

Managing Users, Resources, and Applications

ZENworks® Mobile Management 3.2.x

October 2015

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 © 2012-15 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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

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

Novell Trademarks

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

Third-Party Materials

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

Table of Contents

Accessing the Dashboard	5
Managing Users	7
The User/Device Grid	7
Customizing the User/Device Grid.....	8
Assigning Settings and Resources to Groups/Folders from the Grid	11
The Device Panel.....	13
The Administration Panel.....	15
Exporting Data from the User/Device Grid	16
Adding / Removing / Disabling Users	16
The Apple DEP User/Device Grid.....	17
The Discovered Devices Grid	18
The Device Profile.....	20
User Information	20
Device Administration	26
Corporate Resource Assignments	43
Device Summary.....	51
Local Groups	52
Managing Local Groups	53
Add a Group and Assign Users	54
Edit a Group Name or Change Group Membership	54
Prioritizing Groups	55
Configure the Group Settings	56
Remove a Group.....	57
Application Management	58
Application Categories	59
Creating, Editing, or Removing Categories	59
Associating an Application with a Category.....	59
View Managed Apps by Category	60
Assigning a Category to LDAP Groups/Folders or Local Groups.....	60
Managed Apps	62
Adding and Managing Apps for Android Devices	63
Android Kiosk Mode Apps.....	68
Adding and Managing Apps for iOS Devices.....	70
Adding Managed Apps for BlackBerry Devices	85
Novell Filr	87
Whitelists/Blacklists.....	90
Corporate Resource Management	93
Resource Configurations	95
Assigning Resources to LDAP Groups and Folders.....	101
Assigning Network Resources to Local Groups	102
Simple Certificate Enrollment Protocol (SCEP) Servers.....	104
Tracking Data Usage	107

Define a Data Plan	107
Assigning Devices to a Data Plan.....	110
Assign Devices to a Data Plan.....	110
Remove Devices from a Data Plan.....	112
File Share	113
Group Notifications	116
Send Group Notifications	116
Send Group E-mail	118
Search Group E-mail	119
The Activity Monitor	120
Reporting	127
Using the Reports	128
Sample Reports	129
Appendix A: Recovering User Information	134

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



Novell.
ZENworks Mobile Management

© 2013 Novell, Inc. All Rights Reserved

Login with     

Zone

Continue



Novell.
ZENworks Mobile Management

© 2013 Novell, Inc. All Rights Reserved

Login with     

Organization

Continue

Customizing the User/Device Grid

Customize the user list view by:

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

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)	Device Type	Device Model	Policy Su
Yes	broberts	Corporate	12/15/2010 3:32 PM	Android	Nexus One	NotifyTes
Yes	dbadger	Personal	12/20/2010 4:18 PM	BlackBerry	9630	NotifyTes
Yes	hburkett	Corporate	12/17/2010 11:23 PM	Android	ADR6300	NotifyTes
Yes	iOStest	Personal	11/23/2010 6:13 PM	iPhone	iPhone 4	NotifyTes
Yes	jconrad	Personal	12/18/2010 1:49 AM	iPhone	iPhone 3GS	Engineer
Yes	jecker@2007dc	Corporate	12/07/2010 7:59 PM	iPhone	iPod4,1	NotifyTes

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

Choose the visible columns. Click the *Choose Visible Columns* button in the bottom left corner of the User/Device 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/Device 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.



Available Columns

- | | |
|--|--|
| Activation Date | Last APN Sent (Server Local) |
| Activation Lock Status | Last Name |
| Active | Last ZENworks Sync (Server Local) |
| ActiveSync Authorization Failures (User) | Liability |
| ActiveSync User Agent | Linked Identifier |
| ActiveSync Version | Memory Capacity |
| Apple DEP Device | Network Type |
| Battery Level | OS Language |
| Charging Status | OS Version |
| Device Connection Schedule | Ownership |
| Device GMT Offset | Pending remove |
| Device IMEI | Phone Number |
| Device Model | Plan Type |
| Device Name | Policy Suite |
| Device Platform | Roaming |
| Device Time Zone | SD Card Free Memory |
| Device UID | SD Card Installed |
| DeviceSAKey | SD Card Memory |
| Domain | Shared |
| Email Address | Signal Strength |
| Expiration Date | SIM Removed or Changed |
| First Name | Suspended |
| Free Memory | TouchDown Enrolled |
| IMSI Number | User Name |
| iOS Installed Profiles | UserSAKey |
| iOS Managed Profiles | Violation Status |
| Jailbroken | VPP Association Status |
| KNOX Status | ZENworks App Language |
| KNOX Workspace Status | ZENworks App Version |
| Last ActiveSync Sync (Server Local) | ZENworks Authorization Failures (user) |
| Last APN Check-In (Server Local) | |

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 screenshot 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 --

At the bottom, there are three buttons: 'Search All', 'Search Folder', and '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.



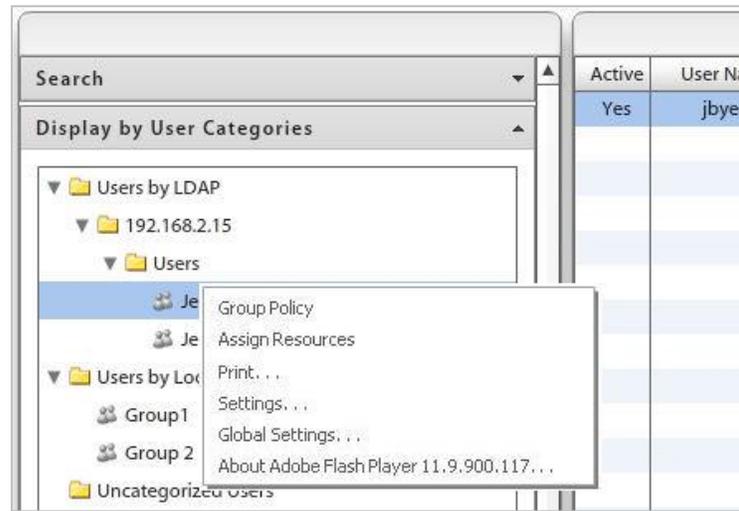
The screenshot shows a 'Display by User Categories' panel with a tree view of user categories:

- 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/Device 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.



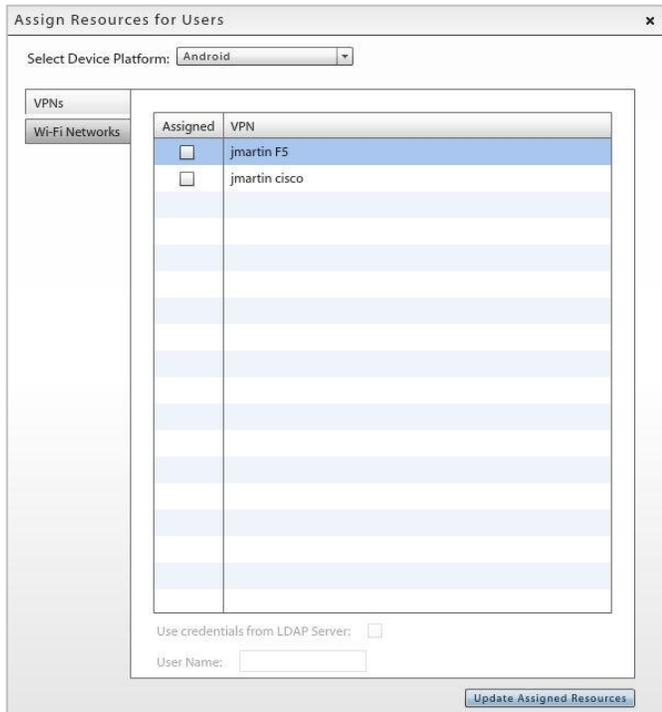
Standard Policy Enforcement



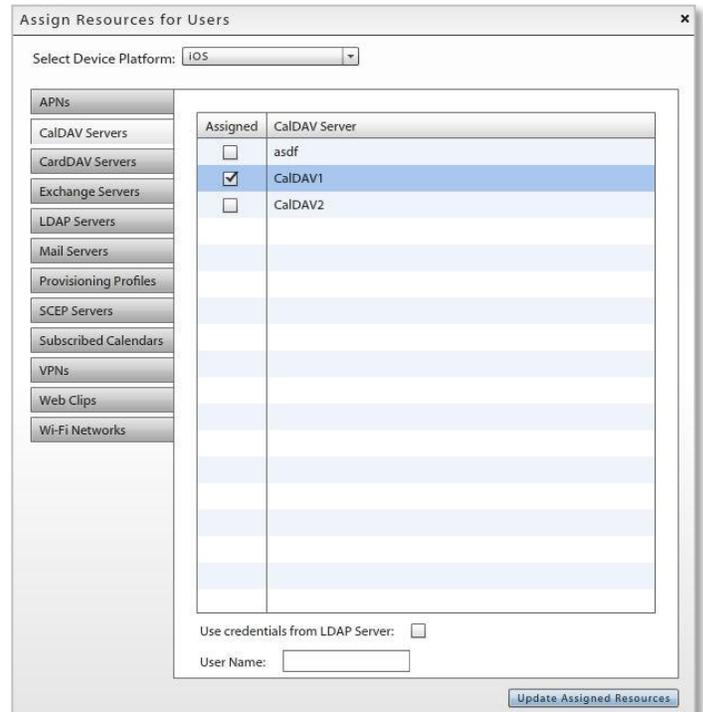
Schedule-Based Policy Enforcement

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.



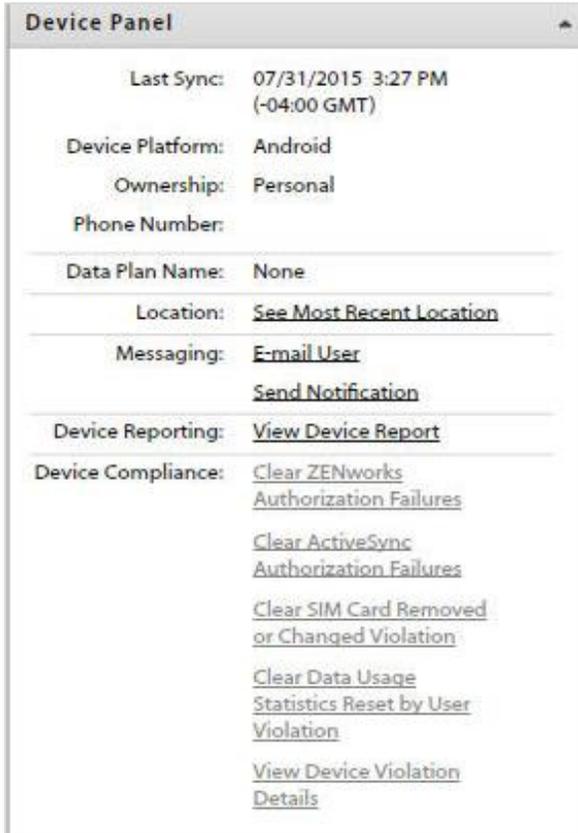
Android Resource Assignments



iOS Resource Assignments

The Device Panel

Select a user/device from the grid. A 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.



Device Panel Content

Quick Device Stats - displays last sync time, device platform, ownership, and phone number

Data Plan Statistics - Displays the plan name and limit. Also displays data used by device, data used by other devices on the plan, and remaining data for the current billing period.

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
- [Send Notification](#) – Compose and send a notification to an Android or iOS device (160 character limit).
- [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.

Monitoring Device Compliance from the Device Panel

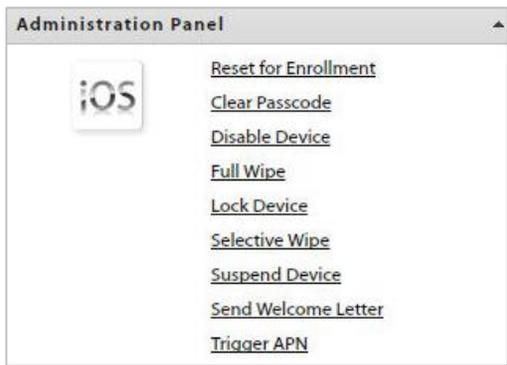
If you have implemented the *Compliance Manager* to monitor and restrict devices or users who are non-compliant with corporate policies, you might want to display the **Violation Status** column in the *Users* grid. You can quickly see which devices are restricted. Use the following options in the *Device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

Administrative Action	Description	Result
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.
Clear Data Usage Statistics Reset by User Violation	A user has reset the data usage statistics on the device and is in violation of the <i>Restrict if data usage statistics reset by user</i> access restriction.	This <i>Clear</i> button releases the device from restrictions imposed by this violation. A user exception is not created, so if the user resets the data usage statistics again, the device will be in violation.
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.



Violation Details Pop-up

The Administration Panel



Sample Administration Panel

Administration Panel Content

Administration – Security commands and administrative actions can be performed quickly. Only options that apply to the device platform will appear. Administrative actions can also be issued through the User Self Administration Portal.

- **Security Commands** - Gives quick access to reactive security commands, such as *Full Wipe*. See a list of [Remote Security Commands](#).
- **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.
- **Reboot** – Reboots the device. Applicable for Samsung KNOX devices only.
- **Power Off** – Turns the device off. Applicable for Samsung KNOX devices only.
- **Unblock Password Entry** – unblocks the password entry on a device blocked due to a password policy violation. Applicable for Samsung KNOX devices only.

Exporting Data from the User/Device 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

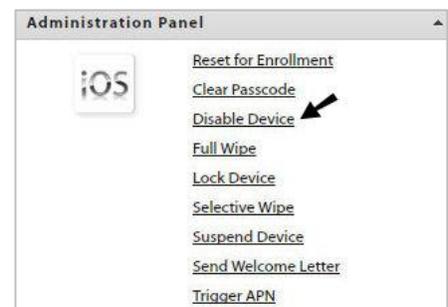
The **Remove User** button deletes the user from the *ZENworks Mobile Management* server. A user can also be temporarily disabled by using the *Disable Device* option on the Device Panel. This prevents the device from synchronizing with the *ZENworks Mobile Management* and ActiveSync servers, but retains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

Note: Shared Users can only be removed when status is *Not Enrolled* (no devices have been enrolled with the shared user credentials) or all devices enrolled with the shared user credentials have been wiped. The *Remove User* button will be disabled under any other condition.

Any DEP devices assigned to the shared user will be unassigned when the shared user is removed.



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 *Device Panel* or from the *Security* option in the Device Profile Administration view.



The Apple DEP User/Device Grid

If your organization has deployed devices through the Apple Device Enrollment Program (DEP) you can view these devices on a grid separate from the standard User/Device Grid.

Note: For information on configuring your system for DEP devices, see the [Supervised iOS Devices](#) guide.

From the dashboard, select the **Users** view. Click the **Apple DEP Devices** button in the upper right corner of the User/Device Grid page. This flips the view to a list of the DEP devices. Devices that have already been enrolled with user credentials, appear on the standard User/Device Grid as well.

A screenshot of the 'Apple DEP User/Device Grid' interface. On the left is a sidebar with 'Search', 'Display by User Categories', and 'Device Panel' (showing details for serial number C02MJ00KFD56). The main area is a table with columns: User Name, Domain, Status, Serial Number, Device Model, Description, and Profile Status. The table contains three rows of device data.

User Name	Domain	Status	Serial Number	Device Model	Description	Profile Status
N/A		Not Enrolled	C02MJ00KFD56	MacBook Pro 15.4 - inch	MBP 15.4/2.0GHZ/8GB/256GB FLASH-USA	assigned
N/A		Not Enrolled	C8QLF1ZMFFHG	iPhone 5C	IPHONE 5C WHITE 16GB-USA	pushed
N/A		Not Enrolled	DMQMC1EFF182	iPad Wi-Fi With Retina Display	IPAD WI-FI 16GB BLACK-USA	assigned

Apple DEP User/Device Grid

The Discovered Devices Grid

If you have imported device, user, and policy information from an ActiveSync server using PowerShell capabilities, the information discovered during the retrieval process is displayed in the *Discovered Devices* grid.

Note: For more information on retrieving information from an ActiveSync server, see the [PowerShell Configuration](#) guide.

From the dashboard, select the **Users** view. Click the **Discovered Devices** button located in the right corner above the User/Device Grid. This flips the view to a list of the devices discovered on the ActiveSync server. Devices that have already enrolled the *ZENworks Mobile Management* application appear on the standard User/Device Grid as well.



 A screenshot of the "Discovered Devices User/Device Grid" interface. On the left, there is a sidebar with "Search", "Device Panel", and "Administration Panel" sections. The "Administration Panel" contains an Android icon and a "Full Wipe" link. The main area is a table with the following data:

User Name	First Name	Last Name	Access State	MDM Status	Device Type	Device Platform	
bchandler	Bernard	Chandler	Allowed	Discovered	iPhone	iOS	4NVE
bchandler	Bernard	Chandler	Allowed	Discovered	iPhone	iOS	EPL10
cburrows	Craig	Burrows	Allowed	Discovered	SAMSUNGSPHD7	Android	SA
cburrows	Craig	Burrows	Allowed	Discovered	0PJA2	0PJA2	HTC8c
cmcmore	Charlene	McLemore	Allowed	Discovered	iPad	iOS	
cschuster	Carmela	Schuster	Allowed	Enrolled	SAMSUNGSMG92	SAMSUNGSMG92	
cschuster2	Carmela	Schuster2	Allowed	Discovered	SAMSUNGSMG92	SAMSUNGSMG92	

Discovered Devices User/Device Grid

Discovered Devices Grid Information

Information unique to the Discovered Devices grid will help you monitor who has not yet enrolled with the *ZENworks Mobile Management* server.

