned to a local group or LDAP group/folder directly from the user grid. In addition, Android and iOS resources can be assigned to LDAP group/folder directly from the grid.

1. Expand the **Display by User Categories** option on the left panel and navigate to an LDAP group or folder, under *Users by LDAP*, or to a local group under *Users by Local Group*. Right-click on the group or folder.



2. From the pop-up, select the **Group (Folder) Policy** option and choose the Policy Suite, Device Connection Schedule, Liability, and Novell Filr profile\* (if applicable) assignments for the group/folder. Click **Save**.

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



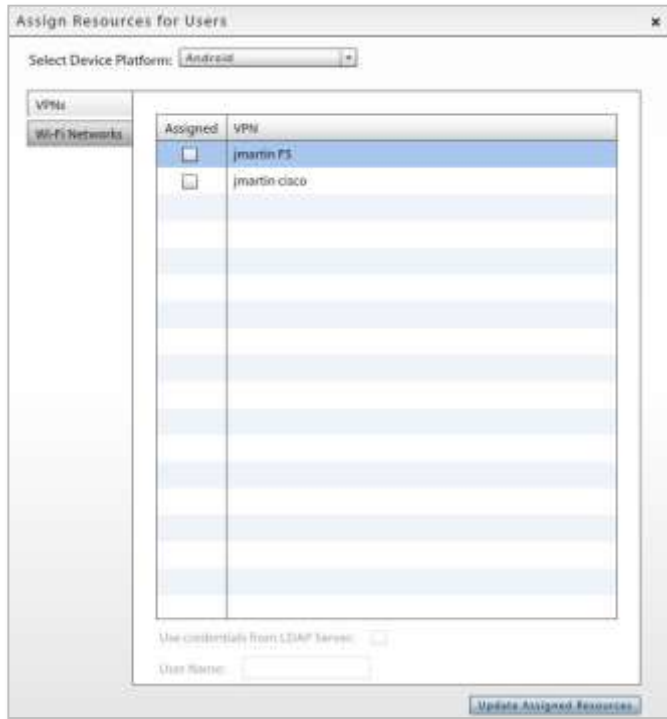
*Standard Policy Enforcement*



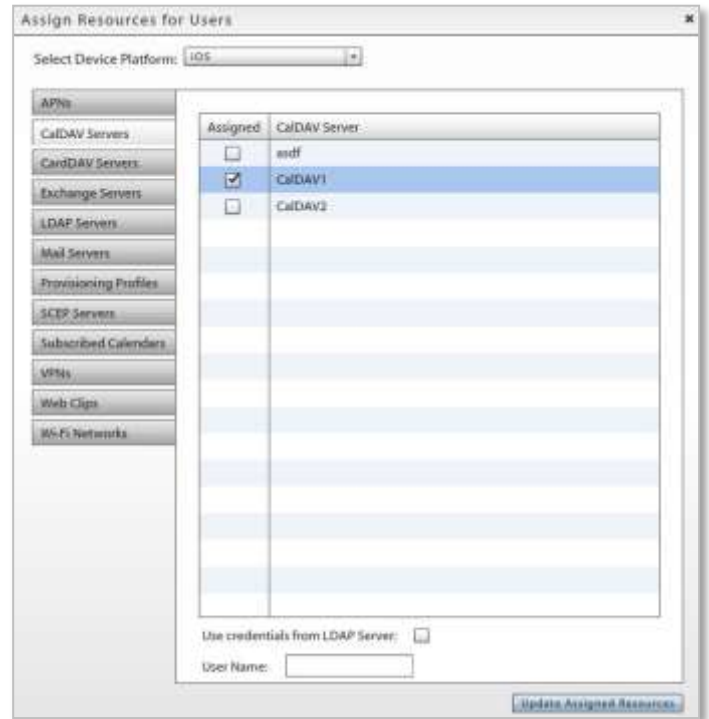
*Schedule-Based Policy Enforcement*

3. Right click on an LDAP group/folder and select the **Assign Resources** option to assign resources.
  - Select a device platform from the drop-down: android or iOS
  - Mark the checkbox next to the resource you want to assign to the group/folder.
  - Mark the checkbox labeled **Use credentials from LDAP Server** to assign the resource to the users associated with the group/folder.

Or, leave the option disabled to assign the resource to a single **User Name** from the group or folder.



*Android Resource Assignments*



*iOS Resource Assignments*

## The User Panel

Select a user from the user grid. A user panel for that user appears in a column to the left of the grid. Only administration options that apply to the device platform will appear in the panel.



### Panel Content

- **Quick Device Stats** - displays last sync time, device platform, ownership, and phone number
- **Pop-up Views** - provides the following links to pop-up views:
  - [See Most Recent Location](#) - Location statistics
  - [E-mail User](#) - Compose and send an email
  - [View Device Report](#) - Device statistics
- **Device Compliance** – allows the administrator to clear a violation restriction or view device violation details and create a User Exception for a violation. See [Monitoring Device Compliance](#) for details.
- **Security Commands** - Gives quick access to reactive security commands, such as *Full Wipe*. See [Remote Security Commands](#) for functionality. Security commands can also be issued through the User Self Administration Portal.
- **Show Recovery Password** - Allows the administrator to view the recovery password issued by a device. User can also view the recovery password through the User Self Administration Portal. See [Enabling Password Recovery](#).
- **Send VPP Invitation** - Send an invitation to an iOS 7.0.3+ user to join the Apple Volume Purchase Program if they have not yet been invited or have not yet accepted an invitation. Check user's status in the *VPP Association Status* column of the *User Grid*.
- **Send Welcome Letter** - Send the Welcome Letter email to the user.
- **Reset for Enrollment** – Used for troubleshooting enrollment issues. Clears server data that prevents a user from re-enrolling a device or reloading iOS profiles when a device experiences enrollment issues.
- **Clear Passcode** – The iOS device passcode is cleared. If the passcode is required by the user's policy, the user is prompted to enter a new passcode.
- **Trigger APN / Trigger GCM** – Sends an immediate notification to an iOS / Android device causing it to retrieve pending commands from the server and send latest stats and location.

## Monitoring Device Compliance from the User Panel

If you have implemented the *Compliance Manager* to monitor and restrict devices or users who are non-compliant with corporate policies, you might want to display the **Violation Status** column in the *Users* grid. You can quickly see which devices are restricted. Use the following options in the *User Panel* to view details about the restriction or release a user from the restriction.

Administrative Action	Description	Result
View Device Violation Details	An administrator can view violations and use the <i>Clear Selected Violations</i> button to release a device from restrictions.	The administrator can select and clear a violation listed in the pop-up dialog box. The device is released from restrictions imposed by the violation. An exception is created for the user, which prevents the device from being restricted again because of this violation.
Clear ZENworks Authorization Failures	A device passes invalid credentials for the <i>ZENworks Mobile Management</i> account of a known user to the server a number of times that exceeds the set limit.	This <i>Clear</i> button releases the device from restrictions imposed by this violation. The counter for the set <i>Failed login attempt limit</i> is reset to zero.  A <i>User Exception</i> is not created, so if the device's <i>ZENworks Mobile Management</i> connections continue to fail, the device is in violation again.
Clear ActiveSync Authorization Failures	A device passes invalid credentials for the ActiveSync account of a known user to the server a number of times that exceeds the set limit.	This <i>Clear</i> button releases the device from restrictions imposed by this violation. The counter for the set <i>Failed login attempt limit</i> is reset to zero.  A <i>User Exception</i> is not created, so if the device's ActiveSync connections continue to fail, the device is in violation again.
Clear SIM Card Removed or Changed Violations	A user has removed or changed the SIM card in a device and is in violation of the <i>Restrict if SIM Card is Removed or Changed</i> access restriction.	This <i>Clear</i> button releases the device from restrictions imposed by this violation.  A <i>User Exception</i> is not created, so if the SIM card is removed or changed again, the device is in violation.



*Violation Details Pop-up*

## Exporting Data from the User Grid

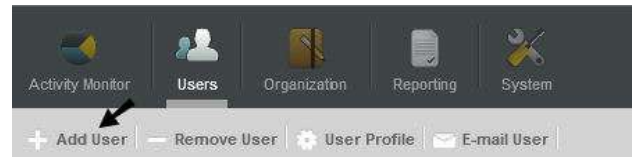
Exporting data from the list to a comma separated values (CSV) or Excel (XLS) file. Choose the *Export Format*, then click the *Export Data Grid* button to save the current grid to a file.



## Adding / Removing / Disabling Users

The **Add User** button launches a window that allows the manual addition of individual users or addition of users via batch import methods (.CSV file or an LDAP server).

For more documentation on adding users, see the [Configuration Guide: Adding Users, Enrolling Devices](#).



Add User button

The **Remove User** button deletes the user from the *ZENworks Mobile Management* server. A user can also be temporarily disabled by using the *Disable Device* option on the User Panel. This prevents the device from synchronizing with the *ZENworks Mobile Management* and ActiveSync servers, but retains the user account.



The **Disable Device** option can be used when you want to disable device synchronization, but not remove the user from the system. Initiate the command from the *User Panel* or from the *Security* option in the User Profile Administration view.



---

## The User Profile

Select a user from the list and click the **User Profile** button on the action bar above the grid (or double-click the user). There are several views to select from in the menu panel to the left.

### User Information

Select *User Information* from the left panel of the User Profile. There are four tabs that display the following user information:

- [Configuration](#)
- [Custom Column Values](#)
- [Certificates](#)
- [Local Groups](#)

### User Information: Configuration

Select the *Configuration* tab to display basic user information that can be edited.