Grid Columns	Description
Access State	<p>A mobile device that is connecting to Exchange ActiveSync can be in one of several "access states" at any given time. The states most often seen in the grid are:</p> <ul style="list-style-type: none"> • <i>Allowed</i> – a state in which the device is synchronizing email, calendar, and tasks as long as it is compliant with the ActiveSync mailbox policy. • <i>Quarantined</i> – the state in which a device is placed when it has reached the quarantine date without enrolling with the MDM server.
MDM Status	<ul style="list-style-type: none"> • <i>Discovered</i> – the device information has been imported from an ActiveSync server • <i>Enrolled</i> – the device information has been imported from an ActiveSync server and it has enrolled with the MDM server.
ActiveSync Server Name	The ActiveSync server from which device information was retrieved.
ActiveSync User Agent	The ActiveSync device client on the device.

Discovered Devices Grid: Search

The *Search* option can be used to filter the discovered devices by Username, Device Platform, or Phone Number.

Discovered Devices Grid: Administration Panel

The *Administration Panel* to the left of the grid displays several device management options.

Administration Panel	Description
Devices Statistics	Displays device platform and phone number.
Hide Device	Removes a device from the grid display. Although the device is not removed from the ActiveSync server, it will not appear in the grid again when subsequent requests for information are made on the ActiveSync server. Should the device eventually enroll with MDM, it will appear on the standard Device/User grid.
E-mail User	Compose and send an email
Allow Quarantined Device	The device was not enrolled during the grace period and has been denied access to email. This <i>clear</i> button releases the device from restrictions imposed by this violation. <i>Note:</i> If the organization is configured to restrict ActiveSync connections (via Compliance Manager) when a device is out of compliance, the device cannot be released from quarantine.
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 unlock password that has been generated. A user can also view it from the <i>ZENworks Mobile Management Self-Administration</i> portal. See Enabling Password Recovery

Discovered Devices Grid: Device Profile

Select a device and click the device profile button in the action bar above the grid. The profile will display user information and device statistics, along with security actions available for the device type. If the discovered device is enrolled with MDM, the profile will show the same information that is available on a standard user profile.



The screenshot shows the ZENworks Mobile Management interface. On the left, there is a navigation pane with three sections: 'Search', 'Device Panel', and 'Administration Panel'. The 'Administration Panel' is expanded, showing an Android icon and a 'Full Wipe' button. The main area displays a table of discovered devices.

User Name	First Name	Last Name	Access State	MDM Status	Device Type	Device Platform	
bchandler	Bernard	Chandler	Allowed	Discovered	iPhone	iOS	4NVE
bchandler	Bernard	Chandler	Allowed	Discovered	iPhone	iOS	EPL1
cburrows	Craig	Burrows	Allowed	Discovered	SAMSUNGSPHD7	Android	SA
cburrows	Craig	Burrows	Allowed	Discovered	0PJA2	0PJA2	HTC8
cmcmore	Charlene	McLemore	Allowed	Discovered	iPad	iOS	
cschuster	Carmela	Schuster	Allowed	Enrolled	SAMSUNGSMG92	SAMSUNGSMG92	
cschuster2	Carmela	Schuster2	Allowed	Discovered	SAMSUNGSMG92	SAMSUNGSMG92	

The Device Profile

Select a user from the list and click the **Device 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 Device Profile. There are four tabs that display the following user information:

- [Configuration](#)
- [Certificates](#)
- [Custom Column Values](#)
- [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 page for user 'surya'. The left sidebar contains a tree view with 'User Information' selected. The main area has four tabs: 'CONFIGURATION' (active), 'CUSTOM COLUMN VALUES', 'CERTIFICATES', and 'LOCAL GROUPS'. The configuration fields are as follows:

User Name:	surya	ActiveSync Server:	192.168.21.54
Created On:	2015-02-27 14:29:20.197	LDAP Server:	192.168.21.54
First Name:	Surya	Password:	Change Password
Last Name:		Expiration:	Never
E-mail Address:	* surya@ninja3.notify.net		
Domain:	ninja3		
Maximum Number of Devices Per User:	99		
	<input checked="" type="checkbox"/> Auto (Organization Default)		

If the user is a shared user, the configurations permitted on devices enrolled with the user's credentials are displayed and can be edited.

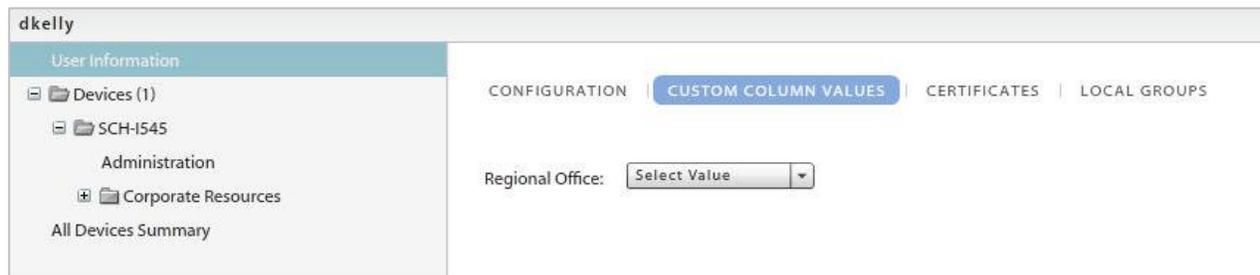
The screenshot shows a box titled 'Configurations permitted for Users signing into shared device'. It contains a list of services with checkboxes:

ActiveSync Email:	<input checked="" type="checkbox"/>	Subscribed Calender:	<input checked="" type="checkbox"/>
CalDAV:	<input checked="" type="checkbox"/>	VPN:	<input checked="" type="checkbox"/>
CardDAV:	<input checked="" type="checkbox"/>	Web Clip:	<input checked="" type="checkbox"/>
Exchange Server:	<input checked="" type="checkbox"/>	Wi-fi:	<input checked="" type="checkbox"/>
LDAP Server:	<input checked="" type="checkbox"/>		
Mail Server:	<input checked="" type="checkbox"/>		

User Information: Custom Column Values

If custom columns have been configured for users, they will be displayed here. Select this tab to view, add, or edit custom column values for this user.

Custom Columns may also be configured at the device level. See [Device Administration: Custom Column Values](#).



User Information: Certificates

Select the *Certificate* tab to upload a client authentication certificate for the user or view any *ZENworks Mobile Management* generated enterprise certificate authority (CA) certificates.

Uploaded Certificates

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>

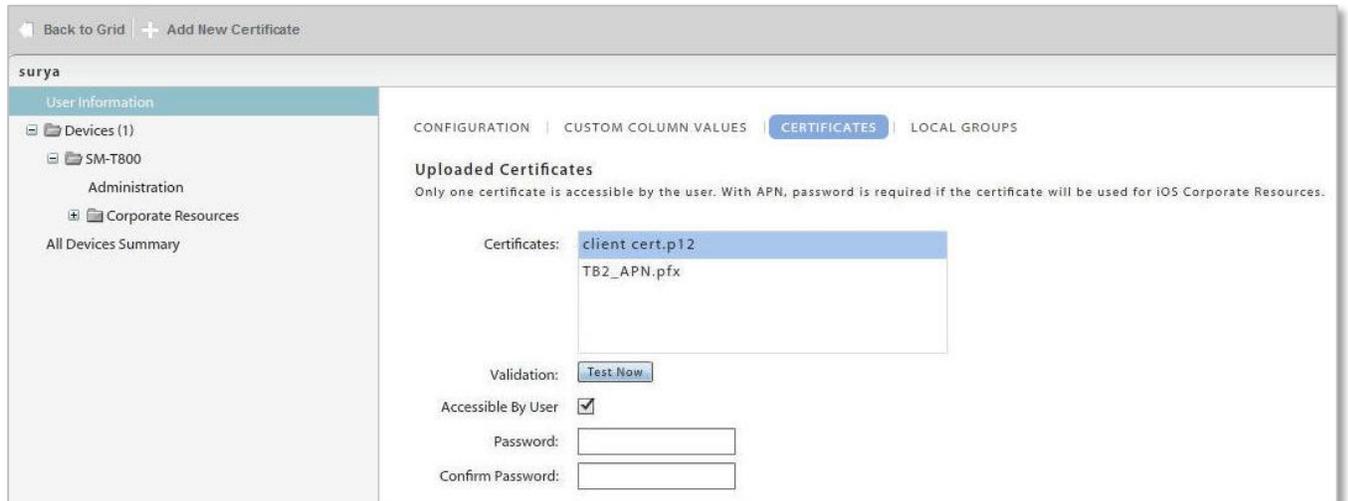
- Mobile User Self-Administration Portal: <serveraddress>/mobile
- Create a second Web server (mirroring the *ZENworks Mobile Management* server) where only the User Self-Administration Portals are available
- Create a firewall rule that allows the user to access the User Self-Administration Portal URLs 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 **Device 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. The certificate will appear in the *Uploaded Certificates* section of the page.
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 (with <i>GO!NotifySync</i>)	OS 4.5	
	OS 4.6	
	OS 5.0	
	OS 6.0	OS 6.0
	OS 7.0	OS 7.0
iOS	iOS 6+	iOS 6+

ZENworks Mobile Management Generated Enterprise CA Certificates

The lower half of the *Certificates* page lists any *ZENworks Mobile Management* generated enterprise certificate authority (CA) certificates. A certificate of this type can be re-issued or revoked from this page.

For more information on managing enterprise CA certificates, see the [Certificate Management Guide](#).

These certificates provide:

- Authentication of users with Android KNOX and iOS devices accessing ActiveSync mail servers - when *ZENworks* is configured so that it does not proxy ActiveSync traffic.
- Authentication of users with Android and iOS devices for Wi-Fi access.

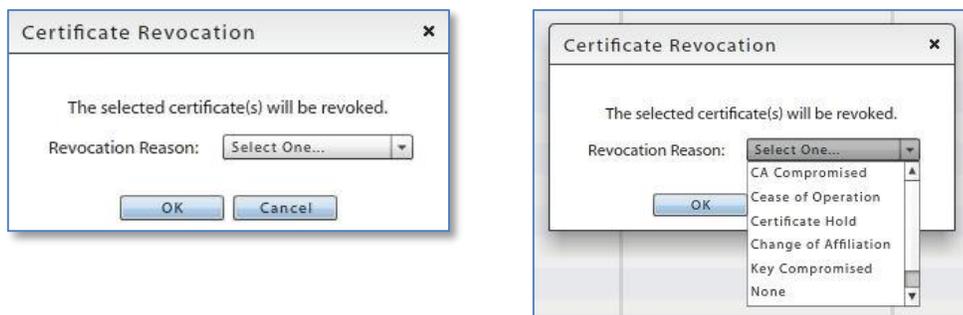
ZENworks Mobile Management Generated Enterprise CA Certificates				
Certificate Name	Corporate Resource	Issue Date	Expiry Date	Status
Surya	192.168.21.54 (ActiveSync)	02/27/2015	02/27/2016	Active

Revoke a Certificate

Certificates issued from the organization's certificate server via *ZENworks Mobile Management* can be revoked from the user's profile or from the Certificate Grid (*Organization > Certificate Management > Certificates*).

Once the Certificate Authority publishes a certificate revocation list, any resource (ActiveSync email, Wi-Fi, etc.) that uses the certificate for authentication will be inaccessible. Please note that in most cases, this does not occur immediately after an administrator has revoked the certificate. A user may still have access to resources for a short time after a certificate has been revoked.

1. Select a certificate and click the **Revoke Certificate** button.
2. Select a **Revocation Reason**.



CA Compromised	Certificate authority (CA) that issued the certificate has been compromised
Cease of Operation	Client no longer qualifies for the certificate
Certificate Hold	Certificate has been placed on hold
Change of Affiliation	Subject value associated with the certificate has been modified
Key Compromised	Certificate's key has been compromised
None	No reason specified
Superseded	Certificate is no longer valid for the intended purpose or has been superseded by another certificate

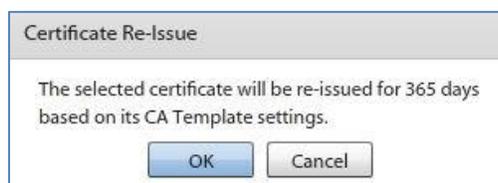
3. Click **OK** to confirm the revocation.

Re-Issue a Certificate

Certificates issued from the organization's certificate server via *ZENworks Mobile Management* can be re-issued from the user's profile or from the Certificate Grid (*Organization > Certificate Management > Certificates*).

When a certificate is re-issued it is valid for the number of days specified on the template from which the certificate was generated.

1. Select a certificate and click the **Re-Issue Certificate** button.



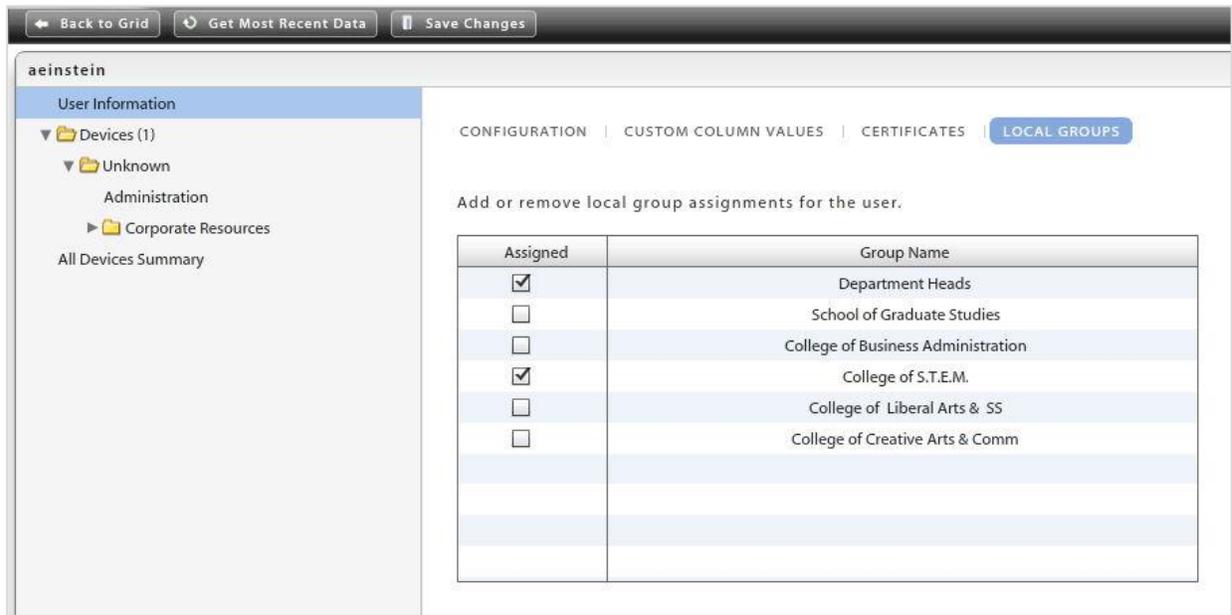
2. Click **OK** to confirm the action.

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.



The screenshot displays the user management interface for 'aeinstein'. At the top, there are buttons for 'Back to Grid', 'Get Most Recent Data', and 'Save Changes'. The left sidebar shows a navigation tree with 'User Information' selected. The main content area has tabs for 'CONFIGURATION', 'CUSTOM COLUMN VALUES', 'CERTIFICATES', and 'LOCAL GROUPS'. Below the tabs, there is a heading 'Add or remove local group assignments for the user.' and a table with two columns: 'Assigned' and 'Group Name'.

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.