In addition, server address information obtained by ActiveSync Autodiscover displays for users interfacing with servers using ActiveSync protocol version 12.0 or higher. This information does not display if ZENworks *Mobile Management* does not resolve a server address via Autodiscover. Failure to resolve might occur if the ActiveSync server is not configured for Autodiscover, if the DNS is not configured for the correct Autodiscover address, or if general network issues occur.

You can also override the organization default setting for **Maximum Number of Devices Per User** by removing the checkmark from the *Auto* box and defining the maximum number of devices this user can enroll.

The screenshot shows the 'Configuration' tab of the user profile for 'jwitmer'. The left sidebar contains a tree view with 'Devices (1)' expanded to show 'iPhone 4', and 'Administration' containing 'Corporate Resources' and 'All Devices Summary'. The main content area has three tabs: 'CONFIGURATION' (selected), 'CUSTOM COLUMN VALUES', and 'CERTIFICATES'. The configuration fields include: 'User Name: jwitmer', 'Created On: 2013-09-06 11:41:17.353', 'ActiveSync Server: Exchange 2007', 'LDAP Server: None', 'Password: Change Password', 'Expiration: Never', 'First Name: [empty]', 'Last Name: [empty]', 'E-mail Address: [empty]', 'Domain: ea07', and 'Maximum Number of Devices Per User: 00' with a checked 'Auto (organization default)' checkbox.

### User Information: Custom Column Values

If custom columns have been configured, they will be displayed here. Select this tab to view custom column values for this user. The values can be edited here, as well.



## User Information: Certificates

Select the *Certificate* tab to upload a client authentication certificate for the user or view any identity certificates that are associated with the user.

A certificate can be uploaded here by an administrator or via the *ZENworks Mobile Management Desktop* User Self-Administration portal by a user. Users can then install the certificate on the device using the *ZENworks Mobile Management* Mobile User Self-Administration portal.

It is possible to upload more than one certificate to the user's profile; however, only one certificate at a time can be used. One certificate can be used on multiple devices associated with a single user.

The *ZENworks Mobile Management* server supports .cer, .pfx, or .p12 format certificates. Functionality of these certificate file formats is dependent upon the device platform or operating system (see the table below listing tested device operating systems). Certificates obtained from *VeriSign* have been tested and verified as functional. Certificates obtained from other certificate authorities might be functional if the device platform recognizes the certificate authority as trusted.

**Test Certificate Validity.** Use the **Test Now** button to test the validity of the client certificate. Initiating the test verifies whether the certificate is in a format that can be read, and it verifies the certificate name and expiration date.

Tests initiated for a.pfx format certificate will require the certificate's assigned password.

**When the ZENworks Mobile Management server is behind your corporate firewall.** In this scenario, users must have a client authentication certificate to access your network, but must first acquire the certificate via the *ZENworks Mobile Management* server, which sits behind the network's corporate firewall.

Use one of the following methods to make the certificate accessible to the user:

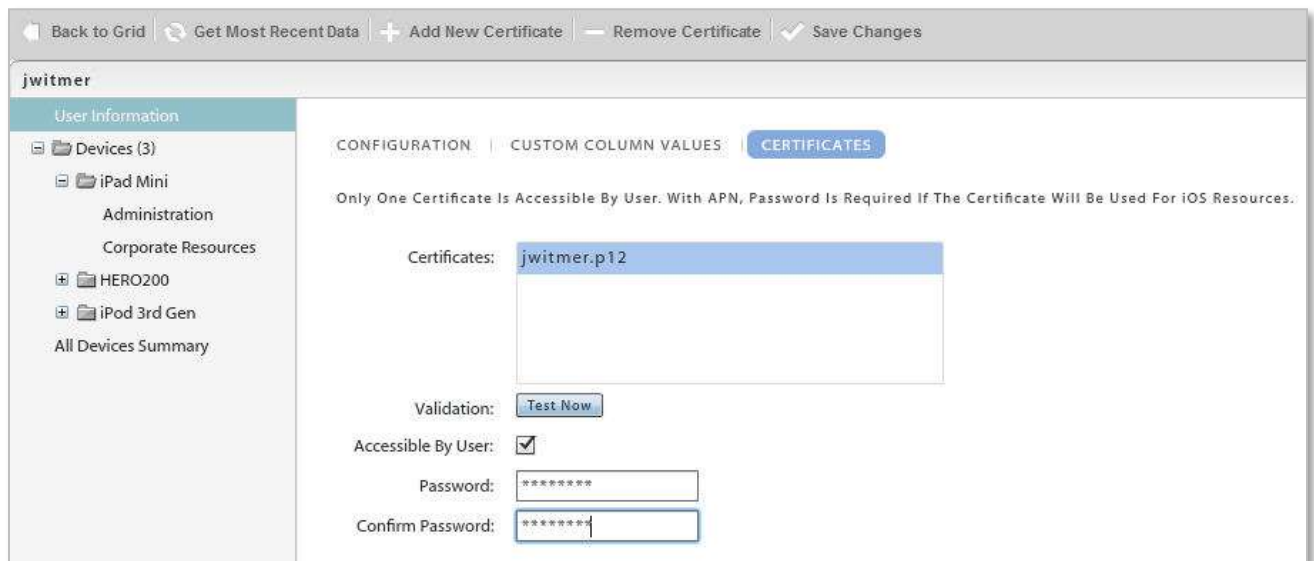
- Instruct users to install the certificate, while in the corporate setting, using Wi-Fi.
- Locate the *ZENworks Mobile Management* Desktop and Mobile User Self-Administration portals outside the corporate firewall.
  - Assign a second address to the *ZENworks Mobile Management* server for the User Self-Administration Portal, allowing access to only these user portals.
    - Desktop User Self-Administration Portal: <serveraddress>
    - Mobile User Self-Administration Portal: <serveraddress>/mobile
  - Create a second Web server (mirroring the *ZENworks Mobile Management* server) where only the User Self-Administration Portals are available
  - Create a firewall rule that allows the user to access the User Self-Administration Portal URLs without a certificate.

**Upload the Certificate.** When you have obtained a client certificate, upload it to the user's profile. You must have access to the certificate file itself and know any password associated with it.

Alternatively, you can have a user upload the certificate himself using the *ZENworks Mobile Management Desktop User Self-Administration* portal. The user must have access to the certificate file and know any password associated with it.

To upload a certificate file:

1. Access the **Users** view of the dashboard. Select a user from the grids and click **User Profile**.
2. Select **User Information** from the left panel, then select the **Certificates** tab.
3. Select the **Add New Certificate** button to browse and select the certificate file.
4. Check the box **Accessible By User** to designate this as the active certificate. It is possible to upload more than one certificate to the user's profile, however, only one certificate at a time can be active. One certificate can be used on multiple devices associated with a single user.
5. If the certificate is protected by a password, enter the **Password** and confirm it.
6. Click **Save Changes**.



**Instruct the User to Install the Certificate.** When the certificate has been uploaded and associated with a user account, instruct the user to install the certificate on the device via the *ZENworks Mobile Management Mobile User Self-Administration Portal*. An example of the installation process for each device type is available in *Appendix A* of every *ZENworks Mobile Management* device user guide.

Certificate Formats Supported on Various Device Platforms		
	.cer	.pfx / .p12
Android	OS 2.1 update 1	
	OS 2.2	OS 2.2
	OS 2.3	OS 2.3
	OS 2.3.4	OS 2.3.4
BlackBerry	OS 4.5	



(with GO!NotifySync)		
	OS 4.6	
	OS 5.0	
	OS 6.0	OS 6.0
	OS 7.0	OS 7.0
iOS	iOS 4.1	iOS 4.1
	iOS 4.3.5	iOS 4.3.5
	iOS 5+	iOS 5+
Symbian	OS 9.1	OS 9.1
	OS 9.2	OS 9.2
Windows Mobile	OS 6.1 Standard	OS 6.1 Standard
	OS 6.1 Professional	OS 6.1 Professional
	OS 6.5 Professional	OS 6.5 Professional

## User Information: Local Groups

[\(return to User Information menu\)](#)

Select the *Local Groups* tab to view the local groups with which the user is associated.

You can add or remove local group assignments for the user, as well. Changes to a user's group association will update the user's policy suite, connection schedule, and liability settings accordingly.

aeinstein

User Information

Devices (1)

Unknown

Administration

Corporate Resources

All Devices Summary

CONFIGURATION | CUSTOM COLUMN VALUES | CERTIFICATES | LOCAL GROUPS

Add or remove local group assignments for the user.

Assigned	Group Name
<input checked="" type="checkbox"/>	Department Heads
<input type="checkbox"/>	School of Graduate Studies
<input type="checkbox"/>	College of Business Administration
<input checked="" type="checkbox"/>	College of S.T.E.M.
<input type="checkbox"/>	College of Liberal Arts & SS
<input type="checkbox"/>	College of Creative Arts & Comm

## Device Administration

The user's devices are listed in the selection panel. Select a device and expand the menu underneath it. Choose **Administration** and choose from tabs to view information about the device.

- [Device Information](#)
- [Configuration](#)
- [Security](#)
- [Location](#)
- [Phone Calls and Texts](#)
- [Viewing Logs](#)
- [File List](#)

### Device Administration: Device Information

[\(return to Device Administration menu\)](#)

Select the **Device Information** tab to view device statistics from the latest synchronization. The information available varies by device platform. If a device does not report a statistic, *N/A* (not available) is displayed. See the document, [Device Platform Comparison: Device Statistics](#) for detailed information.