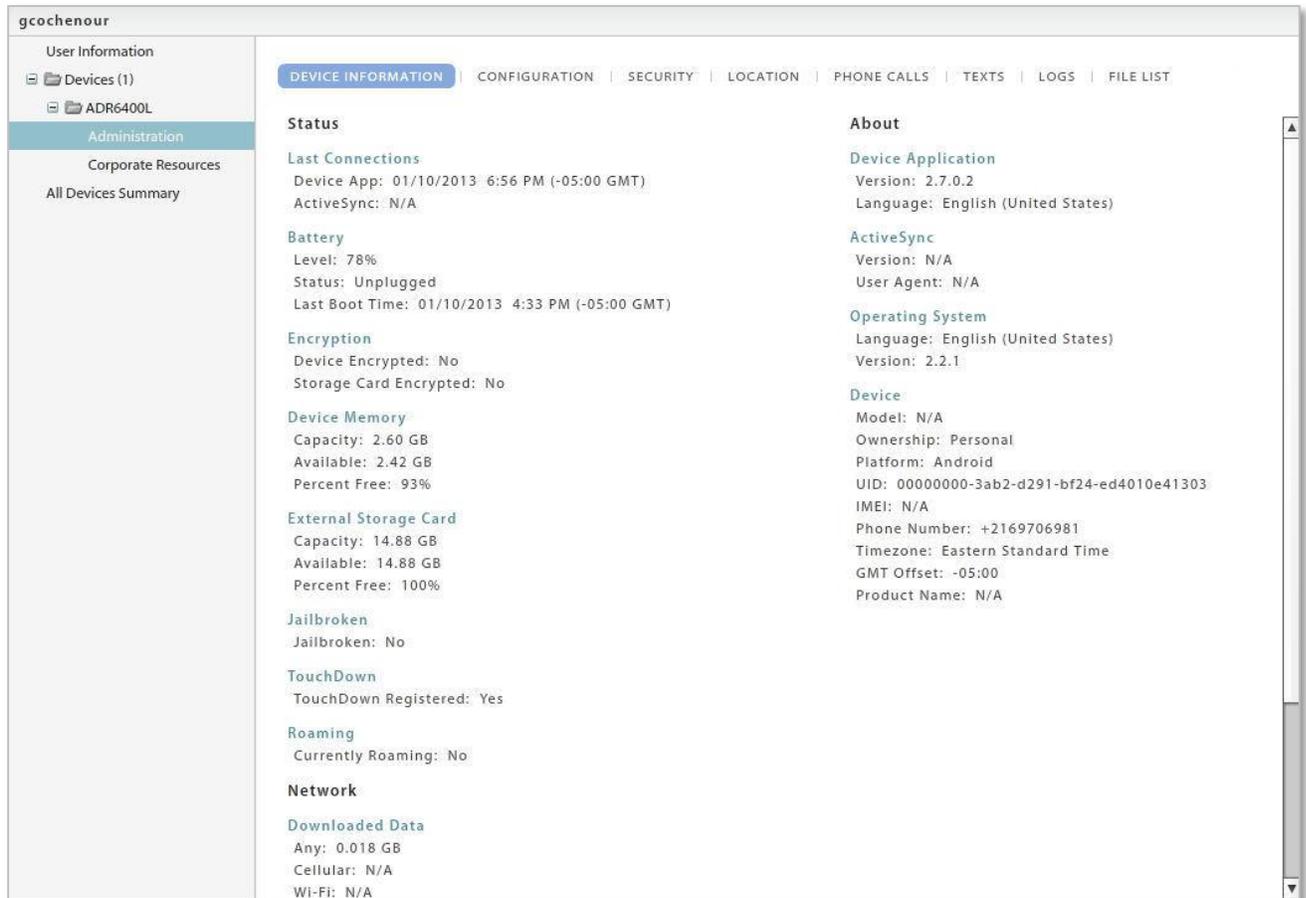
- [Device Information](#)
- [Location](#)
- [Configuration](#)
- [Phone Calls and Texts](#)
- [Custom Column Values](#)
- [Viewing Logs](#)
- [Security](#)
- [File List](#)

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 two columns of data:

DEVICE INFORMATION	CONFIGURATION	SECURITY	LOCATION	PHONE CALLS	TEXTS	LOGS	FILE LIST
Status Last Connections Device App: 01/10/2013 6:56 PM (-05:00 GMT) ActiveSync: N/A Battery Level: 78% Status: Unplugged Last Boot Time: 01/10/2013 4:33 PM (-05:00 GMT) Encryption Device Encrypted: No Storage Card Encrypted: No Device Memory Capacity: 2.60 GB Available: 2.42 GB Percent Free: 93% External Storage Card Capacity: 14.88 GB Available: 14.88 GB Percent Free: 100% Jailbroken Jailbroken: No TouchDown TouchDown Registered: Yes Roaming Currently Roaming: No Network Downloaded Data Any: 0.018 GB Cellular: N/A Wi-Fi: N/A							
About 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 Data Plan are displayed and can be edited. The Blacklist or Whitelist associated with the user's policy suite can be viewed by clicking the symbol next to the Policy Suite field.

The screenshot shows the 'Configuration' tab for a device named 'iPhone 4S' under the user 'twhitehouse'. The left sidebar contains a navigation menu with 'Administration' selected. The main content area has tabs for 'DEVICE INFORMATION', 'CONFIGURATION', 'SECURITY', 'LOCATION', 'PHONE CALLS', 'TEXTS', 'LOGS', and 'FILE LIST'. The 'CONFIGURATION' tab is active, showing various settings:

- 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...'.
- Plan Type:** Dropdown menu set to 'Unknown'.
- Policy Suite during Schedule:** Dropdown menu set to 'Policy A' with a checkmark icon.
- Carrier:** Dropdown menu set to 'None'.
- Policy Suite outside Schedule:** Dropdown menu set to 'Policy B' with a checkmark icon.
- Auto (Organization Default):** A checkbox that is currently unchecked.
- Device Connection Schedule:** Dropdown menu set to 'default'.
- Schedule:** A checked checkbox with the text 'Auto (Organization Default)' below it.
- Liability:** Dropdown menu set to 'Corporate'.
- Auto (Organization Default):** A checked checkbox with the text 'Auto (Organization Default)' below it.

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

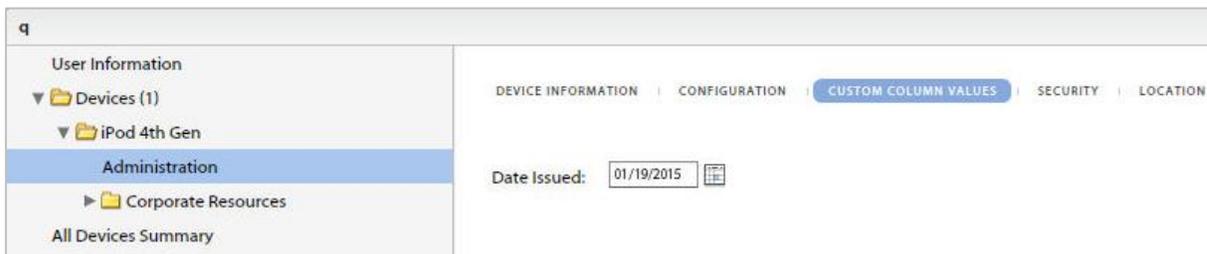
- Blacklists:** A 'Default' row with a 'Permissions' column containing a green 'YES' button.
- Whitelists:** A 'Default' row with a 'Permissions' column containing a red 'NO' button.

Device Administration: Custom Column Values

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

If custom columns have been configured for devices, they will be displayed here. Select this tab to view, add, or edit custom column values for this device.

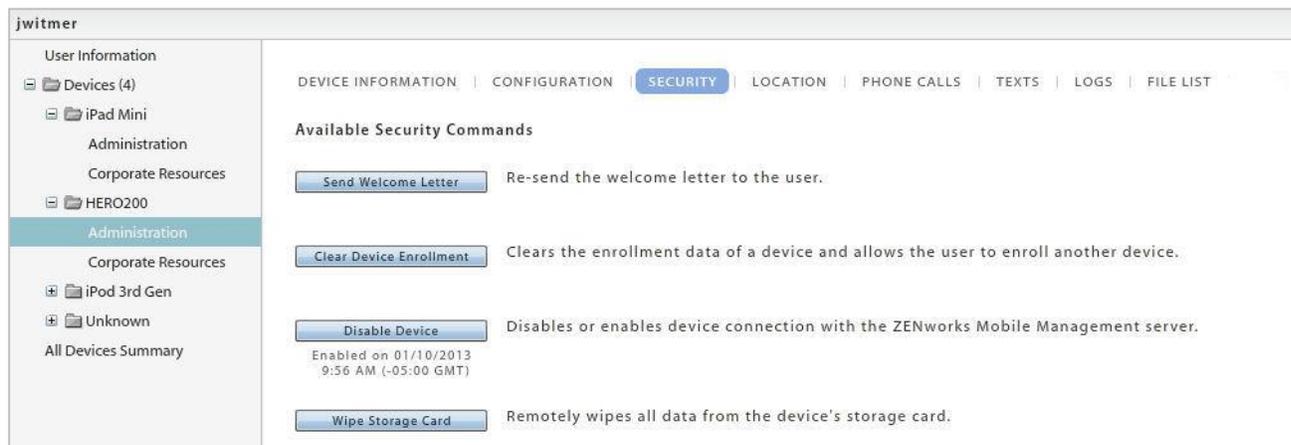
Custom Columns may also be configured at the user level. See [User Information: Custom Column Values](#)



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.



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.



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.

Anrd	Android devices	Windows	Windows devices w/ OS 8.1/10
TD/A	Android devices with TouchDown	wOS	webOS devices
NS/BB	GO!NotifySync for BlackBerry	WP7	Windows Phone 7 devices
iOS	iOS multitasking devices	BB10	BlackBerry 10 devices
TD/iOS	iOS multitasking devices with TouchDown		

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/Device Grid. Functionality varies by device.</p> <p><i>Note:</i> See Appendix A for information on recovering user information for devices removed from the grid.</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>ZENworks Mobile Management app: Anrd, NS/BB, iOS, TD/iOS, TD/A</p> <p>ActiveSync only: BB10, wOS, WP7</p> <p>Windows 8.1+</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><i>Windows 8.1+:</i> the device is unenrolled and returns to factory settings removing all internally stored data and device settings.</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 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><i>Windows 8.1+:</i> device is unenrolled and configured policies, apps, etc. are automatically removed.</p>	<p>ZENworks Mobile Management app: Anrd, NS/BB, iOS, TD/iOS, TD/A</p> <p>Windows 8.1+</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><i>Note:</i> Shared Users can only be removed when status is <i>Not Enrolled</i> or all devices enrolled with the shared user credentials have been wiped. Any DEP devices assigned to the shared user will be unassigned when the shared user is 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.</p>	<p>ZENworks Mobile Management app: Anrd, NS/BB, iOS, TD/iOS, TD/A</p> <p>ActiveSync only: BB10, wOS, WP7</p>
Wipe Storage Card	<p>Remotely wipes all data from the device's storage card.</p>	<p>ZENworks Mobile Management app: Anrd, NS/BB, TD/A</p>
Lock Device	<p>Remotely locks the device, requiring a password to be entered before the device can be used.</p> <p><i>iOS</i> allows for <i>Lock Device</i> to be applied immediately to <i>iOS</i> devices.</p> <p><i>Windows 8.1+:</i> Lock is initiated only if the device has a device security password enabled and only when device syncs with the server; Not supported in <i>Windows 10 Desktop</i>.</p> <p><i>Windows 10 Phones:</i> Locking the phone generates a new unlock PIN and gives the administrator an opportunity to email it to the user. See also, <i>Email Unlock PIN</i> below. Not supported for <i>Windows 10 Desktop</i> or tablets.</p>	<p>ZENworks Mobile Management app: Anrd, NS/BB, TD/A, iOS, TD/iOS</p> <p>Windows 8.1+</p>
Disable / Enable Device	<p>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>	<p>ZENworks Mobile Management app: Anrd, NS/BB, iOS, TD/iOS, TD/A</p> <p>ActiveSync only: BB10, wOS, WP</p>
Disown Device	<p>Disown Device should only be used if you want to permanently remove an Apple DEP device from the grid and notify the Apple servers that your organization no longer owns the device. Once a device is disowned, it cannot be reassigned to the server as an Apple DEP device. Disowning removes the DEP profile from the device.</p> <p>Note: Issue a Selective Wipe prior to disowning a device. <i>(In a future release, disowning a device will initiate a Selective Wipe automatically, as well as remove the DEP profile from the device.)</i></p>	<p>iOS DEP devices</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.	ZENworks Mobile Management app: Anrd, NS/BB, iOS, TD/iOS, TD/A ActiveSync only: BB10, wOS, WP7
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 Enabling Password Recovery .	ZENworks Mobile Management app: NS/BB, TD/A, TD/iOS
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.	ZENworks Mobile Management app: iOS, TD/iOS
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.	ZENworks Mobile Management app: iOS, TD/iOS
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.	ZENworks Mobile Management app: Anrd, TD/A
Reset to Shared Profile	If a user is signed in to a shared device, issuing this command signs the user out, removes all the user's profiles, and configures the device with the shared profile settings. The device remains in a managed state.	ZENworks Mobile Management app: Anrd, iOS, TD/iOS, TD/A
Remote Ring	This action will audibly ring the device to assist in location, even if it is set to vibrate or silent.	Windows 8.1+
Reset PIN	Resets the PIN that unlocks a device and transmits a new PIN to the server. The new PIN can be viewed on the server via the Desktop User Self-Administration Portal. Only supported for Windows 8.1/10 phones.	Windows 8.1+ phones
Email Unlock PIN	Sends an email to the user with the unlock PIN from the most recent lock action. Only supported for Windows 10 phones.	Windows 10 phones

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 this, a section titled 'Select up to 10 Times to Map' features 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 5:13 PM to 5:23 PM (-05:00 GMT) and coordinates 41.024386, -80.711078. To the right of the table is an 'Export Format' dropdown menu. Below the table, there are controls for 'Map Type' (set to 'Roadmap') and 'Zoom Level' (a slider). The main area is a Google Map showing the location of the device at three different points in time, marked with blue pins numbered 1, 2, and 3. The map shows a residential area with streets like Boardman Canfield Rd, Lockwood Blvd, and Mill Creek Blvd, and Mill Creek Park.

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: to

Phone Number: Origin: Status: Roaming: Duration:

Search Results 

Device Local Time	Origin	Phone Number	Status	Roaming	Duration

Summary of Search Results

Call Count Total: 0 Incoming: 0 Outgoing: 0 Unknown: 0	Average Call Duration Overall: -- Incoming: -- Outgoing: -- Unknown: --	Calls While Roaming Total: 0 Incoming: 0 Outgoing: 0 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: Auto Complete Origin: Any Type: Any Status: Any Roaming: Any

Search Results 

Device Local Time	Origin	Type	Phone Number	Status	Roaming	Subject	Message

Summary of Search Results

Text Count	Text Type Count	Texts While Roaming
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.
- **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)
- **Shared User Log** – View a list of sign in and sign out events for a shared device.

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 *Device 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 shows a web interface with a navigation bar at the top containing tabs: DEVICE INFORMATION, CONFIGURATION, SECURITY, LOCATION, PHONE CALLS, TEXTS, LOGS (highlighted), 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. A table with five columns is shown: 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

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.

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 selected in the dashboard. The search filters are set to 'From: 01/22/2013 9:10 AM' and 'To: 01/22/2013 10:10 AM'. The 'Log Type' is set to 'Device Log'. A 'Request Log' button is visible. Below the search area is a table titled 'Device Log Search Results' 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 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.

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

Shared User Log

The Shared User Log shows a list of sign in and sign out events for a shared device.

The log displays:

- Event Type – The event that occurred was a **Sign-In** or a **Sign-Out**
- User – Username of the individual that signed in/out
- Timestamp – Date and time of the Sign-In/Sign-Out

Select **Shared User Log** from the *Log Type* drop-down list.

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

When the Shared User 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 ylus interface for viewing a Shared User Log. The left sidebar contains a navigation tree with 'User Information', 'Devices (1)', 'iPad5,3', 'Administration', and 'Corporate Resources'. The main area has a top navigation bar with tabs: DEVICE INFORMATION, CONFIGURATION, CUSTOM COLUMN VALUES, SECURITY, LOCATION, PHONE CALLS, TEXTS, LOGS (selected), and FILE LIST. Below the tabs are search filters: 'From:' (02/25/2015 3:05 AM) and 'To:' (02/25/2015 4:05 PM). A 'Log Type:' dropdown is set to 'Shared User Log'. There are 'Reset' and 'Search' buttons. Below the filters is a table titled 'Shared User Log Search Results' with columns 'Event Type', 'User', and 'Timestamp'. The table contains one row: 'Sign-In', an empty 'User' field, and '02/25/2015 11:51 AM (-05:00 GMT)'. At the bottom right, there are 'Export Format' and 'Export Grid' buttons.

Event Type	User	Timestamp
Sign-In		02/25/2015 11:51 AM (-05:00 GMT)

Shared User Log

Device Administration: File List

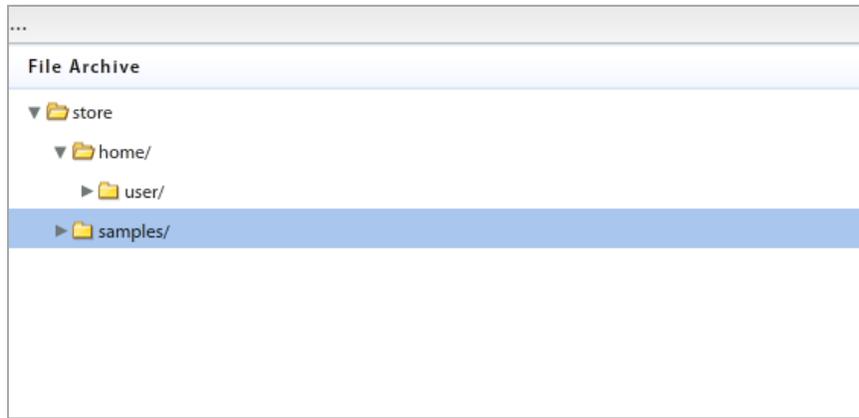
[\(return to Device Administration menu\)](#)

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 Device 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 managed applications.

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 user. If they are set when the resource is created, however, they cannot be changed at the user level.

- **Allow Move** – When disabled, this option prevents an iOS 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 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 *Device Profile*. Click the resource you want to assign.
2. Select a resource from the grid and enter any required user information or credentials.

The screenshot displays the configuration page for CalDAV Servers for user 'jstewart'. The left sidebar shows a tree view under 'Administration' with 'Corporate Resources' expanded to 'CalDAV Servers'. The main content area is titled 'CalDAV Servers' and includes a note: 'Note: Removal of a resource that has been assigned via LDAP group or folder is temporary, since LDAP periodic update will reassign the resource.' Below this is a table of 'Assigned CalDAV Servers' with one entry: CalDAV1, Server Address 123.456.7.89, Port 80, and Use SSL No. Underneath is the 'User Account Settings' section with fields for CalDAV Server (CalDAV1), User Name (jstewart), Password (masked with asterisks), Confirm Password (masked with asterisks), and Principal Address (empty).

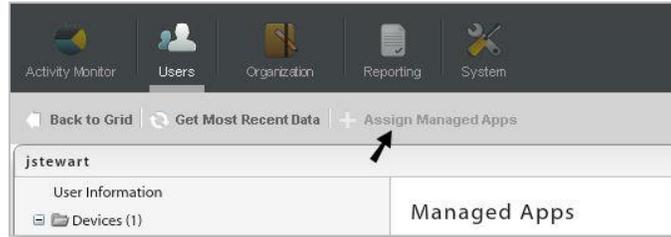
CalDAV Server	Server Address	Port	Use SSL
CalDAV1	123.456.7.89	80	No

Sample iOS Resource Assignment

Corporate Resources: Managed Apps

Assigning Managed Apps to a Device

1. To make an app assignment, expand the **Corporate Resources** option on the left panel of the *Device 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 an 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).

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"/>

[Update Resources](#)

Assign apps that have not already been assigned

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"/>

[Update Resources](#)

Remove only the apps assigned at the user level

4. Click **Update Resources** when you have finished making a selection from the grid.

Assignments made at the user level are not affected by changes in app assignments associated with 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 *Device 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"/>	<input type="checkbox"/>
Frequency for archiving files (in days)	7	7	7
Record phone log		<input type="checkbox"/>	<input type="checkbox"/>
Record text message log		<input type="checkbox"/>	<input type="checkbox"/>
Record installed applications		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Record managed applications		<input type="checkbox"/>	<input type="checkbox"/>

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		
Allow app management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Record installed applications	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

The App Grids: Managed Apps

The **Managed Apps** grid lists all applications available to an Android or iOS user.

When administrators add applications to the Android or iOS managed app list, 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 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 appear on the *Installed Apps* list and cannot be managed. If the server detects that an app published as managed is already installed on the device as unmanaged, it issues a command that changes the app's state from unmanaged to managed. This happens automatically on supervised devices without input from the user. On unsupervised devices, users must acknowledge the change if it involves a non-VPP app.

IOS MANAGED APPS GRID³¹

App Name	Version	Status	Rejection Reason	Remove With MDM	Prevent Backup	Redemption Code	Has Configuration	Has Feedback	Time
ConfigApp	1	Not Installed via MDM					No	No	08/11/2014

Buttons: 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	
Status	<p>The most common status messages include:</p> <ul style="list-style-type: none"> • <i>Managed</i> – Indicates that the app is installed on the device • <i>Not Installed via MDM</i> – <ul style="list-style-type: none"> ○ 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>. OR ○ Indicates the app was installed prior to the device being enrolled with MDM or prior to the app being designated as a managed app. MDM is not able to manage it unless the user removes the app and then re-installs it through MDM. • <i>Managed, but Uninstalled</i> – Indicates an app that is not installed; possibly because it was removed by the user or is not required. <p>Other status messages give additional information about apps on the device.</p>

Rejection Reason	If the app is not installed, look here to see if installation of the app was attempted and why it was rejected.
Remove with MDM	Whether this app is removed, along with its data, if the MDM profile is removed.
Prevent Backup	Whether the user is prevented from backing up this app via iTunes.
Redemption Code	The redemption code associated with a Volume Purchase Program (VPP) app.
Has Configuration	Whether the app has a server-provided configuration.
Has Feedback	Whether the configured app has feedback for the server.
Timestamp	Last update of the app's status.
Install App button	Issues a command that prompts the user to install the app.
Reinstall App button	Issues a command that prompts the user to reinstall the app.
Uninstall App 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.
Remove Redemption Code 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.
Request Config/Feedback 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.
View Config/Feedback button	Links to the Logs tab so that you can view the information the app received via the configuration file and any available feedback information.

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)	Container Id
MDM	3.7.0.3769	User	3769	net.notify.notifymdm	66.023	34.438	None
Active Apps Manager	1.0.0	System	1	com.sec.android.widgetapp.activeapp	0	0	None
Adapt Sound	1.0	System	1	com.sec.hearingadjust	0	0	None
Alarm	1.0	System	1	com.sec.android.widgetapp.alarmwid	0	0	None
AllShare Cast Dongle S/W Upd	1.2.3717	System	1800011	com.sec.android.fwupgrade	1.897	1.662	None
AllShare ControlShare Service	1.0.0	System	10	com.sec.android.allshare.service.contr	0	0	None
AllShare FileShare Service	1.4r476	System	16	com.sec.android.allshare.service.flesh	0	0	None
Amazon Kindle	4.6.0.128	System	1142423680	com.amazon.kindle	0	0	None
Android System	4.4.2-1337U	System	19	android	1.897	1.662	None

Data Display: KB MB GB Export Format

Device Summary

Select **All Devices Summary** from the *Device 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.

The screenshot shows a web interface for user management. On the left is a sidebar for user 'jwitmer' with the following menu items: User Information, Devices (2), iPad Mini, Administration, Corporate Resources, iPod 3rd Gen, and All Devices Summary (highlighted). The main area is titled 'All Devices for jwitmer' and contains a table with the following data:

UserSAKey	Active	User Name	Email Address	First Name	Last Name	Domain	Liability	Ownership	Last ZENworks Sync (S
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 view.

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

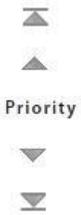
- add groups
- assign group membership
- configure a group with Policy Suite, Device Connection Schedule, Liability settings, and Novell Filr profile (if applicable).
- prioritize groups (necessary only when users belong to multiple groups)
- change group membership or a group name
- remove a group

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.

Group Name: *

Search available users

Username: *

Search Reset

List of available users

Username	Domain
aeinstein	
alincoln	
fnightengale	
jstewart	
khepburn	
mcurie	

List of assigned users

Username	Domain

Add Group

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.

Group Name: * Department Heads

Search available users

Username: *

Search Reset

List of available users

Username	Domain
alincoln	
fnightengale	
jstewart	
khepburn	

List of assigned users

Username	Domain
aeinstein	
mcurie	

Update Group

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

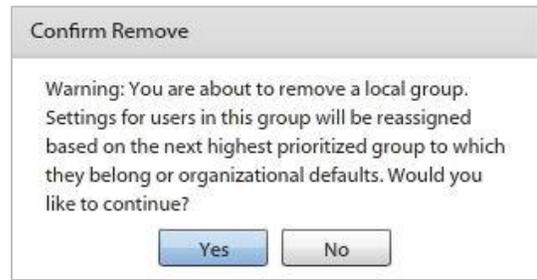
Whitelists/Blacklists: Policy A

	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**.



Application Management

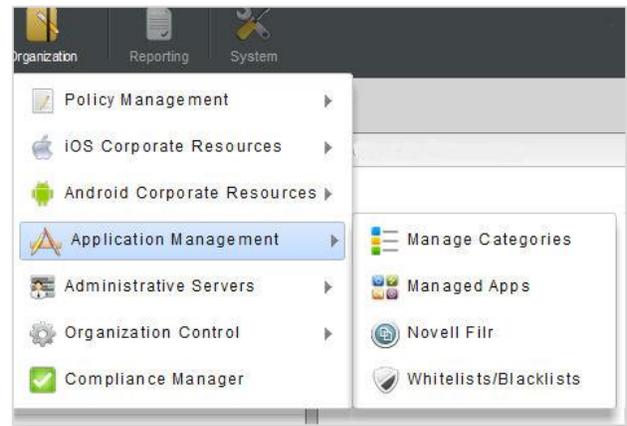
Application Management is located in the *Organization* view of the dashboard.

The [Manage Categories](#) option allows you to create application categories so that apps can be grouped and assigned in bundles to LDAP group/folders or local groups.

The [Managed Apps](#) option gives you the ability to make available to users a list of recommended applications. Android and iOS applications can be designated as mandatory so that users are automatically prompted to install them. In addition, Android and iOS apps can be assigned to the LDAP groups/folders or local groups to which users belong.

[Novell Filr](#), a secure system for mobile file access and sharing, is integrated with *ZENworks Mobile Management* for Android devices and iOS 7.1 or higher devices using the Filr app version 1.0.4 or higher. The integration gives you the ability to create a configuration profile from the dashboard that, when assigned to users, will configure the Novell Filr app on devices.

[Whitelists/Blacklists](#) gives you the ability to restrict a user based on the applications he or she has installed on the device. Users' access to email, shared files, app lists, or other organization resources can be blocked when they are not in compliance with restrictions.



Application Categories

Managed Android and iOS applications can be grouped into categories so that multiple apps can be assigned in bundles to LDAP groups/folders or local groups.

You can create your own categories or use the categories in the *Manage Categories* grid. The existing categories in the grid reflect categories used by App Stores. They can be removed from the list, but not edited. You can sort the list by clicking on either of the column headings.

Creating, Editing, or Removing Categories

From the dashboard, navigate to **Organization > Application Management > Manage Categories**. A list of categories displays. The list initially consists of App Store Categories, however, you can create additional ones. You can edit the categories that you create, but the App Store categories cannot be edited. Click on the column headers to sort the list of categories.

- **Add a category:** Enter a name that describes a group of applications in the **Category Name** field. Click **Add**.
- **Edit a category name:** Select a category that you created (App Store category names cannot be edited) and click **Edit**. Type a revised category name in the text box and click **OK**.
- **Remove a category:** Select a category and click **Remove**. Confirm the removal.

The screenshot shows the 'Manage Categories' interface. At the top, there is a text input field labeled 'Category Name:' and an 'Add' button. Below this is a table with two columns: 'Category Name' and 'App Store Category'. The table contains the following data:

Category Name	App Store Category
Medical	Yes
Music	Yes
Music & Audio	Yes
Navigation	Yes
News	Yes
News & Magazines	Yes
Newsstand	Yes
Personalization	Yes
Photo & Video	Yes
Photography	Yes
Productivity	Yes
Reference	Yes
Sales Team	No
Shopping	Yes
Social	Yes
Social Networking	Yes

To the right of the table, there are three buttons: 'Add', 'Remove', and 'Edit'. The 'Sales Team' row is highlighted in blue.

Associating an Application with a Category

You can associate an Android or iOS app with a category when you add the app to your managed app list. When adding an iOS application, you can apply the categories used by iTunes or you can choose the category(ies) yourself.

[Choosing a Category for an Android App](#)

[Choosing a Category for an iOS App](#)

View Managed Apps by Category

The *Managed Apps* grid can be sorted by application categories.

From the dashboard, navigate to **Organization > Application Management > Managed Apps**.

From the *View* drop-down, select **Category** to view the managed apps by their associated categories. Since an app can be assigned to multiple categories, some apps may be listed under more than one category.

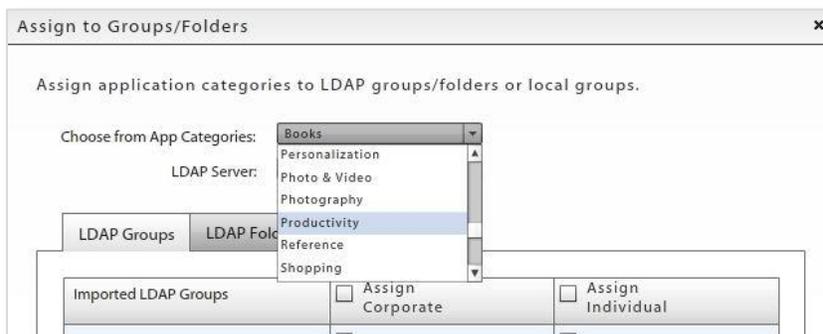


Name	Download Count	Download Limit	Categories	App File Name	App File Size (bytes)	Link
TouchDown	0	<Unlimited>	Communication, Productivity			https://play.google.com/store/apps/c
Skype	0	<Unlimited>	Productivity, Social Network			https://play.google.com/store/apps/c

Assigning a Category to LDAP Groups/Folders or Local Groups

You can assign a category of applications to all members of an LDAP group/folder or local group.

1. From the dashboard, navigate to **Organization > Application Management > Manage Categories**.
2. From the *Manage Categories* grid, select a category to assign to groups.
3. Click the **Assign to Groups/Folders** button on the action bar at the top of the page.
4. From the *App Categories* drop-down, select a category to assign.



5. If you are assigning a category to an LDAP group or folder, select a server from the **LDAP Server** drop-down.

6. In the table, select the **LDAP Groups**, **LDAP Folders**, or **Local Groups** tab.

Assign to Groups/Folders

Assign application categories to LDAP groups/folders or local groups.

Choose from App Categories: Productivity

LDAP Server: Exchange 07

LDAP Groups | LDAP Folders | Local Groups

Local Groups	<input type="checkbox"/> Assign Corporate	<input type="checkbox"/> Assign Individual
Group A	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Group B	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Group C	<input type="checkbox"/>	<input type="checkbox"/>

Save Assignment Save Assignment & Close

7. In the group list, locate the group to which you are assigning the category and mark the check box. You must make this selection for corporate device and personal device users separately.
8. Click **Save Assignment** before you assign another category. Click **Save Assignment & Close** when you are finished.

Managed Apps

Managed Apps enables the administrator to create a recommended list of applications to be made available to users with devices that have installed a *ZENworks Mobile Management* device application or BlackBerry devices with the *GO!NotifySync* application.

When an administrator creates an app list for each supported device, users can access the recommended applications from the *ZENworks Mobile Management* device agent. For Android and iOS users, the managed apps list can be customized by grouping users via an LDAP group/folder or local group and specifying which apps will appear on the group's list.

Enforced application management is supported for the Android and iOS device platforms. Administrators can force push Android and iOS applications on the Managed App list to devices. Users are automatically prompted to install the required applications.

- For **iOS** devices, MDM functionality makes it possible to add and enforce free App Store apps, enterprise apps, and apps that have been pre-purchased through the Apple Volume Purchase Program (VPP).
- For **Android** devices, MDM functionality makes it possible to add and enforce free Google Play Store apps and enterprise apps. (*ZENworks Mobile Management* version 2.7.1 or higher is required.)

If Managed Apps are accessed by users in different countries or regions, see this [Knowledge Base article](#).

Accessing Managed Apps on a Device

Users can access the recommended apps from the *ZENworks Mobile Management* device agent:

- Android users select **Managed Apps** from the *ZENworks* main screen.
- BlackBerry (with *GO!NotifySync*) users select **Managed Apps** from the *GO!NotifySync* pop-up menu.
- iOS device users select the **Managed Apps** icon from the *ZENworks* main screen.

In this section you will find information on:

- [Adding and Managing Apps for Android Devices](#)
- [Kiosk Mode Apps](#)

Adding and Managing Apps for Android Devices

Apple MDM functionality makes it possible for an administrator to manage the Android applications in the Mobile App list.

Management functionality includes:

- Installing/reinstalling/uninstalling apps at the user level
- Force pushing an app so that all users associated with an LDAP group/folder or local group are automatically prompted to install
- Adding Enterprise (in-house) apps to the list

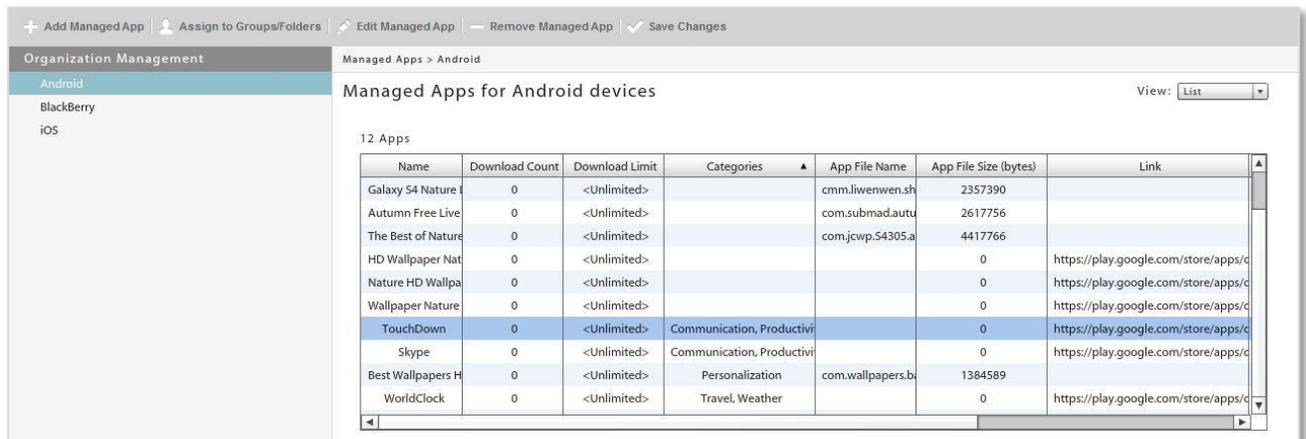
In this section:

[Permission for Managed Android Apps](#)

[Adding an Android Enterprise App](#)

[Updating Android Apps](#)

[Android Kiosk Mode Apps](#)



The screenshot shows the 'Managed Apps for Android devices' interface. It features a table with 12 apps, including 'Galaxy S4 Nature', 'Autumn Free Live', 'The Best of Nature', 'HD Wallpaper Nature', 'Nature HD Wallpapers', 'Wallpaper Nature', 'TouchDown', 'Skype', 'Best Wallpapers HD', and 'WorldClock'. The table columns are Name, Download Count, Download Limit, Categories, App File Name, App File Size (bytes), and Link. The 'TouchDown' app is highlighted in blue.