*Device Information* for iOS devices will also list the *iOS Installed Profiles*. The device periodically sends a list of all configuration profiles assigned to the device which can be viewed here.

The screenshot displays the 'Device Administration' interface for a user named 'gcochenour'. The left sidebar shows a navigation menu with 'Administration' selected. The main content area is titled 'DEVICE INFORMATION' and contains the following data:

Category	Details
<b>Status</b>	Last Connections: Device App: 01/10/2013 6:56 PM (-05:00 GMT) ActiveSync: N/A
<b>Battery</b>	Level: 78% Status: Unplugged Last Boot Time: 01/10/2013 4:33 PM (-05:00 GMT)
<b>Encryption</b>	Device Encrypted: No Storage Card Encrypted: No
<b>Device Memory</b>	Capacity: 2.60 GB Available: 2.42 GB Percent Free: 93%
<b>External Storage Card</b>	Capacity: 14.88 GB Available: 14.88 GB Percent Free: 100%
<b>Jailbroken</b>	Jailbroken: No
<b>TouchDown</b>	TouchDown Registered: Yes
<b>Roaming</b>	Currently Roaming: No
<b>Network</b>	Downloaded Data: Any: 0.018 GB Cellular: N/A Wi-Fi: N/A
<b>About</b>	Device Application: Version: 2.7.0.2 Language: English (United States) ActiveSync: Version: N/A User Agent: N/A Operating System: Language: English (United States) Version: 2.2.1 Device: Model: N/A Ownership: Personal Platform: Android UID: 00000000-3ab2-d291-bf24-ed4010e41303 IMEI: N/A Phone Number: +2169706981 Timezone: Eastern Standard Time GMT Offset: -05:00 Product Name: N/A

## Device Administration: Configuration

[\(return to Device Administration menu\)](#)

Select the **Configuration** tab to view the Policy Suite, Device Connection Schedule, Liability, and Novell Filr profile\* (if applicable) assigned to the device. The source from which each setting originated is displayed in parentheses below the drop down box. When the **Auto** check boxes are marked, the device is assigned the setting based upon local group membership, LDAP group/folder membership, or organization defaults. Changes made to local group settings, LDAP group/folder settings, or organization defaults will automatically update the user's assignments.

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

If you wish to override the automatic assignments, remove the checkmark and select a new setting from the drop-down list. These direct assignments take precedence over all other provisioning sources and will not change as a result of updates to the groups or defaults.

Ownership, Plan Type, Carrier, and the Blacklist or Whitelist associated with the user's policy suite are also displayed. All fields but those in the Blacklist/Whitelist display can be edited.

The screenshot shows the 'Configuration' tab for a device named 'iPhone 4S'. The left sidebar contains a navigation menu with 'Administration' selected. The main content area is divided into several sections:

- Policy Enforcement Type:** Radio buttons for 'Standard' and 'Schedule-Based' (selected).
- Ownership:** Dropdown menu set to 'Personal'.
- Policy Schedule:** Dropdown menu set to 'Select One...'. Below it, a checkbox for 'Auto (Organization Default)' is unchecked.
- Policy Suite during Schedule:** Dropdown menu set to 'Policy A' with a checkmark icon.
- Plan Type:** Dropdown menu set to 'Unknown'.
- Policy Suite outside Schedule:** Dropdown menu set to 'Policy B' with a checkmark icon.
- Carrier:** Dropdown menu set to 'None'.
- Device Connection Schedule:** Dropdown menu set to 'default' with a checkmark icon.
- Liability:** Dropdown menu set to 'Corporate' with a checkmark icon.

A modal window titled 'Restricted Apps: Policy B' is open, showing two sections:

- Blacklists:** A 'Default' row with a 'Permissions' column containing a green 'YES' button.
- Whitelists:** A 'Default' row with a 'Permissions' column containing a red 'NO' button.

## Device Administration: Security

[\(return to Device Administration menu\)](#)

The **Security** tab provides the remote security commands available for the user's device platform. Not all remote security commands are supported on every device type. The functionality of the action might also vary slightly, based on what the device platform supports or even device model. See the table below for specific device functionality.

The screenshot shows the 'Security' tab for user 'jwitmer'. The left sidebar contains a navigation menu with categories like 'User Information', 'Devices (4)', 'Administration', and 'Corporate Resources'. The main content area has tabs for 'DEVICE INFORMATION', 'CONFIGURATION', 'SECURITY', 'LOCATION', 'PHONE CALLS', 'TEXTS', 'LOGS', and 'FILE LIST'. Under the 'SECURITY' tab, there are four security commands listed:

Command	Description
Send Welcome Letter	Re-send the welcome letter to the user.
Clear Device Enrollment	Clears the enrollment data of a device and allows the user to enroll another device.
Disable Device	Disables or enables device connection with the ZENworks Mobile Management server. Enabled on 01/10/2013 9:56 AM (-05:00 GMT)
Wipe Storage Card	Remotely wipes all data from the device's storage card.

### How Security Commands are Issued

**Full Wipe** - The Full Wipe command is issued via ActiveSync. It is issued immediately when the user device is configured in a Direct Push mode. When the user's device is in a scheduled push mode, the device receives the command during the next scheduled device connection session. Apple MDM functionality makes it possible to apply the *Full Wipe* command immediately to iOS devices.

**Selective Wipe, Wipe Storage Card, and Lock Device** - These commands are issued via *ZENworks Mobile Management*. They are issued immediately when the *ZENworks Mobile Management Device Connection Schedule* has Direct Push enabled. When the *ZENworks Mobile Management Device Connection Schedule* has Direct Push disabled, the device gets the command during the next scheduled device connection session. Apple MDM functionality makes it possible to apply *Selective Wipe* and *Lock Device* immediately to iOS devices; however, the device is capable of postponing the action.

### Security Action Confirmation Emails

The administrator issuing the security command has the option to send a confirmation email to the user.

A dialog box titled 'Confirm Security Action' with the question 'Disable this device?'. Below the question is a checked checkbox labeled 'Notify the user by email'. At the bottom are two buttons: 'Yes' and 'No'.

## Remote Security Commands: Functionality by Device

The table below documents which device types support the security commands and any variation in functionality across device platforms.

<b>Anrd</b>	Android devices	<b>S60</b>	Symbian S60 3 <sup>rd</sup> edition devices
<b>TD/A</b>	Android devices with TouchDown	<b>WM</b>	Windows Mobile 6.1/6.5 devices
<b>NS/BB</b>	GO!NotifySync for BlackBerry	<b>wOS</b>	webOS devices
<b>iOS</b>	iOS multitasking devices	<b>WP</b>	Windows Phone devices
<b>TD/iOS</b>	iOS multitasking devices with TouchDown	<b>BB10</b>	BlackBerry 10 devices

Action	Description	Devices that Support
Full Wipe	<p>Administrators can issue a Full Wipe command. Once the wipe is completed, the device is removed from the dashboard User Grid. Functionality varies by device.</p> <p><i>Note: See <a href="#">Appendix A</a> for information on recovering user information for devices removed from the grid.</i></p> <p><i>Android w/ native ActiveSync account (requires OS v2.2 or greater):</i> The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Does not erase the SD card.</p> <p><i>Android w/TouchDown (requires OS v2.2 or greater):</i> The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Does not erase the SD card.</p> <p><i>Android w/TouchDown using OS v2.0 or 2.1:</i> Full Wipe not available – use the <i>Selective Wipe</i> option to wipe the data associated with TouchDown.</p> <p><i>BlackBerry:</i> Requires the <i>GO!NotifySync for BlackBerry</i> application. Removes all mail and PIM data associated with the <i>GO!NotifySync</i> application and removes the <i>GO!NotifySync</i> account. Locks the device if <i>Require Password</i> is enabled. Erases <i>GO!NotifySync</i> data from the SD card.</p> <p><i>iOS:</i> The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. <i>Full Wipe</i> is applied immediately.</p> <p>iOS 7.0.3+ devices enrolled in the Volume Purchase Program : VPP licenses are reclaimed and the user is retired from the program when it is the last iOS 7.0.3+ device associated with the user.</p> <p><i>Symbian:</i> The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Some models (N95 and 6120c) wipe only <i>Mail for Exchange</i> data. Erases the SD card.</p> <p><i>WM:</i> The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Erases the SD card only on Professional devices.</p> <p><i>webOS and WP:</i> The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased.</p>	<p><b>ZENworks Mobile Management app:</b> Anrd, NS/BB, iOS, TD/iOS, TD/A, WM, S60</p> <p><b>ActiveSync only:</b> BB10, wOS, WP</p>
Selective Wipe	<p>Un-enrolls the device. Un-enrollment selectively wipes the device, removing mail/PIM associated with the mail application; clears the ZENworks Mobile Management account; and deletes the device from the grid.</p> <p>Android (native): Devices with native mail app only wipe the ZENworks Mobile Management account. Mail/PIM is not wiped.</p> <p>iOS: Additionally removes managed iOS profiles, thus removing corporate resources and managed apps designated to be removed when the APN</p>	<p><b>ZENworks Mobile Management app:</b> Anrd, NS/BB, iOS, TD/iOS, TD/A, S60, WM</p> <p><b>ActiveSync only:</b> BB10, wOS, WP</p>