Name	Download Count	Download Limit	Categories	App File Name	App File Size (bytes)	Link
Galaxy S4 Nature	0	<Unlimited>		cmm.liwenwen.sh	2357390	
Autumn Free Live	0	<Unlimited>		com.submad.autu	2617756	
The Best of Nature	0	<Unlimited>		com.jcwp.54305.a	4417766	
HD Wallpaper Nature	0	<Unlimited>			0	https://play.google.com/store/apps/c
Nature HD Wallpapers	0	<Unlimited>			0	https://play.google.com/store/apps/c
Wallpaper Nature	0	<Unlimited>			0	https://play.google.com/store/apps/c
TouchDown	0	<Unlimited>	Communication, Productivity		0	https://play.google.com/store/apps/c
Skype	0	<Unlimited>	Communication, Productivity		0	https://play.google.com/store/apps/c
Best Wallpapers HD	0	<Unlimited>	Personalization	com.wallpapers.b	1384589	
WorldClock	0	<Unlimited>	Travel, Weather		0	https://play.google.com/store/apps/c

Permission for Managed Android Apps

The following policy suite rule must be enabled for Managed Android App functionality.

Select **Organization > Policy Management > Policy Suites > (select policy suite)**.

Choose the policy suite category **Audit Tracking** and verify that the following option is enabled:

- **Record managed applications** – required for *Force Push* and administrator-initiated app installations.

Adding Google Play Store Apps

1. Select **Organization > Application Management > Managed Apps**.
2. Select **Android** from the left panel, then click **Add Managed App**.
3. Choose *Google Play Store* as the **Method** to add the app.
4. Enter the **App Name**, **Version**, and **Description** for the app. What you enter displays on the device.
5. Enter the Play Store URL in the **Link to App** field.
6. Browse your image files at the **Icon File** field and select an icon to associate with the application.
7. Select **Remove With MDM** if you want the app to be deleted from the device when the MDM configuration profile is removed.
8. Enter the **Download Limit** if you want to track downloads of a managed app purchased in bulk. Users can no longer download the app once the limit has been reached.

Download Limit and *Download Count* are shown in the *Managed Apps* grid and a compliance alert can be set for when availability is low.

9. If you want to assign the app to an application category, click the **Add** button next to the **Categories** field. Mark check boxes to assign categories. Click **Submit**.
10. Click **Add Android App** to add the App to the Android Managed App list.

The screenshot shows the 'Add Managed App' dialog box with the following fields and options:

- Method: File Link Google Play Store
- App Name: *
- Package Name:
- App File: (Max File Size: 100 MB)
- Link to App: *
- Icon File: (Recommended Max File Size: 100 KB)
- Version: *
- Description: *
- Remove with MDM:
- Download Limit:
- Categories:
-

Category	Assign
Shopping	<input type="checkbox"/>
Social	<input type="checkbox"/>
Social Networking	<input type="checkbox"/>
Sports	<input type="checkbox"/>
Tools	<input type="checkbox"/>
Transportation	<input type="checkbox"/>
Travel	<input checked="" type="checkbox"/>
Travel & Local	<input type="checkbox"/>
Utilities	<input type="checkbox"/>
Weather	<input checked="" type="checkbox"/>
Sales Team	<input type="checkbox"/>

Adding an Android Enterprise App

An enterprise (or in-house) app is one that has been created by an organization using Android API development tools.

1. Select **Organization** > Application Management > **Managed Apps**.
2. Select **Android** from the left panel, then click **Add Managed App**.
3. Choose **File** or **Link** as the **Method** to add the app. Apps can be added as a link to the download page where the user can obtain the app, or as an actual app file that the user can install.
4. Enter the **App Name**, **Version**, and **Description** for the app. What you enter displays on the device.
5. For **Links**, provide a URL for the application in the **Link to App** field.

For **Files**, browse to select an .apk file at the **App File** field.

6. Enter the **Package Name** for the app. This is the unique identifier associated with the app. It must be accurate. For the **Novell Filr** app, enter: com.novell.filr.android

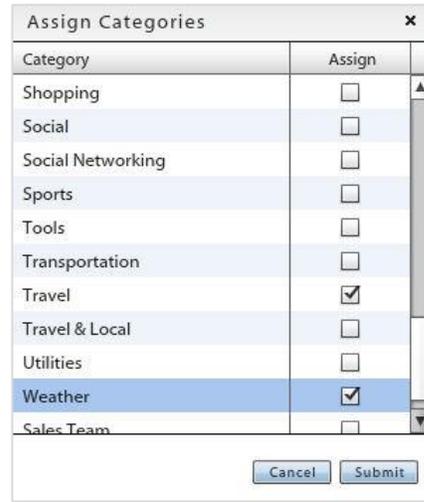
Note: When Force Push is on, *ZENworks Mobile Management* uses this to verify whether the app is installed on the device. If entered incorrectly, it will try to verify by comparing the value in the **App Name** field with the actual application name sent from the device. If Force Push fails to verify that the app is installed, the user will be continually prompted to install.

7. Browse your image files at the **Icon File** field and select an icon to associate with the application.
8. Select **Remove With MDM** if you want the app to be deleted from the device when the MDM configuration profile is removed.
9. Enter the **Download Limit** if you want to track downloads of a managed app purchased in bulk. Users can no longer download the app once the limit has been reached.

Download Limit and *Download Count* are shown in the *Managed Apps* grid and a compliance alert can be set for when availability is low.

The screenshot shows the 'Add Managed App' dialog box. It features a title bar with the text 'Add Managed App' and a close button. The main area contains several input fields and options. At the top, there are three radio buttons for the 'Method': 'File' (which is selected), 'Link', and 'Google Play Store'. Below this are fields for 'App Name' (with a red asterisk), 'Package Name', 'App File' (with a 'Browse...' button, a red asterisk, and a red note 'Max File Size: 100 MB'), 'Link to App', 'Icon File' (with a 'Browse...' button, a red asterisk, and a red note 'Recommended Max File Size: 100 KB'), 'Version' (with a red asterisk), and 'Description' (with a red asterisk). There is a checked checkbox for 'Remove with MDM', a text box for 'Download Limit', and an 'Add' button for 'Categories'. At the bottom of the dialog is a button labeled 'Add Android App'.

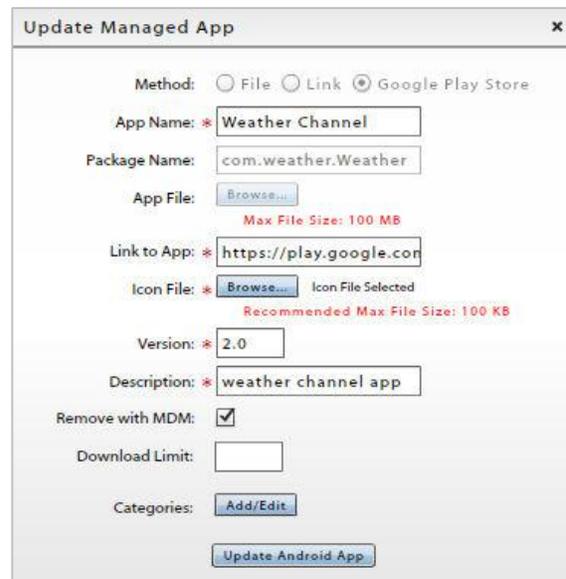
10. If you want to assign the app to an application category, click the **Add** button next to the **Categories** field. Mark check boxes to assign categories. Click **Submit**.
11. Click **Add Android App** to add the App to the Android Managed App list.



Updating Android Apps

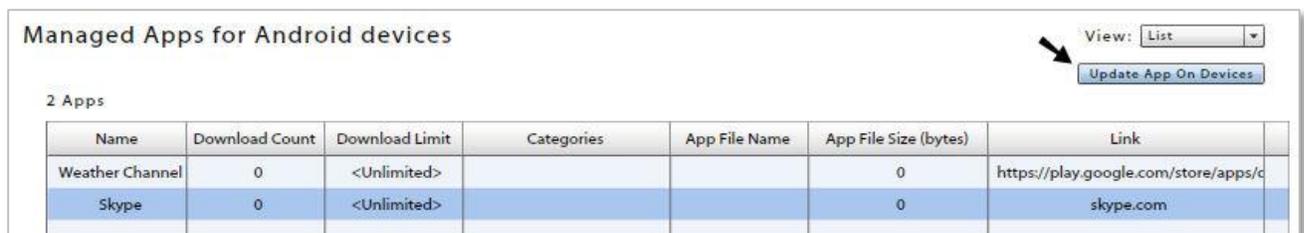
Edit Android App Information

Select an app from the grid and click the **Edit Managed App** button. Edit the original app information and click **Update Android App**.



Update Android App Versions

Select an app from the grid and click the **Update App on Devices** button above the grid to push the latest version of the app from Google Play Store to devices. Users will be prompted to update the app.



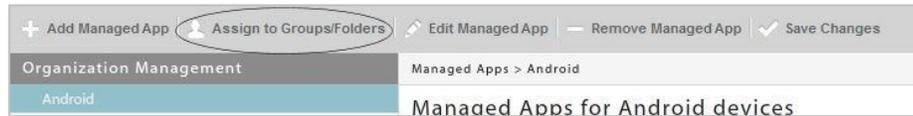
Assigning Android Apps to Members of LDAP Groups/Folders or Local Groups

You can assign Android managed apps to all members of an LDAP group/folder or local group.

Note: You can also assign Android managed apps to individual user devices. See [Corporate Resources: Managed Apps](#).

To assign Android apps to all members of an LDAP group/folder or local group:

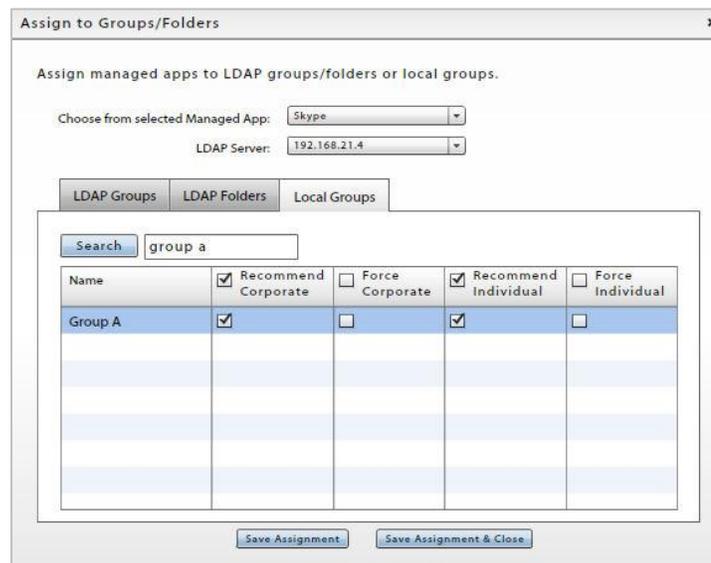
1. From the *Managed Apps* data grid, select an app to assign to groups or use CTRL+click to select multiple apps.
2. Click the **Assign to Groups/Folders** button on the action bar at the top of the page.



3. From the *Managed App* drop-down, select an app to assign or select **All** to assign all apps selected from the Managed Apps data grid.



4. If you are assigning apps to an LDAP group or folder, select a server from the *LDAP Server* drop-down.
5. In the table, select the **LDAP Groups**, **LDAP Folders**, or **Local Groups** tab. You can search the groups by entering a value in the search box and clicking the *Search* button. The group *Name* column can be sorted by clicking the column header.



6. In the group list, locate the group to which you are assigning the app(s) and determine whether or not the app(s) will be required on user devices.
 - Check the **Recommend** box to make the app(s) available to users in this group.
Or check the *Recommend* box in the header to make the app(s) available to users in all groups.
 - Check the **Force** box to force push the app(s) to devices. Users will be required to install the app(s). Checking this box will automatically mark the *Recommend* box as well.
Or check the *Force* box in the header to force push the app(s) to devices of all groups.

You must make this selection for corporate device and personal device users separately.
7. Click **Save Assignment** before you make assignments for another group.
Click **Save Assignment & Close** when you are finished.

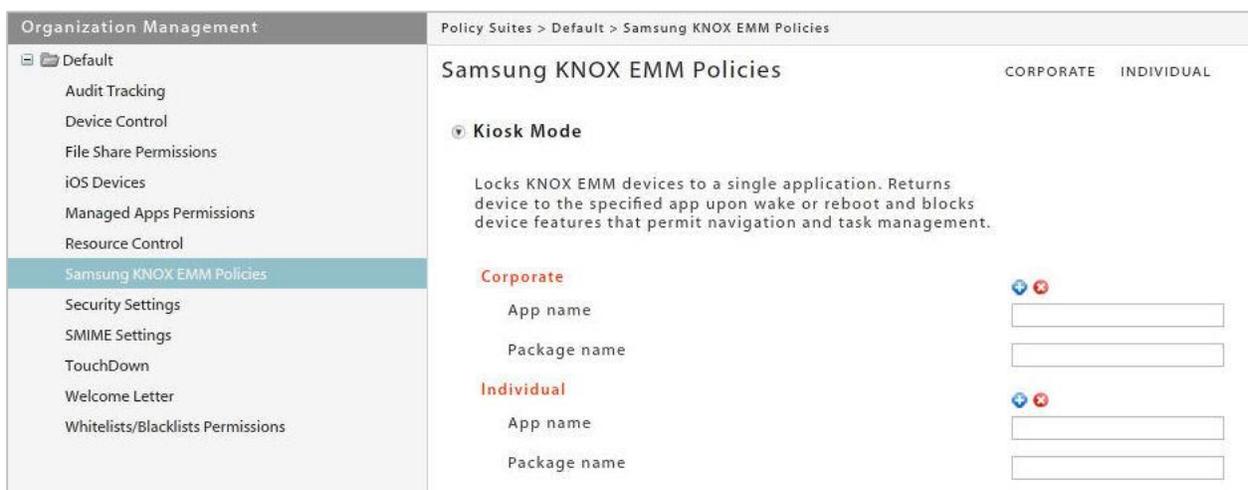
Android Kiosk Mode Apps

Kiosk Mode provides a way for administrators to specify a single application to which KNOX (Samsung SAFE) devices will be locked. The device returns to the specified app upon wake or reboot and blocks device features that permit navigation and task management.

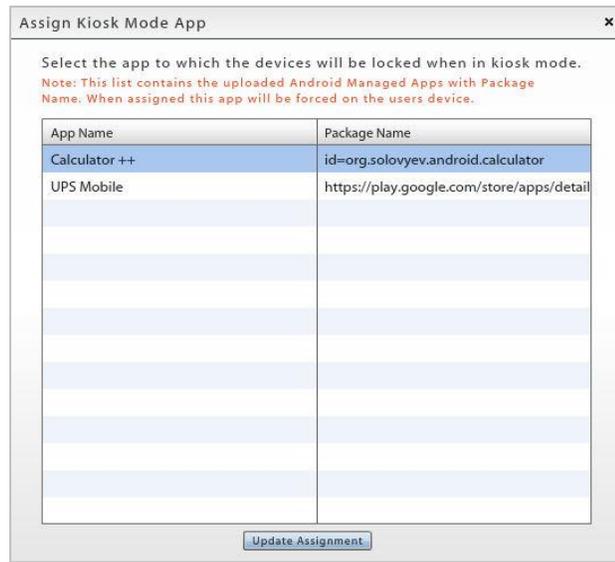
There can only be one kiosk app named at a time. Since device navigation buttons are disabled, the kiosk app should be one that is completely navigable from within the app.

To Define a Kiosk Mode App

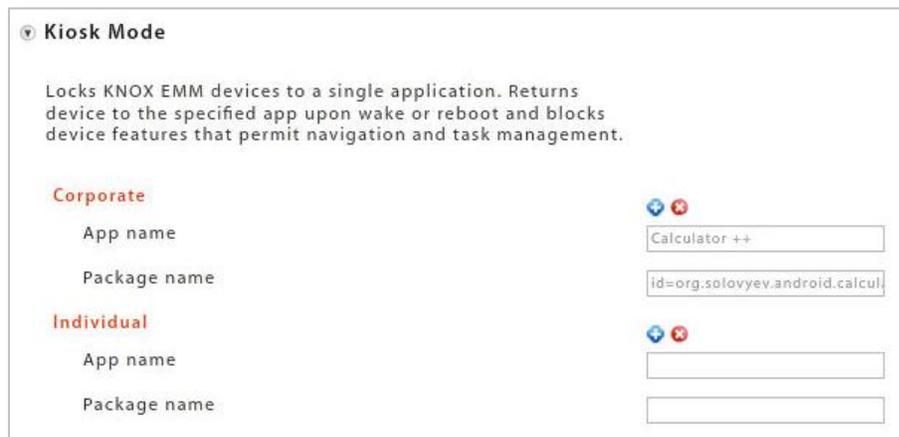
1. Add the app to the Android Managed Apps list. It must contain a *Package Name*. Select **Organization > Application Management > Managed Apps**.
2. From the dashboard, select **Organization > Policy Management > Policy Suites**.
3. From the panel, select **Samsung KNOX Device Policies**.
4. Select an app by clicking the blue plus symbol.



5. Select an app from the pop-up and click the **Update Assignment** button.



The *App name* and *Package name* will populate the Kiosk Mode fields.



To Remove the Kiosk Mode App

1. From the dashboard, select **Organization > Policy Management > Policy Suites**.
2. From the panel, select **Samsung KNOX Device Policies**.
3. Select an app by clicking the red x symbol.
4. Click **Yes** to confirm the deletion of the Kiosk Mode app.