	<p>profile is removed. (Manually created mail profiles and user-installed apps are not removed.)</p> <p>iOS 7.0.3+ devices enrolled in the Volume Purchase Program : VPP licenses are reclaimed and the user is retired from the program when it is the last iOS 7.0.3+ device associated with the user.</p> <p>Devices without ZENworks Mobile Management app: The only action performed is to remove device from the <i>ZENworks Mobile Management</i> server and dashboard grid. Mail/PIM is not wiped.</p>	
Remove User	<p>Stops managing all devices associated with the user and subsequently removes the user from the <i>ZENworks Mobile Management</i> server and dashboard grid.</p> <p>iOS 7.0.3+ devices enrolled in the Volume Purchase Program : VPP licenses are reclaimed and the user is retired from the program.</p>	<p><b>ZENworks Mobile Management app:</b> Anrd, NS/BB, iOS, TD/iOS, TD/A, WM, S60</p> <p><b>ActiveSync only:</b> BB10, wOS, WP7</p>
Wipe Storage Card	Remotely wipes all data from the device's storage card.	<p><b>ZENworks Mobile Management app:</b> Anrd, NS/BB, TD/A, WM</p>
Lock Device	<p>Remotely locks the device, requiring a password to be entered before the device can be used.</p> <p><i>Android or Android w/TouchDown:</i> Requires OS v2.2 or greater.</p> <p><i>iOS</i> allows for <i>Lock Device</i> to be applied immediately to iOS devices.</p>	<p><b>ZENworks Mobile Management app:</b> Anrd, NS/BB, TD/A, iOS, TD/iOS, WM</p>
Disable / Enable Device	Device is unmanaged while disabled and thus blocked from all communication with the server. It does not occupy a license seat in this state.	<p><b>ZENworks Mobile Management app:</b> Anrd, NS/BB, iOS, TD/iOS, TD/A, WM, S60</p> <p><b>ActiveSync only:</b> BB10, wOS, WP</p>
Suspend/Resume Device	Device is managed (it can be wiped and continues to send statistics) while suspended, but blocked from corporate resources. User cannot access the application's Config, Managed Apps, and File Share options and must enter a password to gain full functionality when suspension is lifted.	<p><b>ZENworks Mobile Management app:</b> Anrd, NS/BB, iOS, TD/iOS, TD/A, WM, S60</p> <p><b>ActiveSync only:</b> BB10, wOS, WP7</p>
Show Recovery Password	If a device has the capability to issue a request for a temporary recovery password, this is where you can retrieve the temporary unlock password that has been generated. A user can also view it from the <i>ZENworks Mobile Management</i> User Self-Administration portal. See <i>Enabling Password Recovery*</i> below.	<p><b>ZENworks Mobile Management app:</b> NS/BB, TD/A, TD/iOS</p>
Clear Passcode	iOS device passcode is cleared. If a passcode is required by the user's policy, the user is prompted to enter a new passcode.	<p><b>ZENworks Mobile Management app:</b> iOS, TD/iOS</p>
Trigger APN	Immediately sends an APN to an iOS device causing it to check the server and retrieve any pending commands. This can be used to remedy a situation in which Apple Push Notifications are not synchronizing. A list of pending iOS MDM device commands accompanies this option. Verify that the device is unlocked before issuing this command.	<p><b>ZENworks Mobile Management app:</b> iOS, TD/iOS</p>
Trigger GCM	Immediately sends a notification to an Android device causing it to check the server and retrieve any pending commands. This can be used to remedy a situation in which GCM notifications are not synchronizing, allowing the administrator to get the latest stats and location for the device.	<p><b>ZENworks Mobile Management app:</b> Anrd, TD/A</p>

## Enabling Password Recovery

*Password Recovery* must be enabled on the *ZENworks Mobile Management* server to function. By default, this feature is enabled in the policy suite. The option can only be enabled if *Require Password* is enabled. To verify that both *Require Password* and *Enable Recovery Password* are enabled:

1. Select **Organization > Policy Suites** > (select a policy) > **Security Settings**.
2. Select **Yes** for the **Enable password recovery** option.

When enabled, users with devices that support the feature can generate a temporary recovery password if they forget the unlock password. The recovery password can be viewed by the user via the *ZENworks Mobile Management* Self-Administration Portal. An administrator can also view the recovery password from the *ZENworks Mobile Management* dashboard.

### Viewing the Recovered Password in Outlook Web Access (OWA)

If *Enable Recovery Password* is also turned on in Exchange, users can view the recovery password through OWA in addition to the *ZENworks Mobile Management* dashboard or Self-Administration Portal.

Password Recovery is supported with Exchange 2007 or 2010. It requires ActiveSync protocol 12.0 and 12.1.

To enable it in Exchange, from the *Exchange Management Console*, select the **Client Access** node under **Organization Configuration** in the navigation tree. Right-click the policy and choose the **Properties** tab. Select the **Enable Password Recovery** option.

## Device Administration: Location

[\(return to Device Administration menu\)](#)

Select the **Location** tab to view the location of the device reported by the GPS or triangulation on the device. Information is displayed using Google Maps. Select the date and up to ten times that you want to view.

Map viewing options include:

Choosing the *Map Type* – Roadmap, Satellite, Terrain, or Hybrid

Adjusting the *Zoom Level*

The screenshot displays the 'LOCATION' tab in the Device Administration interface. At the top, there is a navigation bar with tabs for 'DEVICE INFORMATION', 'CONFIGURATION', 'SECURITY', 'LOCATION', 'PHONE CALLS', 'TEXTS', 'LOGS', and 'FILE LIST'. Below the navigation bar, there is a section titled 'Select up to 10 Times to Map' which includes a calendar for January 2013 and a table of location data. The table has four columns: 'Server Local Time', 'Device Local Time', 'Latitude', and 'Longitude'. Three rows of data are visible, all showing a time of 5:23 PM, 5:18 PM, and 5:13 PM respectively, with coordinates 41.024386 and -80.711078. To the right of the table is an 'Export Format' dropdown menu. Below the table, there is a 'Map Type' dropdown menu set to 'Roadmap' and a 'Zoom Level' slider. The main part of the screenshot is a Google Map showing the location of the device. The map is centered on a residential area with several streets labeled, including Boardman Canfield Rd, Lockwood Blvd, and Min Creek Blvd. Three blue location pins are visible on the map, numbered 1, 2, and 3, corresponding to the data in the table. The map also shows Mill Creek Park and various other streets like Wildwood Dr, Ewing Rd, Brookfield Ave, and West Blvd.

Server Local Time	Device Local Time	Latitude	Longitude
5:23 PM (-05:00 GMT)	5:23 PM (-05:00 GMT)	41.024386	-80.711078
5:18 PM (-05:00 GMT)	5:18 PM (-05:00 GMT)	41.024386	-80.711078
5:13 PM (-05:00 GMT)	5:13 PM (-05:00 GMT)	41.024386	-80.711078

On the action bar, click the **Get Most Recent Data** button to refresh the location data. Click the **Locate on Google Maps** button to view a Google Map and the location address.



## Device Administration: Phone Calls and Texts

[\(return to Device Administration menu\)](#)


Select **Phone Calls** tab to view phone call logs synchronized from the device. Select the day you want to view.

You can search the phone call log by date, To/From phone number, call origination, call status, roaming status, or call duration. The search results can be exported to a CSV or XLS file.

DEVICE INFORMATION | CONFIGURATION | SECURITY | LOCATION | **PHONE CALLS** | TEXTS | LOGS | FILE LIST

From: 02/12/2013 to 02/12/2013

Phone Number:  Origin:  Status:  Roaming:  Duration:

**Search Results** 

Device Local Time	Origin	Phone Number	Status	Roaming	Duration

**Summary of Search Results**

<b>Call Count</b>	<b>Average Call Duration</b>	<b>Calls While Roaming</b>
Total: 0	Overall: --	Total: 0
Incoming: 0	Incoming: --	Incoming: 0
Outgoing: 0	Outgoing: --	Outgoing: 0
Unknown: 0	Unknown: --	Unknown: 0

Select **Texts** tab to view text message logs synchronized from the device. Select the day you want to view. Double-click a text message record to view the body of text in the message with any attachments that were sent or received.

You can search the text message log by date, To/From phone number, message origination, message type, message status, or roaming status. The search results can be exported to a CSV or XLS file.

DEVICE INFORMATION | CONFIGURATION | SECURITY | LOCATION | PHONE CALLS | **TEXTS** | LOGS | FILE LIST

From: 02/12/2013 to 02/12/2013

Phone Number:  Origin:  Type:  Status:  Roaming:

**Search Results**

Device Local Time	Origin	Type	Phone Number	Status	Roaming	Subject	Message

**Summary of Search Results**

<b>Text Count</b>	<b>Text Type Count</b>	<b>Texts While Roaming</b>
Total: 0	SMS: 0	Total: 0
Incoming: 0	MMS: 0	Incoming: 0
Outgoing: 0	PIN: 0	Outgoing: 0
Unknown: 0	Unknown: 0	Unknown: 0

## Device Administration: Viewing Logs

[\(return to Device Administration menu\)](#)

User 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.

Select the **Logs** tab to view the logs associated with a user's device. Choose one of the logs from the *Log Type* drop-down list.

- **ActiveSync Log** – View events logged during connections between the *ZENworks Mobile Management* server and the ActiveSync server and between the device's ActiveSync client and the *ZENworks Mobile Management* server.
- **GCM Log** –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** – 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** - View events logged during connections between the device's *ZENworks Mobile Management* app and the *ZENworks Mobile Management* server.
- **Configuration/Feedback Log** – View results of a request to see managed iOS application configuration and feedback information.
- **Data Usage Log** – 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** – to request and view a log from a device running the *ZENworks Mobile Management* application.
- **Error Chain Log** – to view detailed messages for errors logged in the *iOS MDM Sync Log*. (iOS device specific)

Use the **Reset** button on the *Logs* page to reset the date/time range to the last hour and the *Log Type* to ActiveSync Log.