Adding and Managing Apps for iOS Devices

Apple MDM functionality makes it possible for an administrator to manage the iOS applications in the Managed App list.

Management functionality includes:

- Installing/reinstalling/uninstalling apps at the user level
- Force pushing an app so that all users associated with a policy are automatically prompted to install
- Adding Enterprise (in-house) apps to the list
- Managing redemption codes associated with volume-purchased App Store applications.

In this section:

[Permissions for iOS Managed Apps](#)

[Adding iOS App Store Apps](#)

[Adding an iOS Enterprise App](#)

[Updating iOS App Versions](#)

[Assigning Apps to Individual Users](#)

[Assigning iOS Apps to LDAP Groups/Folders or Local Groups](#)

[Volume Purchase Program Apps](#)

[Managing Volume Purchase Program Licenses](#)

[Managing Volume Purchase Program Redemption Codes](#)

[Web Clips](#)

[Configuration File Format](#)

The screenshot shows the ZENworks Mobile Management console interface. The top navigation bar includes 'Activity Monitor', 'Users', 'Organization', 'Reporting', and 'System'. The user is logged in as 'admin@dc03.notify.net'. The main content area is titled 'Managed Apps > iOS' and 'Managed Apps for iOS devices'. It displays a table with 5 apps:

Name	Download Count	Download Limit	Categories	VPP	App File Name	App File Size (bytes)	iPad-Only	
Skype for iPhone	0	<Unlimited>	Productivity, Social Network	No		82664244	No	ht
UPS Mobile	0	<Unlimited>	Business, Productivity	No		50480765	No	ht
World Clock-Time	0	<Unlimited>	Productivity, Travel	No		20802454	No	ht
Pocket Scanner Cl	0	<Unlimited>	Business, Productivity	No		76004694	No	ht
FedEx Mobile	0	<Unlimited>	Business, Reference	No		9304183	No	ht

Below the table, there are sections for 'VPP Settings' (with a 'VPP Token' field and an 'Upload' button) and 'Managed App Description' (with a text input field).

Permissions for iOS Managed Apps

Several policy suite rules must be enabled for Managed iOS App functionality.

Select **Organization > Policy Management > Policy Suites > (select policy suites)**.

1. Choose the policy suite category **iOS Devices > Applications** and enable the following option:
 - **Allow app management** – Required for Force Push and administrator initiated app installations.
 - **Allow managed applications installation** – Required for Force Push and administrator initiated app installations.
 - **Allow iTunes** – Required for Force Push and administrator initiated App Store app installations.
2. If you want to use a Configuration File to configure a third party iOS application, verify that the following policy is enabled

Select **Organization > Policy Management > Policy Suites > (select policy suite) > iOS Devices > Management**. Enable:

- **Allow Management of Settings**

Adding iOS App Store Apps

If Managed Apps are accessed by users in different countries or regions, read this [Knowledge Base article](#).

1. Select **Organization > Application Management > Managed Apps**.
2. Select **iOS** from the left panel, then click **Add Managed App**.
3. Choose **App Store** as the Mobile app *Type*.
4. Choose **Search iTunes** or **Input Manually** as the *Method* by which to add the app.

If searching iTunes, enter a string to search on and the region in which the app is available, then click **Search**. . Select **iPad Only** if you need to search exclusively for iPad applications, then click **Search**.

The screenshot shows the 'Add Managed App' dialog box with the 'Search iTunes' method selected. The search results table is as follows:

App Name	Version	Price
Skype for iPhone	5.2.1	Free
InstaFrame - Photo Collage Editor, Pic Effects, Picture Frames	1.8.2	Free
Emoji 2 Emoticons for iOS 7 - New Free Smiley Symbols & Key	6.1	Free
Pic Joiner - Picture Collage, Camera Effects plus Photo Editor	1.9	Free
Color Text Messages+ for my sms,mms&iMessage free now	1.7	Free
Skype WiFi	1.4.1	Free

If adding manually, enter an **App Name**, **Version**, and **Description** for the app. What you enter is displayed on the device in the managed app list.

Enter the **App Store URL**. (The app URL can be obtained on iTunes by clicking the drop-down arrow below the app icon and selecting **Copy Link**.)

At the **Icon File** field, browse your image files and select an icon to associate with the application. This also displays on the device in the managed app list.

The screenshot shows the 'Add Managed App' dialog box with the 'Input Manually' method selected. The form fields are:

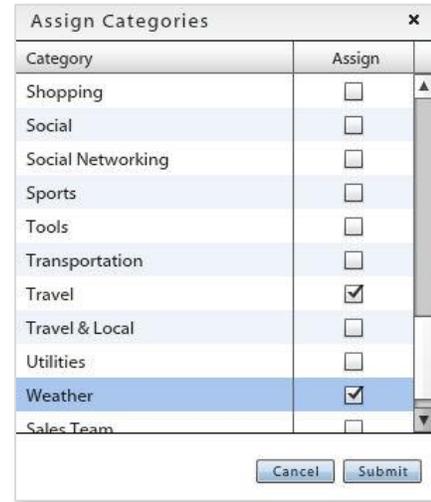
- Type: Enterprise App App Store
- Method: Search iTunes Input Manually
- Max File Size: 100 MB
- App Name: *
- Version: *
- Description: *
- App Store URL: *
- Icon File: *
- Recommended Max File Size: 100 KB
- Remove With MDM:
- Prevent Backup:
- Download Limit:
- Categories:
-

5. Select **Remove With MDM** if you want the app to be deleted from the device when the MDM configuration profile is removed.
6. Select **Prevent Backup** if you want the user to be able to save the app via iTunes.
7. Enter the **Download Limit** if you want to track downloads of a managed app purchased in bulk. Users can no longer download the app once the limit has been reached.

Download Limit and *Download Count* are shown in the *Managed Apps* grid and a compliance alert can be set for when availability or VPP licenses/redemption codes are low.

8. If you want to assign the app to an application category, click the **Add** button next to the **Categories** field.

If you want the app to inherit the categories in which it is found in iTunes, select **Yes** at the *iTunes Category* prompt and the categories will be pre-selected for you. Select **No** to mark the categories yourself.



9. Click **Add iOS App** to add the App to the iOS Managed App list.

Adding an iOS Enterprise App

An enterprise (or in-house) app is one that has been created by an organization by using development tools available through the Apple Developer Enterprise Program (iDEP).

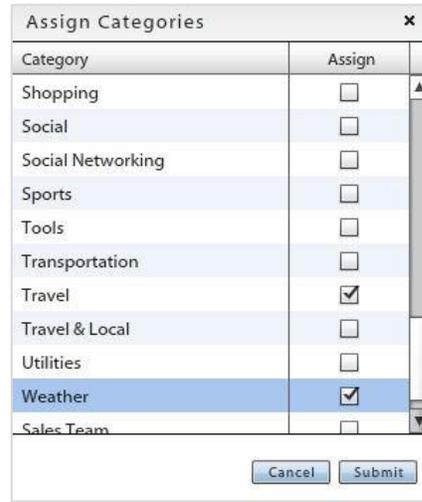
1. Select **Organization > Application Management > Managed Apps**.
2. Select **iOS** from the left panel, then click **Add Managed App**.
3. Choose **Enterprise App** as the mobile app **Type**.
4. Fill out the required fields of information, based on the location of the enterprise app.

Location of the Enterprise App	Manifest File Field	App File Field	Other Required Fields
Manifest and app files are on the <i>ZENworks Mobile Management</i> server	Select Upload File Upload the appropriate .plist file	Select Upload File Upload the appropriate .ipa file	Description
The manifest file is on the <i>ZENworks Mobile Management</i> server and the app file is contained within the manifest.	Select Upload File Upload the appropriate .plist file	Select Read from Manifest	Description, Icon File
Manifest and app files are hosted remotely	Select Provide URL Enter the Manifest URL	<i>Not Applicable</i>	App Name, Version, Description, Icon File

5. If an **Icon File** is required, browse your image files to select an icon to associate with the application.
6. Select **Remove With MDM** if you want the app to be deleted from the device when the MDM configuration profile is removed.
7. Select **Prevent Backup** if you want a user to be able to save the app via iTunes.
8. Enter the **Download Limit** if you want to track downloads of a managed app purchased in bulk. Users can no longer download the app once the limit has been reached.

Download Limit and *Download Count* are shown in the *Managed Apps* grid and a compliance alert can be set for when availability or VPP licenses/redemption codes are low.

- If you want to assign the app to an application category, click the **Add** button next to the **Categories** field. Mark the check boxes to assign categories. Click **Submit**.
- Click **Add iOS App** to add the app to the iOS Managed App list.



Assigning iOS Apps to Individual Users

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



Assigning iOS Apps to Members of LDAP Groups/Folders or Local Groups

You can assign iOS managed apps to all members of an LDAP group/folder or local group.

To assign iOS apps to all members of an LDAP group/folder or local group:

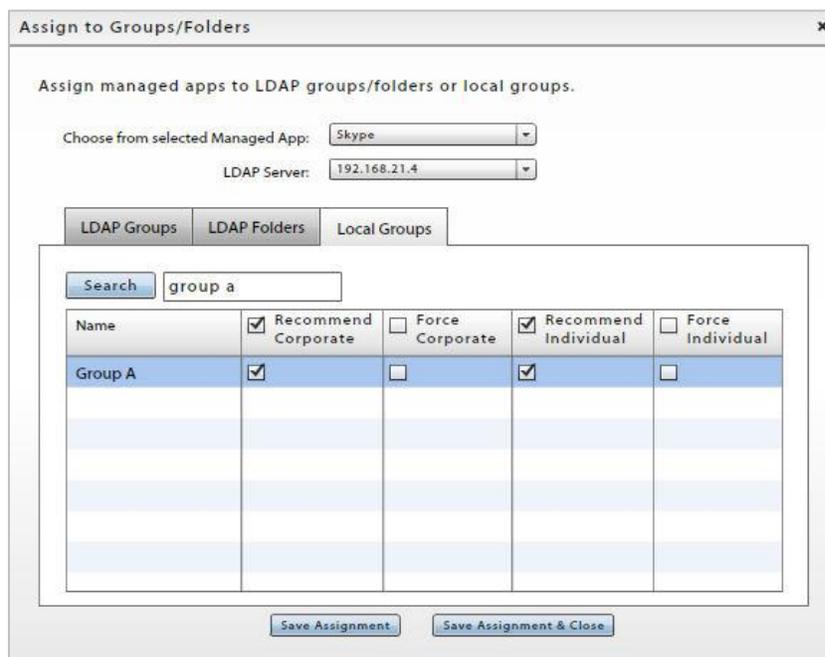
- From the *Managed Apps* data grid, select an app to assign to groups or use CTRL+click to select multiple apps.
- Click the **Assign to Groups/Folders** button on the action bar at the top of the page.



- From the *Managed App* drop-down, select an app to assign or select **All** to assign all apps selected from the Managed Apps data grid.



- If you are assigning apps to an LDAP group/folder, select a server from the **LDAP Server** drop-down.
- In the table, select the **LDAP Groups**, **LDAP Folders**, or **Local Groups** tab. You can search the groups by entering a value in the search box and clicking the *Search* button. The group *Name* column can be sorted by clicking the column header.



- In the group list, locate the group to which you are assigning the app(s) and determine whether or not the app(s) will be required on user devices.
 - Check the **Recommend** box to make the app(s) available to users in this group.
Or check the *Recommend* box in the header to make the app(s) available to users in all groups.
 - Check the **Force** box to force push the app(s) to devices. Users will be required to install the app(s). Checking this box will automatically mark the *Recommend* box as well.
Or check the *Force* box in the header to force push the app(s) to devices of all groups.

You must make this selection for corporate device and personal device users separately.

- Click **Save Assignment** before you make assignments for another group.
Click **Save Assignment & Close** when you are finished.

Updating iOS App Versions

Edit iOS App Information

Select an app from the grid and click the **Edit Managed App** button. Edit the original app information and click **Update iOS App**.

Update iOS App Versions

Select an app from the grid and click the **Update App on Devices** button above the grid to push the latest version of the app from the App Store to devices. Users will be prompted to update the app.

Managed Apps for iOS devices View: List

[Update App On Devices](#)

17 Apps

Name	Download Count	Download Limit	Categories	VPP	App File Name	App File Size (bytes)	iPad-Only
Twitter	0	<Unlimited>	Social Networking, Utilities	No		61013140	No
OneDrive	0	<Unlimited>	Productivity	No		6604783	No

Volume Purchase Program Apps

Apple's Volume Purchase Program (VPP), available in over 25 countries/regions, enables organizations to purchase applications in bulk. *ZENworks Mobile Management* provides an efficient way to distribute and manage those applications.

Enroll in the Apple VPP at:
<https://deploy.apple.com>

Other helpful VPP websites:
<http://www.apple.com/business/vpp/>
<http://www.apple.com/education/it/vpp/>

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

VPP apps have a status of **Yes** in the *VPP* column on the *Managed Apps* grid (*Organization > Application Management > Managed Apps*). The grid also displays the number of *Available Licenses* for each app.

Config File Name	Remove With GO!Enterprise MDM	Prevent Backup	Available Redemption Codes	Available Licenses	Region	Im
	Yes	Yes	0	99		
	Yes	Yes	0	198		
	Yes	Yes	0	0		
	Yes	Yes	0	0		
	Yes	Yes	0	0		
	Yes	Yes	0	999		
	Yes	Yes	0	497		
	Yes	Yes	0	1		
	Yes	Yes	0	1		
	Yes	Yes	0	1		

VPP Token Upload

An APNs certificate must be uploaded on the *Organization Settings* page before managing the VPP token. The VPP token will be deleted if the APNs certificate is removed.

1. Select **Organization > Application Management > Managed Apps**.
2. Select **iOS** from the left panel, then click the **Upload** button beside **VPP Token**.

Name	Download Count	Download Limit	Categories	VPP	App File Name	App File Size (bytes)	iPad-Only	ht
Skype for iPhone	0	<Unlimited>	Productivity, Social Network	No		79543078	No	ht
US Postage+	0	<Unlimited>	Utilities	No		313750	No	ht
World Clock-Time	0	<Unlimited>	Productivity, Travel	No		20802454	No	ht

VPP Settings
 VPP Token:

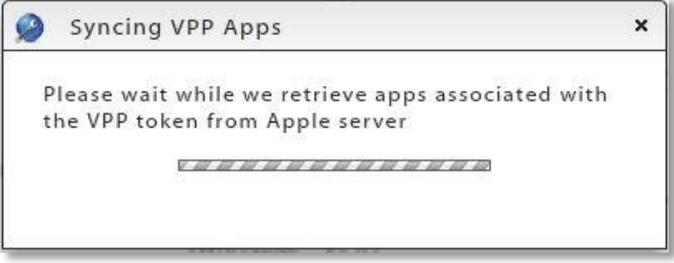
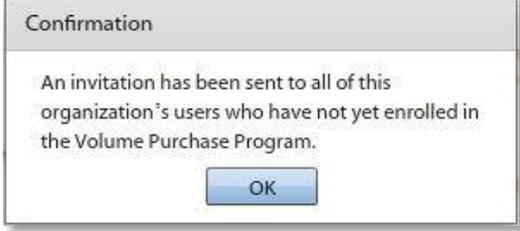
3. Assuming you have already signed in to Apple's web portal and downloaded your VPP token, click **Browse** to navigate to the location where the token is stored and select it.

4. Enter an E-mail address for communications about your VPP account.
5. Click **Submit**. Apps associated with the token are retrieved from the Apple server and the Managed Apps grid will begin to populate. Qualifying users are invited to join the VPP.
6. The *VPP Settings* appear after the token has been uploaded.
 - a. Configure *ZENworks Mobile Management* to poll the App Store for version updates to the VPP apps at a set interval. Enter a value in hours at **Check for Updates Every:**
 - b. If you want devices to be automatically updated when a new version is available for any VPP app, enable **Auto Update All VPP Apps on Devices**.

If you leave this disabled, you can use the **Auto Update on Devices** button, located under *VPP App Settings*, to automatically update individual apps.

VPP Settings	
VPP Token:	<input type="button" value="Edit"/> <input type="button" value="Remove"/> <input type="button" value="Sync Now"/> <input type="button" value="Invite Users"/>
VPP Token Organization Name:	Globo Mobile Technologies Inc
VPP Token Expiration Date:	Jul 14 2016 5:07PM
VPP Account E-mail:	jdoe@company.com
Check for Updates Every (Hours):	<input type="text" value="24"/> <input type="button" value="+"/> <input type="button" value="-"/>
Auto Update All VPP Apps on Devices:	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="NO"/>

Managing the VPP Token

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

Managing Volume Purchase Program Licenses

If you have uploaded an Apple VPP Token to the *ZENworks Mobile Management* server, all apps associated with the token populate the *Managed Apps* data grid and users with a qualifying device (running iOS 7.0.3 or higher) receive an invitation to join the Volume Purchase Program. See also [Organization Configuration and Management guide: VPP Token Upload](#).

VPP apps can be differentiated from other apps on the *Managed Apps* grid by the available licenses listed for the app and by looking at the app's status (*Yes*) in the column labeled *VPP*. The apps can be assigned to an individual user through their *Device Profile* or to groups of users via a Policy Suite, LDAP Group/Folder, or Local Group. While the user has the app, one license seat is occupied. (Users running iOS versions less than 7.0.3 will consume one redemption code when assigned a VPP app.)