## Configuration/Feedback Log

The Configuration/Feedback Log shows the results of a request to see managed iOS application configuration and feedback information. Request the information by clicking the **Request Config/Feedback** button on the *User Profile Managed Apps* grid.

The log displays:

- App Name – Name of the application
- Time Requested – Date and time the request for information was made
- Requester – Username of the person who made the request
- Received – Whether the configuration/feedback
- Time Received – Date and time information was received

Select **Configuration/Feedback Log** from the drop-down list.

Set a date/time range, then click the *Search* button.

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

The screenshot displays the Configuration/Feedback Log interface. At the top, there is a navigation bar with tabs: DEVICE INFORMATION, CONFIGURATION, SECURITY, LOCATION, PHONE CALLS, TEXTS, LOGS (selected), and FILE LIST. Below the navigation bar, there are search filters for 'From:' and 'To:' with date and time pickers. The 'From:' filter is set to 09/04/2013 at 9:43 AM, and the 'To:' filter is set to 09/04/2013 at 10:43 AM. A 'Log Type' dropdown menu is set to 'Configuration/Feedback Log'. There are 'Reset' and 'Search' buttons. Below the filters, the title 'Configuration/Feedback Log Search Results' is displayed with a refresh icon. The main area contains a table with the following columns: App Name, Time Requested, Requester, Received, and Time Received. The table is currently empty. At the bottom of the interface, there are buttons for 'Download Selected Log', 'Export Format', and 'Export Grid'.

Sample Configuration/Feedback Log Grid

## Synchronization Logs

Synchronization logs give administrators the ability to view events associated with a particular device that have been logged during connections between servers and between the device and 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 device's 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.

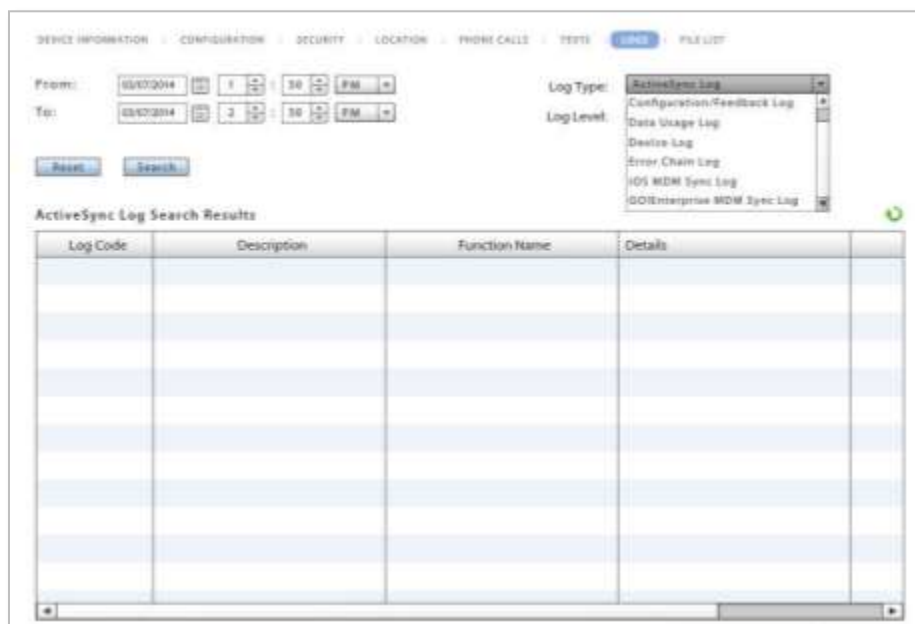
The logs display:

- Log code – Code number associated with the logged event
- Description – Description of the log event
- 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** from the drop-down list.

Set the Log Level (Normal or Verbose) and a date/time range, then click the *Search* button.

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.



The screenshot shows the ZENworks Mobile Management interface. At the top, there are navigation tabs: DEVICE INFORMATION, CONFIGURATION, SECURITY, LOCATION, PHONE CALLS, TESTS, and LOGS. The LOGS tab is selected. Below the tabs, there are search filters for From: (05/07/2014), To: (05/07/2014), Log Type: (ActiveSync Log), and Log Level: (Normal). There are buttons for Reset and Search. Below the search filters, the title "ActiveSync Log Search Results" is displayed. The main area contains a table with the following columns: Log Code, Description, Function Name, and Details. The table is currently empty.

Log Code	Description	Function Name	Details
----------	-------------	---------------	---------

Sample Synchronization Log Grid

## 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:

- Traffic Type – ActiveSync, iOS MDM Sync, or *ZENworks* sync
- Direction – Incoming or Outgoing
- Size (Bytes) – Size of the data transferred
- Timestamp – Date and time of the data transfer

Select **Data Usage Log** from the drop-down list.

Set a date/time range, then click the *Search* button.

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.

DEVICE INFORMATION | CONFIGURATION | SECURITY | LOCATION | PHONE CALLS | TEXTS | **LOGS** | FILE LIST

From: 01/22/2013 9 : 10 AM  
To: 01/22/2013 10 : 10 AM  
Log Type: Data Usage Log

Reset Search

Data Usage Log Search Results

Traffic Type	Direction	Size (Bytes)	Timestamp

## Device Logs

The device logging option can be used to request a log from any device running the *ZENworks Mobile Management* application or a BlackBerry device running the *GO!NotifySync* application. Administrators should instruct users to turn on the logging feature of the device, so they can obtain the log.

Device Type	Device Requirements / Behavior
Android	The device sends only the logcat log to the dashboard. <i>ZENworks</i> logging must be enabled on the device ( <i>Log Settings</i> ). The <i>ZENworks</i> log is written to the SD card.
BlackBerry (with <i>GO!NotifySync</i> )	BlackBerry devices must have logging enabled on the device ( <i>Log Settings</i> ) and must have an SD card.
iOS	No special requirements. Logging is always enabled on iOS devices.
Symbian S60, 3	<i>ZENworks</i> Logging must be enabled on the device ( <i>Log Settings</i> ).
Windows Mobile 6	<i>ZENworks</i> Logging must be enabled on the device ( <i>Log Settings</i> ).

Select **Device Log** from the drop-down list.

Set a date/time range.

Click the **Request** button. The screen displays a *Log Request Pending* message until the device sends the log the next time it connects to the *ZENworks Mobile Management* server.

The dashboard grid does not display log records, but gives information on whether a log has been received. The grid displays:

- Time Requested and Requester
- Time Received – date / time a response was received
- Received – whether or not log has been received
- Error – error message if log could not be obtained

The screenshot shows the 'LOGS' tab in the ZENworks Mobile Management interface. At the top, there are navigation tabs: DEVICE INFORMATION, CONFIGURATION, SECURITY, LOCATION, PHONE CALLS, TEXTS, LOGS (selected), and FILE LIST. Below the tabs, there are search filters for 'From' and 'To' dates and times, a 'Log Type' dropdown menu set to 'Device Log', and a 'Request Log' button. There are also 'Reset' and 'Search' buttons. Below the search filters, the 'Device Log Search Results' section is visible, featuring a table with the following columns: Time Requested, Requester, Received, Time Received, and Error. The table currently contains no data rows.

*Device Log Grid*

When the log has been received, select the 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.

Edit the date and time filters in order to access logs you previously requested. Click **Search**. This filters the timestamp of the logs, not the records in the log. When you edit the date/time filter, the system maintains the changes as preferred settings for all user level log views until you change the settings or log out of the dashboard.

## 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:

- Error Code – Code number associated with the error
- Error Domain – Contains internal codes used by Apple useful for diagnostics (might change between Apple releases)
- Localized Description – Description of codes
- Time stamp – Date and time the error occurred

Select *Error Chain Log* from the drop-down list.

Set a date/time range, then click the *Search* button.

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.

DEVICE INFORMATION | CONFIGURATION | SECURITY | LOCATION | PHONE CALLS | TEXTS | **LOGS** | FILE LIST

From: 01/22/2013 9 : 10 AM  
To: 01/22/2013 10 : 10 AM  
Log Type: Error Chain Log

Reset Search

Error Chain Log Search Results

Error Code	Error Domain	Localized Description	Timestamp

*Error Chain Log Grid*



## Device Administration: File List

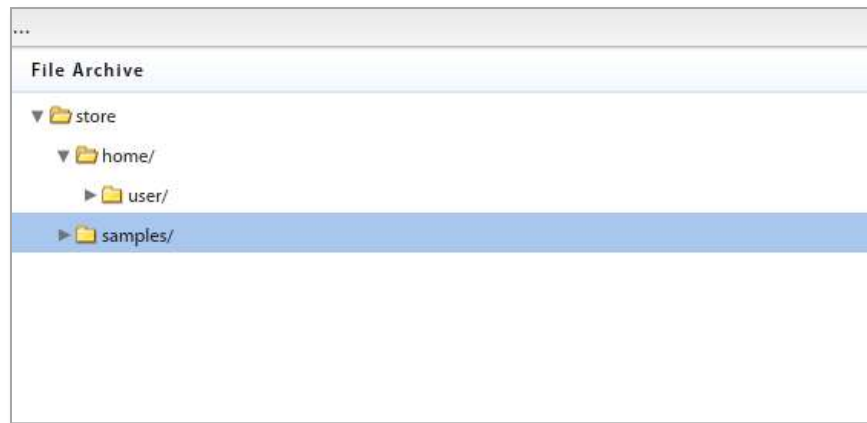
[\(return to Device Administration menu\)](#)

Select the **Archive device file list** tab to view the file list sent up from the device. The *Archive files on device* policy rule must be enabled in the policy suite to which the user belongs. When the rule is enabled, the device periodically sends a list of all folders and files stored on the device and the SD card, to the server. Administrators can view the list here.