When VPP app assignments are removed from the user device (and given it is the last iOS 7.0.3+ device associated with the user), they are also removed from the user's iTunes account and the VPP app license is reclaimed for reuse.

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

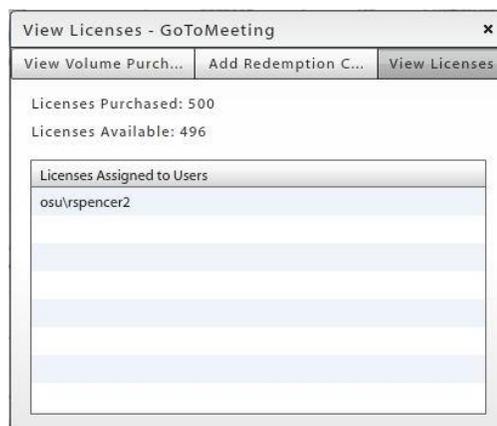
Note: The *Application Ratings* policy must be configured so that users can install VPP apps without having to enter their Apple ID credentials. From the Policy Suite, navigate to **iOS Devices > Ratings > Application Ratings** and select **Allow All**.

To View VPP License Counts:

1. Select the app and click **Manage Volume Purchase**.
2. Select the **View Licenses** tab.

The number of *Licenses Purchased* and *Licenses Available* are displayed. Users to which the licenses have been assigned are listed in the grid.

Note: Changes in the license count information will not show until the information has been processed and reported by the Apple server.



To Synchronize VPP Applications:

The MDM server automatically connects to the Apple server to retrieve the list of licenses associated with the VPP token when: a VPP token is added to the MDM server, a VPP token is edited, and each time you access the iOS section of *Managed Apps*.

You can also initiate this synchronization by clicking the **Sync Now** button under the VPP Settings section.



A message pops up on the screen while the retrieval is in progress:



Managing Volume Purchase Program Redemption Codes

For applications obtained through the Volume Purchase Program that carry redemption codes, add the redemption codes to the server. There will be one redemption code for every copy of the app purchased.

Apple's Volume Purchase Program is available in over 25 countries/regions. Redemption codes are different for each country, so you must add multiple sets of codes if you have purchased apps for users in more than one country.

When assigned a VPP app, users with devices running iOS versions less than 7.0.3 will consume one redemption code. Users running iOS 7.0.3 or higher will occupy a VPP app license.

To Add Redemption Codes:

1. Add the app to the iOS Managed App list.
2. Select the app, then click **Manage Volume Purchase**.
3. Select the **Add Redemption Codes** tab.

4. Select **Manual** or XLS (for XLS, proceed to step 6). If you are entering each code individually, choose **Manual**.

If you are entering each code individually, choose **Manual**.

Enter each code on a new line.

5. Click the **Add Redemption Codes** button.



Add Redemption Codes - Skype for iPhone

View Volume Purch... Add Redemption C... View Licenses

Add Redemption Code: Manual XLS

Enter Redemption Codes: *

Add Redemption Codes

6. Select **XLS** if you will enter multiple codes from a spreadsheet.

Browse to select the .xls file containing the redemption codes. The number of codes detected in the file displays.

There are volume purchase details at the top of the spreadsheet. Specify the column and row where the actual redemption codes begin.

7. Click the **Add Redemption Codes** button.



Add Redemption Codes - Skype for iPhone

View Volume Purch... Add Redemption C... View Licenses

Add Redemption Code: Manual XLS

Redemption Codes File: * Browse...

Number of Codes detected:

Redemption Code Column#: * 1

Redemption Code Row#: * 11

Redemption Code	Status

Add Redemption Codes

To View or Remove Redemption Codes:

1. Select an app from the iOS Managed App list, then click **Manage Volume Purchase**.
2. Select the **View Redemption Codes** tab.
3. Choose to view either the **Unused** or **Redeemed** codes.

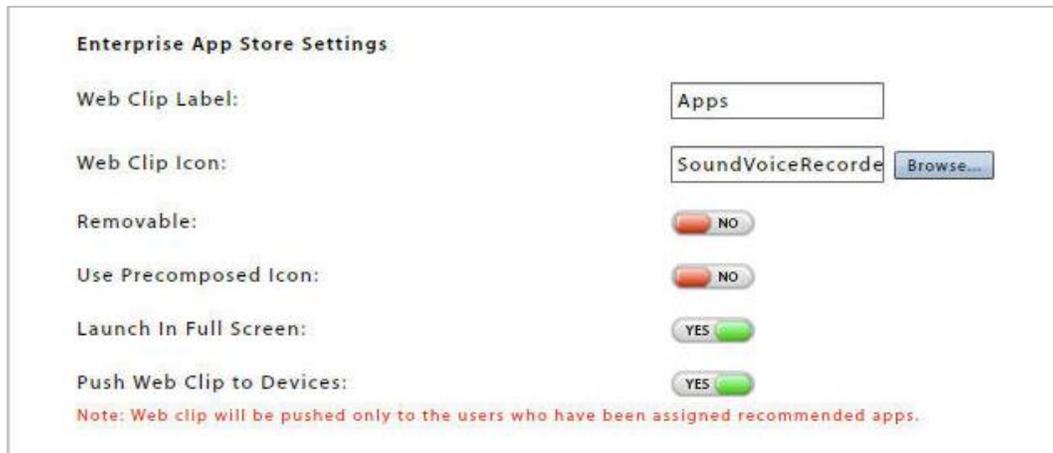
You can remove unused redemption codes from the list if necessary. Select one or more codes and click the *Removed Selected* button or click *Remove All* to delete all unused codes from the list.



Web Clips

Managed Apps can be pushed to iOS devices via a web clip. A web clip icon appears next to the *ZENworks Mobile Management* application on the device Home screen. Users access the **recommended app** list when they tap the icon. Required apps do not appear on the list.

Note: Users can also access the managed app list by opening the *ZENworks Mobile Management* application and tapping the **Apps** icon at the bottom of the screen. This list will include both required and recommended apps.



Web Clip Label	Label which appears bellows the web clip icon on users' devices.
Web Clip Icon	Browse to select your own icon for the web clip.
Removable	Determines whether or not users will be permitted to remove the icon.

Use Pre-composed Icon	Use the pre-composed web clip icon (<i>ZENworks Mobile Management</i> logo) instead of selecting your own.
Launch in Full Screen	Determines whether the Managed App list will launch in full screen mode.
Push Web Clip to Devices	This must be enabled in order to push the web clip to devices. The web clip is only pushed to users who have been assigned recommended apps.

Configuration File Management

Format

If you are using a **Configuration File** to configure a third party app, the file should follow the general format displayed here:

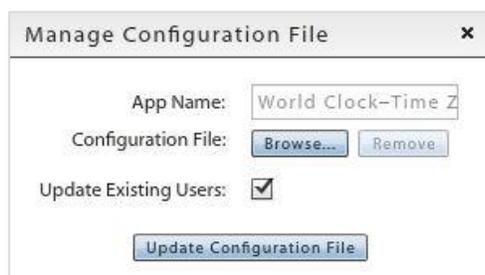
General Format	Example
<pre><dict> <key>key1</key> <string>value1</string> <key>key2</key> <string>value2</string> </dict></pre>	<pre><dict> <key>username</key> <string>username</string> <key>password</key> <string>password</string> </dict></pre>

Since tags and values will be specific to each app, you should contact the app developer for a suitable file.³

Applying the Configuration File

If you are using a configuration file to configure a third party iOS app, select an app from the *Managed Apps* grid and click the **Manage Configuration File** button on the action bar at the top of the page.

Click the **Browse** button and select your configuration file.



Adding Managed Apps for BlackBerry Devices

1. Select **Organization > Application Management > Managed Apps**.
2. Select **BlackBerry** from the left panel, then click **Add Managed App**.



App Name: *

Icon File: *
Recommended Max File Size: 100 KB

Link to App: *

Version: *

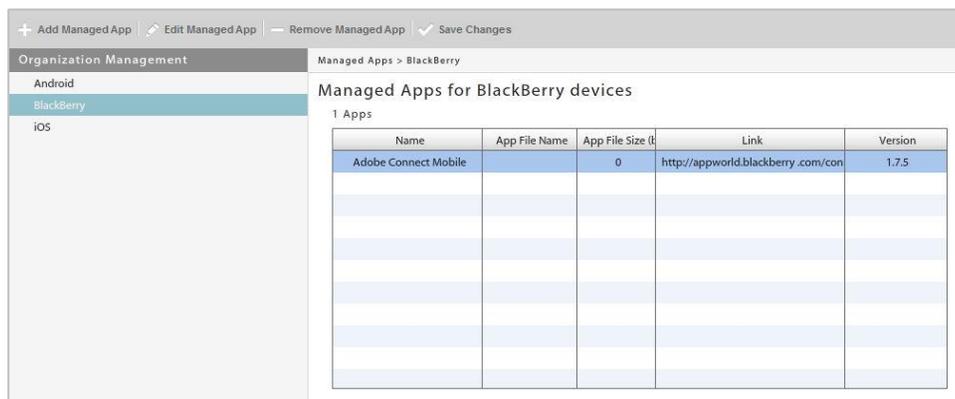
Description: *

Add Apps for BlackBerry

3. Enter a **Name**, **Version**, and **Description** for the app. What you enter displays on the device.
4. Browse your image files in the **Icon File** field to associate an icon with the application. This also displays on the device.
5. Provide the application store URL in the **Link to App** field.
6. Click the **Add App** button.

In the dashboard, there is an app list grid for each device type. Select the device type from the left panel to view the list to which the app was added.

You can select an individual app from a grid and click the **Edit Managed App** or **Remove Managed App** button to edit or delete an app.



Organization Management

Managed Apps > BlackBerry

Managed Apps for BlackBerry devices

1 Apps

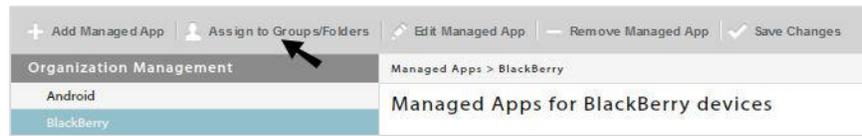
Name	App File Name	App File Size (B)	Link	Version
Adobe Connect Mobile		0	http://appworld.blackberry.com/con	1.7.5

Assigning BlackBerry Apps to Members of LDAP Groups/Folders or Local Groups

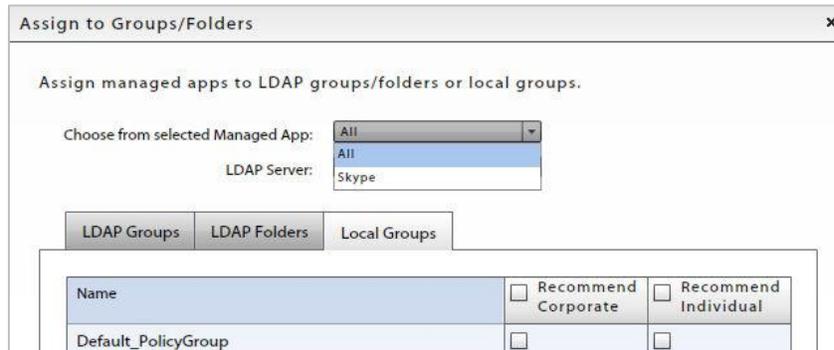
You can assign BlackBerry managed apps to all members of an LDAP group/folder or local group.

1. From the *Managed Apps* data grid, select an app to assign to groups or use CTRL+click to select multiple apps.

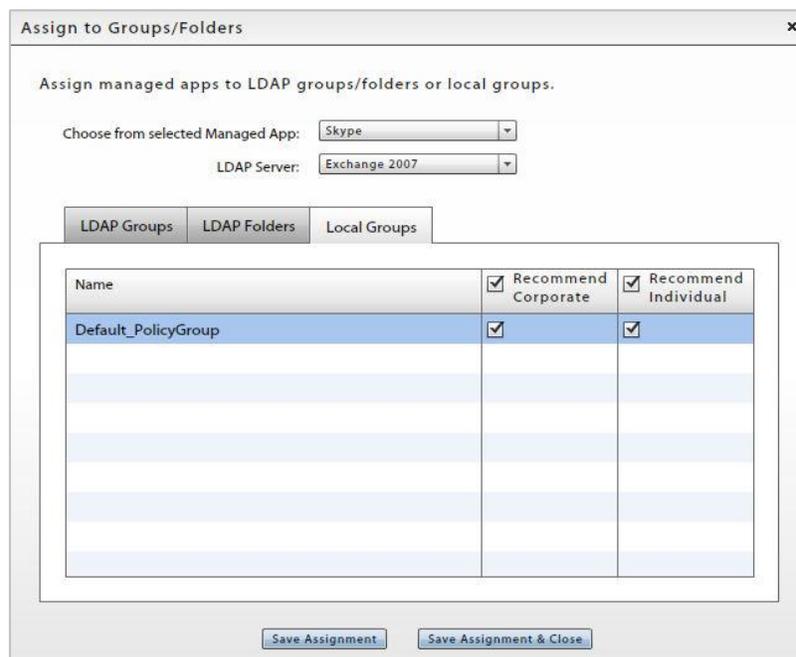
- Click the **Assign to Groups/Folders** button on the action bar at the top of the page.



- From the *Managed App* drop-down, select an app to assign or select **All** to assign all apps selected from the Managed Apps data grid.



- If you are assigning apps to an LDAP group or folder, select a server from the **LDAP Server** drop-down.
- In the table, select the **LDAP Groups**, **LDAP Folders**, or **Local Groups** tab.



- In the group list, locate the group to which you are assigning the app(s) and determine whether the app(s) will be recommended for Corporate or Individual owned devices or both.
- Click **Save Assignment** before you make assignments for another group. Click **Save Assignment & Close** when you are finished.

Novell Filr

Novell Filr, a secure system for mobile file access and sharing, is integrated with *ZENworks Mobile Management* for Android devices or iOS devices running iOS 7.1 or higher and Novell Filr app version 1.0.4 or higher. *ZENworks Mobile Management* ensures that only tracked, managed, and authorized devices can access Novell Filr. The Filr app itself can be uploaded to devices via the *ZENworks Mobile Management Managed Apps*. The integration gives you the ability to create a configuration profile from the *ZENworks Mobile Management* dashboard that, when assigned to users, will configure the Novell Filr app on devices. The profile also allows you to limit the following functions for secure files:

- **Disable cut and copy** – Use this option to ensure that users do not circumvent Filr sharing limitations by cutting and copying file content.
- **Disable Screen Capture** – Use this option to ensure users do not circumvent Filr sharing limitations by taking screen shots of file content.
- **Disable Open-in** – Ensure that users do not open a secure file in a non-secure application.
- **Whitelist applications** – Limit users so that they can only open secure files in the applications you have whitelisted.

Assigning the Profile. Novell Filr profiles can be assigned to individual users (see [Adding Users Guide](#)) or to groups of users via LDAP groups/folders (see [Organization Configuration Guide](#)) or [local groups](#), or as organization default settings (see [Organization Configuration Guide](#)).

Note: 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.

Configuration. The Novell Filr server and the *ZENworks Mobile Management* server must be configured so that user credentials are the same on each server.

To create a Novell Filr configuration

1. From the dashboard, select **Organization > Application Management > Novell Filr**.
2. Click **Add New Novell Filr**.

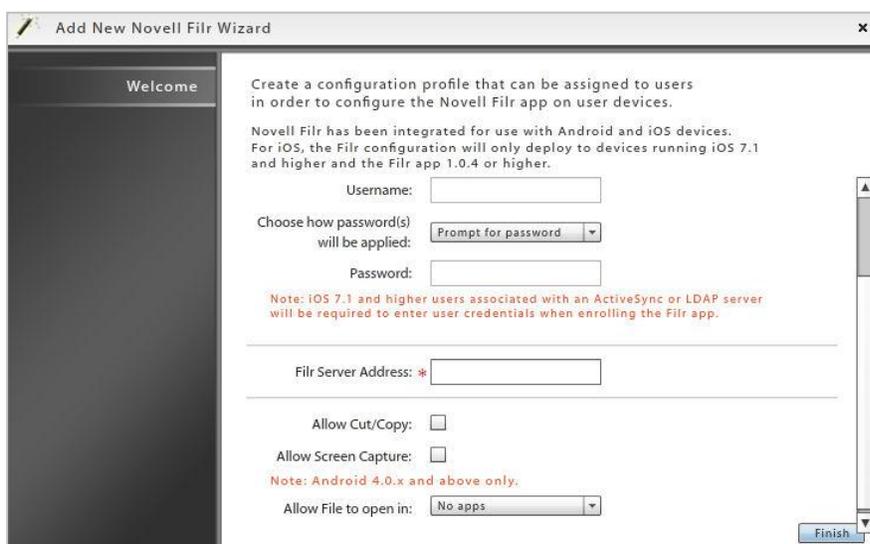
3. Enter a **Display Name** for the profile.
4. Determine how usernames will be applied:
 - Prompt for username – Prompt the user to enter a username.
 - Enter generic username – Enter a generic username in the **Username** field.
 - Use ZMM username – Apply the username used for authentication with ZENworks Mobile Management.

Note: iOS 7.1 or higher users associated with an ActiveSync or LDAP server will be required to enter user credentials when enrolling the Filr app, regardless of what is chosen here.

5. Determine how user passwords will be applied:
 - Prompt for password – Prompt the user to enter a password.
 - Enter generic password – Enter a generic password in the **Password** field.
 - Use ZMM password – Apply the password used for authentication with *ZENworks Mobile Management*.