The *Archive device file list on device* policy rule is located in the *Audit Tracking* category of each policy suite. You can enable file archiving here and specify how often devices send the file list.



The device file directory is displayed in the User Profile.



## Corporate Resource Assignments

Corporate Resources are a collection of servers, networks, and other resources that you can make available to users. From an iOS user's profile you can Manage apps, associate a device with servers or networks in the enterprise system, and configure user account settings to push out to the device. You can also push out resources such as Provisioning Profiles, Subscribed Calendars, Web Clips, and an Access Point Name.

For Android devices, you can manage apps, and assign a Wi-Fi network or VPN connection. Managed Apps, Wi-Fi and VPN are the only supported resources for Android devices at this time.

**Note:** Configuration of these resources is done from the *Organization* view. See the [Organization Administration Guide](#). Reference the sections, *Corporate Resource Management* and *Application Management*.

Removal of a resource that has been assigned via LDAP group or folder is temporary, since LDAP periodic updates will keep reassigning the resource.

**Access Point Names.** Assign a new Access Point Name to a user only when necessary. The Access Point Name (APN) identifies the external network a phone accesses for data. When you assign a new APN, it you must have the correct settings for the carrier and account provisioning. Incorrect settings can result in a loss of functionality or additional charges. See the [Organization Administration Guide: Resource Configuration](#).

**CalDAV or CardDAV Servers.** Associate the user with a CalDAV/CardDAV server and configure contact account settings (username, password and principal address) to push out to the user's device.

**Exchange Servers\*.** Associate the user with an Exchange server or a server utilizing the Exchange ActiveSync protocol and configure ActiveSync account settings to push out to the user's device.

**LDAP Servers.** Associate the user with an LDAP server and configure LDAP settings so the user can access corporate directory information via the device.

**Mail Servers\*.** Associate the user with a mail server and configure email account settings to push out to the user's device.

**Managed Apps.** View a list of installed and/or managed apps on Android, BlackBerry, and iOS devices. Assign an app to an Android or iOS device from lists of applications available as determined by the *Managed App Permissions* on the policy suite with which a user is associated.

**Provisioning Profiles.** Associate an iOS device user with a provisioning profile in order to enable him/her to install an in-house iOS app.

**SCEP Server.** Associate the user with a SCEP server in order to issue digital certificates to devices using an automatic enrollment technique. This provides a method of delivering encrypted configuration profiles to iOS devices.

**Subscribed Calendars.** Associate the user with Subscribed Calendars to push out to the user's device. When the device synchronizes, the Subscribed Calendar account is automatically set up on the device.

**VPN.** Associate an iOS or Android user with a VPN Network and define the network credentials to push out to the user's device.

**Web Clips.** Assign Web Clips to be pushed out to the user's device. When the device synchronizes, the web clip is automatically added to the user's device Home screen.

**Wi-Fi Networks.** Associate an iOS or Android user with a Wi-Fi Network and define the wireless network credentials to push out to the user's device.

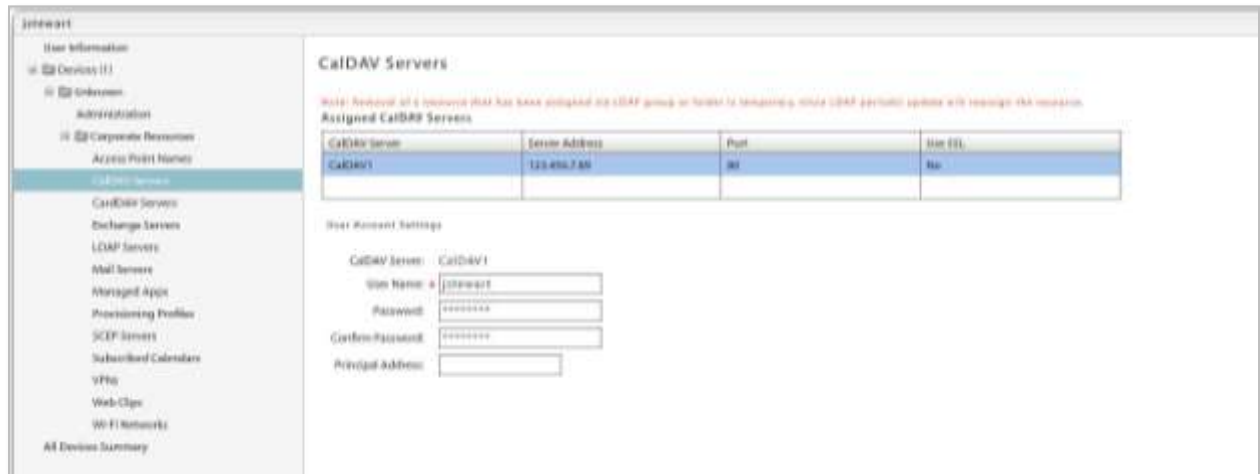
\***Mail Servers** and **Assign Exchange Servers** have two options that can be enabled/disabled to govern how the mail account can be used by an iOS 5+ user. If they are set when the resource is created, however, they cannot be changed at the user level.

- **Allow Move (iOS 5+)** – When disabled, this option prevents an iOS 5+ device user from moving messages from corporate mail account folders to folders associated with other mailbox accounts. For example, a user could not move a message from the corporate mail account Inbox to a folder associated with his or her personal mail account.
- **Use Only in Mail (iOS+)** – When enabled, this option prevents an iOS 5+ device user from setting the corporate mail account as the default. The corporate mail account can then only be used in conjunction with the device's *Mail* application.

This prevents messages created outside of the device's native *Mail* application from being sent from the corporate account. For example, if the user sends a photo from the device *Photo* application, it is not be sent from the corporate mail account; nor can the user send an attached contact file from the device's *Contacts* application using the corporate mail account.

## Corporate Resources: Servers, Networks, etc.

1. To assign resources, expand the **Corporate Resources** option on the left panel of the *User Profile*. Click the resource you want to assign.
2. Select a resource from the grid and enter any required user information or credentials.

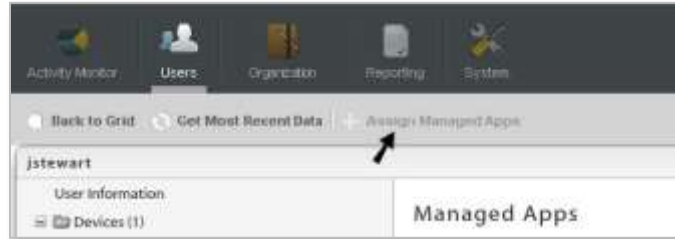


Sample iOS Resource Assignment

## Corporate Resources: Managed Apps

### Assigning Managed Apps

1. To make an app assignment, expand the **Corporate Resources** option on the left panel of the *User Profile*. Select **Managed Apps**.
2. Use the **Assign Managed Apps** button to make an app assignment at the user level.



3. A pop-up grid appears listing all apps available for the user's device type. Check boxes for apps that have already been assigned to the user via a Policy Suite, LDAP Group/Folder, or Local Group will be grayed out and cannot be edited. An administrator can check any box that is not grayed out to make a new app assignment for the user. Subsequently, the administrator can remove any assignment made at the user level (check boxes not grayed out).
4. Click **Update Resources** when you have finished making a selection from the grid.

A screenshot of the 'Assign Managed Apps' dialog box. It contains a table with three columns: 'Name', 'Recommend', and 'Force'. The 'Recommend' and 'Force' columns have checkboxes. The 'Recommend' column checkboxes are checked for 'World Clock' and 'UPS Mobile', and unchecked for 'Skype'. The 'Force' column checkboxes are checked for 'World Clock' and 'UPS Mobile', and unchecked for 'Skype'. An 'Update Resources' button is at the bottom right.

Name	<input type="checkbox"/> Recommend	<input type="checkbox"/> Force
Skype	<input type="checkbox"/>	<input type="checkbox"/>
World Clock	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
UPS Mobile	<input checked="" type="checkbox"/>	<input type="checkbox"/>

*Assign apps that have not already been assigned*

A screenshot of the 'Assign Managed Apps' dialog box. It contains a table with three columns: 'Name', 'Recommend', and 'Force'. The 'Recommend' and 'Force' columns have checkboxes. The 'Recommend' column checkboxes are checked for 'Skype', 'World Clock', and 'UPS Mobile'. The 'Force' column checkboxes are checked for 'World Clock' and 'UPS Mobile', and unchecked for 'Skype'. An 'Update Resources' button is at the bottom right.

Name	<input checked="" type="checkbox"/> Recommend	<input type="checkbox"/> Force
Skype	<input checked="" type="checkbox"/>	<input type="checkbox"/>
World Clock	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
UPS Mobile	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

*Remove only the apps assigned at the user level*

Assignments made at the user level are not affected by changes in app assignments associated with Policy Suites, LDAP Groups/Folders, or Local Groups.

## The App Grids: Policies that Control Application Reporting and Management

Expand the **Corporate Resources** option on the left panel of the *User Profile* and select **Managed Apps** to view the lists of applications on the device. For Android, BlackBerry, and iOS devices, you can view *Managed Apps* and/or *Installed Apps*.

Certain policies must be enabled in order for app information to be reported in the grids.

### ANDROID POLICIES

A policy rule must be enabled in the policy suite to which the user belongs in order for an Android device to send application lists.

In the **Audit Tracking > General** category of each policy suite, enable one of the following policy rules:

- **Record Installed Applications** – to require devices to send data usage statistics for all apps on the device.
- **Record Managed Applications** – to require devices to send app information for only managed apps. Turning this off will disable *Managed App* functionality for Android devices.

Audit Tracking		CORPORATE	INDIVIDUAL
▼ General			
Archive device file list		<input type="checkbox"/> NO	<input type="checkbox"/> NO
Frequency for archiving files (in days)	7	7	7
Record phone log		<input type="checkbox"/> NO	<input type="checkbox"/> NO
Record text message log		<input type="checkbox"/> NO	<input type="checkbox"/> NO
Record installed applications		<input checked="" type="checkbox"/> YES	<input checked="" type="checkbox"/> YES
Record managed applications		<input type="checkbox"/> NO	<input type="checkbox"/> NO

### IOS POLICIES

Two policy rules must be enabled in the policy suite to which the user belongs in order for an iOS device to send application lists and for the administrator to be able to manage the apps from the server.

The **Record Installed Applications** and **Allow app management** policy rules are located in the **iOS Devices: Applications** category of each policy suite. Changes to these access rights will require iOS device users to reload a new APN profile.

Applications		CORPORATE	INDIVIDUAL
Allow app management		<input checked="" type="checkbox"/> YES	<input checked="" type="checkbox"/> YES
Record installed applications		<input checked="" type="checkbox"/> YES	<input checked="" type="checkbox"/> YES

## The App Grids: Managed Apps

The **Managed Apps** grid lists all applications available to an Android or iOS user as determined by the *Managed App Permissions* on the policy suite with which the user is associated.

When administrators add applications to the Android or iOS app permissions list via the policy suite, a user can access the list on the device and conveniently installed apps from the list. If the policy suite also has the *Allow app management* policy enabled, an administrator can install, reinstall, or uninstall an app on the user's device, using the option buttons below the *Managed Apps* grid. Administrators can also remove, from an iOS device, an invalid Redemption Code for a Volume Purchase Program (VPP) app.

For Android devices, any app that has been enabled through the Managed App Permissions of the users' policy suite can be managed.

For iOS devices, a managed app is one that has been installed on the device through MDM by either the user, an administrator, or by a forced push of the application. Applications that are not installed through MDM or those already existing on the device before the app was made available through MDM appear on the *Installed Apps* list and cannot be managed.

### IOS MANAGED APPS GRID

Managed Apps									
App Name	Version	Status	Rejection Reason	Remove With MDM	Prevent Backup	Redemption Code	Has Configuration	Has Feedback	Tin
ConfigApp	1	Not Installed via M					No	No	08

[Install App](#)
[Reinstall App](#)
[Uninstall App](#)
[Remove Redemption Code](#)
[Request Config/Feedback](#)
[View Config/Feedback](#)
[Export Format](#)
[Export Grid](#)

Information in the iOS Managed Apps Grid	
<b>Status</b>	<p>The most common status messages include:</p> <ul style="list-style-type: none"> <li>• <i>Managed</i> – Indicates that the app is installed on the device</li> <li>• <i>Not Installed via MDM</i> – Indicates that the app is available through <i>ZENworks Mobile Management</i>, but is not required and has not been installed by <i>ZENworks</i>.</li> <li>• <i>Managed, but Uninstalled</i> – Indicates an app that is not installed; possibly because it was removed by the user or is not required.</li> </ul> <p>Other status messages give additional information about apps on the device.</p>
<b>Rejection Reason</b>	If the app is not installed, look here to see if installation of the app was attempted and why it was rejected.
<b>Remove with MDM</b>	Whether this app is removed, along with its data, if the MDM profile is removed.
<b>Prevent Backup</b>	Whether the user is prevented from backing up this app via iTunes.
<b>Redemption Code</b>	The redemption code associated with a Volume Purchase Program (VPP) app.
<b>Has Configuration</b>	Whether the app has a server-provided configuration.

<b>Has Feedback</b>	Whether the configured app has feedback for the server.
<b>Timestamp</b>	Last update of the app's status.
<b>Install App</b> button	Issues a command that prompts the user to install the app.
<b>Reinstall App</b> button	Issues a command that prompts the user to reinstall the app.
<b>Uninstall App</b> button	Issues a command that prompts the user to uninstall the app. The <i>Force Push</i> option should be disabled first, so that the app does not get pushed back to the device after the user uninstalls it.
<b>Remove Redemption Code</b> button	Remove an unused redemption code so that it can be reused. A redemption code is sent with volume purchase apps, however, if it is not, it can be reclaimed in this way.
<b>Request Config/Feedback</b> button	If an app in the Managed Apps list has a server-provided configuration or feedback, click this button to request information about whether the app received the configuration file.
<b>View Config/Feedback</b> button	Links to the <b>Logs</b> tab so that you can view the information the app received via the configuration file and any available feedback information.

## ANDROID MANAGED APPS GRID

App Name	Version	Status	Remove With MDM	Required	Timestamp	Last Attempted Install	Last Attempted Uninstall
7x7	1.0.1	Attempting Install	No	No	03/26/2013 2:42 PM (-04:00 GMT)	03/26/2013 2:42 PM (-04:00 GMT)	
Kobo	4.2	Not Installed	No	No	03/26/2013 3:02 PM (-04:00 GMT)	03/26/2013 2:42 PM (-04:00 GMT)	03/26/2013 3:02 PM (-04:00 GMT)

Information in the Android Managed Apps Grid	
<b>Version</b>	Application version number.
<b>Status</b>	Status messages include: <ul style="list-style-type: none"> <li>• <i>Not Installed</i> – Application is not installed</li> <li>• <i>Pending Install</i> – Server has issued a <i>Force Push</i> for the application</li> <li>• <i>Attempting Install</i> – Device has received the <i>Force Push</i> and is in the process of installing the app</li> <li>• <i>Managed</i> – Application is installed and managed</li> <li>• <i>Pending Uninstall</i> – Server has pushed an uninstall command for the app</li> <li>• <i>Attempting Uninstall</i> – Device has received the uninstall command and is in the process of uninstalling the app</li> </ul>
<b>Remove with MDM</b>	Whether this app is removed, along with its data, if the MDM profile is removed.

<b>Required</b>	Whether the application is one that has been Force Pushed to the device.
<b>Timestamp</b>	Date and time of the last update of the app's status.
<b>Last Attempted Install</b>	Date and time of the last attempted installation of the app.
<b>Last Attempted Uninstall</b>	Date and time of the last attempted removal of the app.
<b>Install App</b> button	Issues a command that prompts the user to install the app.
<b>Reinstall App</b> button	Issues a command that prompts the user to reinstall the app.
<b>Uninstall App</b> button	Issues a command that prompts the user to uninstall the app. The <i>Force Push</i> option should be disabled first, so that the app does not get pushed back to the device after the user uninstalls it.



## The App Grids: Installed Apps

The *Installed Apps* grid lists all non-system applications that have been installed on a device.

- An iOS device will only report its applications if the *Record Installed Applications* policy rule is enabled on the policy suite with which the user is associated.
- An Android devices will only report its applications if the *Record Installed Applications* and *Record Managed Applications* policy rules are enabled on the policy suite with which the user is associated.

The *Installed Apps* grid is updated each time the device connects with the server.

### IOS INSTALLED APPS GRID

**Installed Apps**  
The "Record installed applications" policy in "Policy Suites->iOS Devices->Applications" must be enabled to see this information.

App Name	Version	Identifier	Bundle Size	Dynamic Size
Crosswords	1.8.3	com.magmic.NYTCrosswords09	19009536	8192
GOIMDM	3.6.3.4	com.notifylink.mdm2	2461696	77824
ZENworks	2.9.1.5	com.notifylink.zenent	3342336	286720

Data Display:  KB  MB  GB Export Format

### ANDROID INSTALLED APPS GRID

**Installed Apps**  
The "Record installed or managed applications" policies in "Policy Suites->Audit Tracking->General" must be enabled to see this information.

App Name	Version	Installed By	Version Code	Package Name	Data Downloaded (KB)	Data Uploaded (KB)
Boxed	1.9.3	User	24	com.boxed.prod	0	0
eBay	1.0	User	1	com.ebay.mobile	0	0
Eureka Offers	1.0	User	1	com.pinsight.eureka.offers	0	0
GOIMDM	3.6.3.0	User	3630	net.notify.notifymdm	0	0
Jellyflop	1.1.4	User	10104	com.concretesoftware.jellyflop_d	0	0
Lookout Security	4.0-d57a8a1	User	40000	com.lookout	0	0
Messaging+	1.0	User	1	msgplus.jibe.sca	0	0
NASCAR Mobile 2014	1.0	User	1	com.nascar.nascarmobile	0	0
NBA Game Time	1.0	User	1	com.nbadigital.gametimelite	0	0

Data Display:  KB  MB  GB Export Format

## Device Summary

Select **All Devices Summary** from the *User Profile* panel to see a list of the devices the user has enrolled. The columns displayed in the grid can be rearranged and the data can be exported to a .CSV or .XLS file.

UserSAKey	Active	User Name	Email Address	First Name	Last Name	Domain	Liability	Ownership	Last ZENworks Sync
27	Yes	jwitmer	jwitmer@dc03.n	Josh	Witmer		Corporate	Company	01/29/2013 4:25 PM
789	Yes	jwitmer	jwitmer@dc03.n	Josh	Witmer		Corporate	Company	01/29/2013 3:59 PM

# Local Groups

**Local Groups** are groups created on the *ZENworks Mobile Management* server for the purpose of categorizing users. Users with similar roles, functions, hierarchical levels, etc. can be assigned the same policy suite, device connection schedule, and liability through their group membership.

The functionality of Local Groups is similar to that of LDAP Folders/Groups. Organizations that utilize an LDAP server can leverage LDAP information and the LDAP folder and group structure to provision categories of *ZENworks Mobile Management* users. Groups created locally on the *ZENworks Mobile Management* server give similar functionality to organizations that do not use an LDAP server. See the [Organization Configuration Guide](#) for information LDAP Folders/Groups.

A user may belong to multiple groups. The groups can be prioritized to determine the order in which the settings are inherited. See *Prioritizing Groups* below,

# Managing Local Groups

Add or edit local groups from the dashboard's Organization Management view.

Select **Organization > Organization Control > Local Groups**. Use this page to:

- add groups
- assign group membership
- configure a group with Policy Suite, Device Connection Schedule, Liability settings, and Novell Filr profile (if applicable).
- prioritize groups (necessary only when users belong to multiple groups)
- change group membership or a group name
- remove a group

## Local Groups

A user's individual settings are determined first by any direct user assignments, then by any assignments associated with the user's highest prioritized local group, then by any assignments made to the user's highest prioritized LDAP group, and finally by any assignments made to the user's LDAP folder. Organization defaults are applied if none of these have associated assignments.

Select a group to make or edit Policy Suite, Connection Schedule, or Liability assignments. Use the arrows to change group priority. Priorities determine settings when a user belongs to more than one groups.

Priority	Group Name	Policy Suite	Connection Schedule	Liability	Novell Filr
1	Department Heads	Default	Default	Corporate	<Not Assigned>
2	School of Business	<Not Assigned>	<Not Assigned>	<Not Assigned>	<Not Assigned>
3	School of Engineering	<Not Assigned>	<Not Assigned>	<Not Assigned>	<Not Assigned>



Add Group Edit Group Remove Group

Group Name: Department Heads

Policy Enforcement Type: Standard

Policy Suite: \* Default

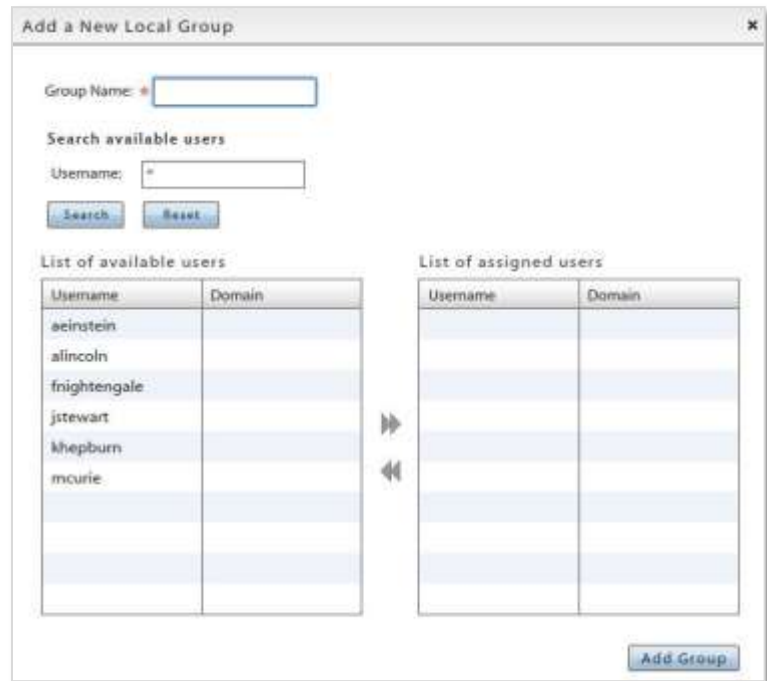
Connection Schedule: Default

Liability:  Unknown  Corporate  Individual

Novell Filr: Select One...

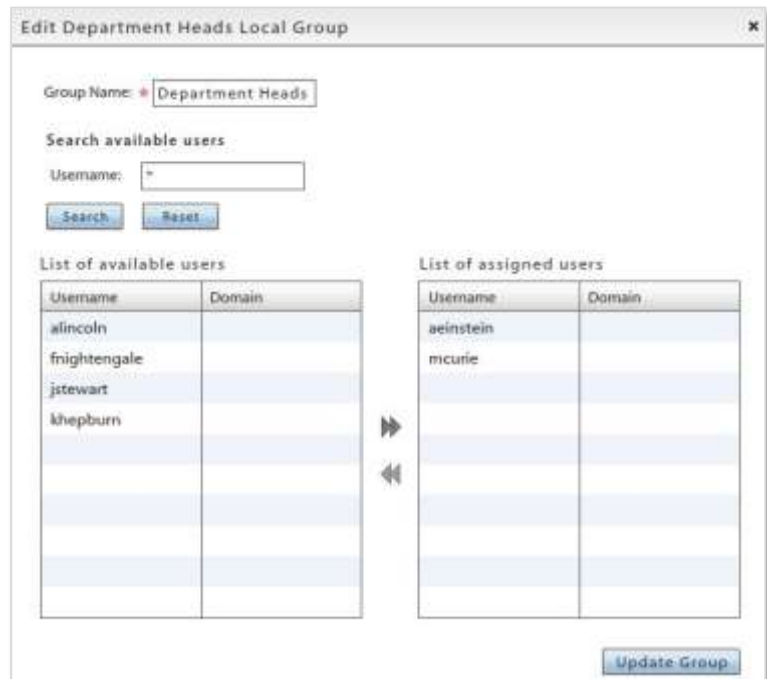
## Add a Group and Assign Users

1. To add a group and assign users to it, click the **Add Group** button.
2. Enter a name for the group.
3. Select user names from the **List of available users** on the left. Click the right arrow to move your selections to the **List of assigned users**.
4. Click the **Add Group** button.



## Edit a Group Name or Change Group Membership

1. To edit the name of a group or change the members of the group, click the **Edit Group** button.
2. Edit the name of the group if necessary or change the group members by using the arrows to move users to/from the available and assigned user columns.
3. Click the **Update Group** button.  
Changes to a user's group association will update the user's policy suite, connection schedule, and liability settings accordingly.



## Prioritizing Groups

A user may belong to multiple groups. The groups can be prioritized to determine the order of inheritance. The group with the highest priority will determine the user's policy suite, device connection schedule, and liability settings.

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

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

**Note:** If a user is a member of an LDAP group as well as a local group, local group assignments will take precedence over LDAP group assignments.

### A Prioritization Example

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

Select a group to make or edit Policy Suite, Connection Schedule, or Liability assignments. Use the arrows to change group priority. Priorities determine settings when a user belongs to more than one groups.

Priority	Group Name	Policy Suite	Connection Schedule	Liability
1	Department Heads	default	default	<Not Assigned>
2	School of Business	<Not Assigned>	<Not Assigned>	<Not Assigned>
3	School of Engineering	<Not Assigned>	<Not Assigned>	<Not Assigned>

Priority

Add Group Edit Group Remove Group

## Configure the Group Settings

1. Select a group from the grid.
2. Below the grid, select the settings for the group: Policy Suite(s), Device Connection Schedule, Liability, and Novell Filr profile\* (if applicable).

You can view the Whitelist/Blacklist permissions associated with a policy suite by clicking the symbol next to the *Policy Suite* field.

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

3. Click **Save Changes**.
4. Use the **Reset All** button if you need to clear all the settings.

Group Name: Group1

Policy Enforcement Type: Standard

Policy Suite: \* Policy A

Connection Schedule: Default

Liability:  Unknown  
 Corporate  
 Individual

Novell Filr: Filr Profile1

Reset All

Standard Policy Enforcement

Group Name: Group1

Policy Enforcement Type: Schedule-Based

Policy Schedule: \* General Staff

Policy Suite During Schedule: \* Policy A

Policy Suite Outside Schedule: \* Policy B

Connection Schedule: Default

Liability:  Unknown  
 Corporate  
 Individual

Novell Filr: Filr Profile1

Reset All

Whitelists/Blacklists: Policy A

	Corporate	Individual
Blacklists		
Default	YES	YES
Whitelists		
Default	NO	NO

Schedule-Based Policy Enforcement

## Remove a Group

1. To remove a group, select a group from the grid and click the **Remove Group** button.
2. At the confirmation prompt, click **Yes**.



# Appendix A: Recovering User Information

The following script provides a way to retrieve user information from the database for users who have been removed from the dashboard grid via a Full Wipe.

```
USE [MDM]
GO

DECLARE @NumberOfDays INT
--*****
-- if need be, change value of @NumberOfDays (currently 30) to differ the number of
-- days in the past to search for records.
--*****
SET @NumberOfDays = 30

SELECT *
FROM Devices WITH (NOLOCK)
JOIN [MDMUsers] WITH (NOLOCK) ON [Devices].[UserSAKey] = [MDMUsers].[UserSAKey]
WHERE [FullWipeLastSent] > GETUTCDATE() - @NumberOfDays
```