Note: iOS 7.1 or higher users associated with an ActiveSync or LDAP server will be required to enter user credentials when enrolling the Filr app, regardless of what is chosen here.

6. Enter the **Filr Server Address**. You might need to enter the address in the format, serveraddress:port
7. Set additional security options.
 - **Allow Cut/Copy** – Leave this unchecked to ensure that users do not circumvent Filr sharing limitations by cutting and copying file content.
 - **Allow Screen Capture** – Leave this unchecked to ensure users do not circumvent Filr sharing limitations by taking screen shots of file content. *(Applicable only for Android devices running OS 4.0.x or higher.)*
 - **Allow File to open in** – Ensure that users do not open a secure file in a non-secure application by selecting **No apps**, or choose **Whitelisted apps** and designate the application in which they are permitted to open secure file.



Allow File to open in: Whitelisted apps only

Whitelisted Android Apps:

App Name	Package Name
TouchDown	8.1.00012

Whitelisted iOS Apps:

App Name	App Identifier
Task Manager +	com.appmedia.NoteApp
File Manager Pro App	de.zuhanden.filemanager

Buttons: Add, Edit, Remove

8. Click **Finish**.

Whitelists/Blacklists

Blacklists enable the administrator to create a list of character strings that filter blacklisted applications on Android and iOS devices. When one or more blacklisted applications are installed on a device, the user's access to email, shared files, app lists, or other organization resources can be blocked. You will specify these restrictions using the Compliance Manager.

Whitelists enable the administrator to create a list of strings that filter applications on Android and iOS devices. When one or more applications are installed on a device that are not on the whitelist a user's access to email, shared files, app lists, or other organization resources can be blocked. You will specify these restrictions using the Compliance Manager.

Android KNOX Devices. On Android KNOX devices, Blacklist/Whitelist restrictions will prevent apps that do not meet the criteria from being installed on the device.

On Android KNOX Workspace devices, Blacklist/Whitelist restrictions will prevent apps that do not meet the criteria from being installed in the Workspace container. Workspace devices require KNOX v2.0.

Apps installed on a device, prior to restrictions being applied, cannot be restricted.

So that they are informed about which apps should not be installed, users can view the blacklist and whitelist filters via the *ZENworks Mobile Management* app on their device or the Self-Administration portals.

Add Strings to the Blacklist/Whitelist

First, create the list of strings. Select **Organization > Application Management > Whitelists/Blacklists > Blacklists** or **Whitelists**.

Choose to add a filter string that will match against **App Names** or **App Identifiers**. *App Identifier* is the ID the application's developer has assigned to the app.

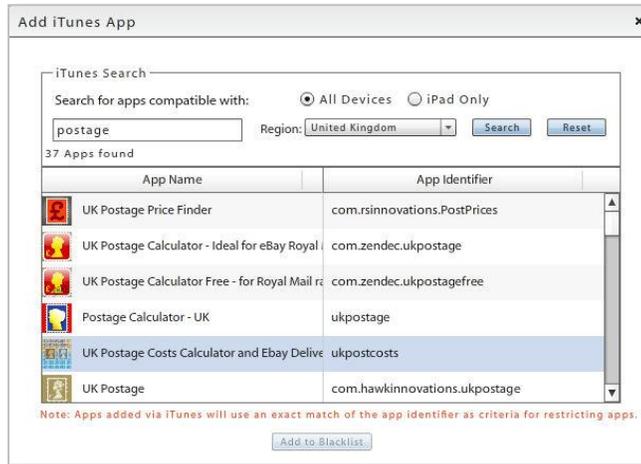
Choose *containing* or *exactly matching* from the drop-down list, then enter a string and click the **Add** button.

Note: An exact match of the app identifier must be provided for apps to be restricted on Android KNOX compatible devices.

App Name	App Identifier	Method	Type
Angry Birds		Containing	Manual
poker		Containing	Manual
iBooks		Exactly Matching	Manual
Pandora Radio	com.pandora	Exactly Matching	iTunes
SoundHound	com.melodis.soundhound.free	Exactly Matching	iTunes

Add iOS Apps to the Blacklist/Whitelist via an iTunes Search

You can also select iOS apps for the list by searching and selecting from iTunes. Click the **Add by iTunes Search** button. Enter a string to search on and the region in which the app is available. Select *iPad Only* if you need to search exclusively for iPad applications, then click **Search**. Apps added in this way are matched against their *App Identifier*.



Activating a Blacklist or Whitelist

Blacklists or Whitelists will not affect users until the *Restricted App Permissions* and the Blacklist or Whitelist Compliance Restriction option have been enabled.

Enable the Whitelists/Blacklists Permissions. Once the list is created, enable the *Blacklist Permissions* in the policy suite(s). Select *Organization > Policy Management > Policy Suites > (expand a policy suite) > Whitelists/Blacklists Permissions*. Enable either the Blacklist or Whitelist permissions. You cannot enable the Blacklist and Whitelist simultaneously.

Note: When you enable either the blacklist or the whitelist permission, the **Record installed applications** option (under the policy suite category *Audit Tracking*) is automatically enabled. This option must remain enabled in order to monitor application usage.



Enable the Blacklist or Whitelist Restriction Compliance Option. Set the blacklist restrictions using the Compliance Manager. Select *Organization > Compliance Manager > Access Restrictions > Restriction Options*. Under *Access Restrictions*, enable the **Restrict when Blacklist App detected** option or the **Restrict when non-Whitelist App detected** and select the restrictions.

Restrict when Blacklist App detected YES

No configurable options.

Restrict the following resources when this access restriction is violated:

ActiveSync	iOS corporate resources	<input type="checkbox"/> Select All iOS	Android corporate resources
<input checked="" type="checkbox"/> ActiveSync Connections	<input checked="" type="checkbox"/> Access Point Name	<input type="checkbox"/> Provisioning Profiles	<input checked="" type="checkbox"/> VPNs
ZENworks corporate resources	<input checked="" type="checkbox"/> CalDAV Servers	<input type="checkbox"/> Subscribed Calendars	<input checked="" type="checkbox"/> Wi-Fi Networks
<input checked="" type="checkbox"/> File Share	<input checked="" type="checkbox"/> CardDAV Servers	<input checked="" type="checkbox"/> VPNs	
<input checked="" type="checkbox"/> Managed Apps	<input checked="" type="checkbox"/> Exchange Servers	<input type="checkbox"/> Web Clips	
	<input checked="" type="checkbox"/> LDAP Servers	<input checked="" type="checkbox"/> Wi-Fi Networks	
	<input checked="" type="checkbox"/> Mail Servers		

OR

Restrict when non-Whitelist App detected YES

No configurable options.

Restrict the following resources when this access restriction is violated:

ActiveSync	iOS corporate resources	<input type="checkbox"/> Select All iOS	Android corporate resources
<input checked="" type="checkbox"/> ActiveSync Connections	<input checked="" type="checkbox"/> Access Point Name	<input checked="" type="checkbox"/> Provisioning Profiles	<input checked="" type="checkbox"/> VPNs
ZENworks corporate resources	<input checked="" type="checkbox"/> CalDAV Servers	<input type="checkbox"/> Subscribed Calendars	<input checked="" type="checkbox"/> Wi-Fi Networks
<input checked="" type="checkbox"/> File Share	<input checked="" type="checkbox"/> CardDAV Servers	<input checked="" type="checkbox"/> VPNs	
<input checked="" type="checkbox"/> Managed Apps	<input checked="" type="checkbox"/> Exchange Servers	<input type="checkbox"/> Web Clips	
	<input checked="" type="checkbox"/> LDAP Servers	<input checked="" type="checkbox"/> Wi-Fi Networks	
	<input checked="" type="checkbox"/> Mail Servers		

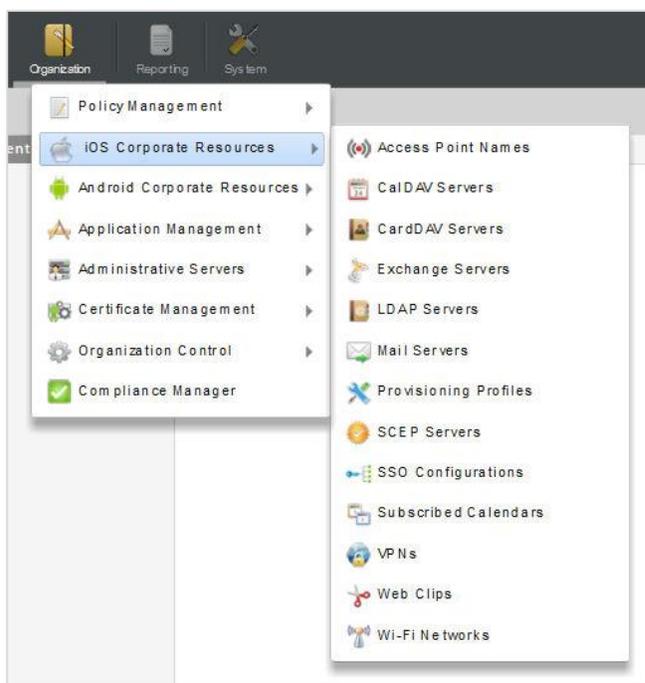
Corporate Resource Management

Corporate Resources refer to servers, networks, and other resources which are available to iOS and Android users. They include resources such as, LDAP and mail servers, Wi-Fi and VPN networks, or Provisioning Profiles, Subscribed Calendars and Web Clips.

Use the resource tools in the dashboard's **Organization** view to define credentials for the server and network resources. Then use the resources in the *Device Profile* to associate iOS or Android device users with a resource and configure user account settings to push out to devices.

You can also make resource assignments to members of LDAP groups or folders from these options. User credentials are obtained from the LDAP server, thus saving the administrator from having to make resource assignments per individual user.

Android devices currently support only VPN and Wi-Fi Network resources.



iOS Corporate Resources



Android Corporate Resources

Assigning Corporate Resources to Users

Corporate resources can be assigned to individual devices through the Device Profile. See [Corporate Resource Assignments](#).

You can also assign corporate resources via an LDAP group or folder. Choose the resources for a group or folder. Users are then assigned resources based on their LDAP group/folder association. This can be accomplished from the User/Device Grid or from the [resource management page](#).

iOS Resource Expiration (iOS 6+ devices)

Any iOS resource (with the exception of SCEP Servers) can be configured to expire on a given date or after an interval of time. A user whose iOS 6+ device has been assigned the resource can access it only until it expires.

- Date expirations occur at the beginning of the designated day (12:00 a.m.).
- Interval expirations occur at the end of the day (11:59 p.m.) after the interval has elapsed. For example, a resource available for 5 days will expire at 11:59 p.m. on the fifth day.

If you update the expiration of a resource and save the changes, you can choose to reload the existing installed resources, which will reset the expiration date on devices.

Connection Testing

Use the **Test Now** button on the server screens to test the general connectivity of the server after you initially add it or if you suspect there is a connection problem. These servers are accessed by devices, not the *ZENworks Mobile Management* server, so these tests merely verify that the server has a port open to authorized users.

Server	Tests:	Credentials entered for the test
Mail Servers	-General connectivity; -Accessibility by an authorized user	User name and Password of an active user on the mail server
Exchange Servers	-General connectivity; -Accessibility by an authorized user; -Autodiscover	A set of active user credentials in the format required by the Exchange server.
LDAP Servers	-General connectivity; -Accessibility by an authorized user	User name and Password of an active user on the LDAP server
SCEP Servers	-General connectivity	None
CalDAV Servers	-General connectivity; -Accessibility by an authorized user	User name, Password, and Principal Address of an active user on the CalDAV server
CardDAV Servers	-General connectivity; -Accessibility by an authorized user	User name, Password, and Principal Address of an active user on the CardDAV server
Subscribed Calendars	-General connectivity; -Accessibility by an authorized user	User name and Password of an active user of Subscribed Calendars

Resource Configurations

You can define the following servers and networks:

Resource	Description	Devices that Support
Access Point Names (APN)	<p>The Access Point Name identifies the external cellular network a phone accesses for data. When you configure a new APN, you must have the correct settings for the carrier and type of account provisioning. Incorrect settings can result in a loss of functionality or additional charges.</p> <p>Reasons you may need to assign a new APN:</p> <ul style="list-style-type: none"> • The APN settings are incorrect and user is getting error messages. • You are assigning a different carrier's APN to a user with an unlocked phone. • A user is traveling outside of the wireless provider's service area and needs a different APN to avoid data roaming charges. 	iOS
CalDAV Servers	Define your corporate CalDAV servers. Then associate a user with the server and configure calendar account settings to push out to the user's device.	iOS
CardDAV Servers	Define your corporate CardDAV servers. Then associate a user with the server and configure contact account settings to push out to the user's device.	iOS
Exchange Servers	Define your corporate Exchange server or server utilizing the Exchange ActiveSync protocol servers. Then associate a user with the server and configure ActiveSync account settings to push out to the user's device.	iOS
LDAP Servers	<p>Define your corporate LDAP server(s). Then associate a user with the server and configure LDAP settings to push out to the device so the user can access corporate directory information via the device.</p> <p>LDAP searches can be added to limit the number of users pulled from the LDAP server. Specify the Base DN and search scope, so that only users belonging to a specified group are queried.</p>	iOS
Mail Servers	Define your corporate mail servers. Then associate a user with the server and configure email account settings to push out to the user's device.	iOS
Provisioning Profiles	Define and upload provisioning profiles that enable iOS device users to install in-house iOS apps. You can push out a provisioning profile to individual users or check <i>Apply to Organization</i> to assign to all iOS device users in the organization.	iOS
SCEP Servers	Define your Simple Certificate Enrollment Protocol (SCEP) server(s). Then associate a 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. See SCEP Servers for more information.	iOS
SSO Configurations	<p>Define the Single Sign On configuration. From the Device Profile page, assign the configuration to a user so that it is pushed to the device during enrollment.</p> <p>Single Sign On (SSO) is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.</p>	iOS
Subscribed Calendars	Define the subscribed calendars you want to push out to iOS devices. These are read-only calendars that use the iCalendar (.ics) format. Calendars are obtained	iOS

	from calendar-based services that support calendar subscriptions, including iCloud, Yahoo, Google, and the Mac OS x iCal application.	
VPNs (Android)	<p>Define your VPN networks.</p> <p>Instruct users to download and install the third party app, available through the Google Play Store (or add to your <i>Managed Apps</i> list), required for the VPN connection type. Then associate a user with the VPN network and define the wireless network credentials to push out to the user's device.</p> <p>Supported connection types are:</p> <ul style="list-style-type: none"> • Cisco AnyConnect • F5 SSL <p>Note: Users installing Cisco AnyConnect should enable <i>External Control</i> in the app's settings prior to receiving a VPN assignment from the <i>ZENworks Mobile Management</i> server. If enabled after the assignment is sent, they must use the <i>VPN Settings</i> in the <i>ZENworks Mobile Management</i> settings to establish the connection.</p>	Android (OS 4.0+)
VPNs (iOS)	<p>Define your VPN networks.</p> <p>Instruct users to download and install the third party app, available through the App Store or iTunes (or add to your <i>Managed Apps</i> list), required for the VPN connection type. Then associate a user with the VPN network and define the wireless network credentials to push out to the user's device.</p> <p>Supported connection types are:</p> <ul style="list-style-type: none"> • IPSec (Cisco) • Cisco AnyConnect • Juniper SSL • F5 SSL • SonicWALL Mobile Connect • Aruba VIA • Checkpoint Mobile VPN • OpenVPN <p>Note: IPSec does not require a device application.</p>	iOS
Web Clips	Define shortcuts to a specific web application or web page that can be pushed to users' device Home screen. When a user taps the web clip, the web browser automatically launches and takes the user to that application or page.	iOS
Wi-Fi Networks	Define your Wi-Fi networks using various levels of security, including WEP, WPA, and WPA2. Then associate a user with the Wi-Fi network and define the wireless network credentials to push out to the user's device. Enterprise certificate authority certificates can be associated with these resources.	iOS, Android

Configuring Server Settings

The credentials for each server are defined using a wizard:

Mail Servers	Exchange Servers	LDAP Servers	CalDAV Servers	CardDAV Servers
-Email Server Type	-Exchange Server Name	-LDAP Display Name	-Display Name	-Display Name
-Account Name	-Exchange Server Address	-LDAP Server Address	-Server Address	-Server Address
-Server Address	-Exchange Port	-LDAP Port	-Server Port	-Server Port
-Server Port	-Use SSL	-Use SSL	-Use SSL	-Use SSL
-Use SSL	-Use S/MIME	-LDAP Searches	-Expiration (iOS 6+)	-Expiration (iOS 6+)
-Allow Move	-Allow Move	-Expiration (iOS 6+)		
-Account Type	-Use Only in Mail			
-IMAP Path Prefix	-Allow Recent Address Syncing (iOS 6+)			
-Authentication Type	-Expiration (iOS 6+)			
-Expiration (iOS 6+)				

Sample Add New Server Wizard

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

- **Allow Move** – When disabled, this option prevents an iOS 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** – When enabled, this option prevents an iOS 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 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.

- **Allow Recent Address Syncing (iOS 6+)** – When enabled, recently used email addresses are stored on the device. They will then appear in a selection list if the user begins to type the address in a subsequent email.

Configuring Network Settings

The credentials for each network are defined using a wizard.

Wi-Fi Networks (iOS) -Resource Name -SSID -Auto Join -Hidden Network -Security Type -Password -Password Per Connection -Accepted EAP Types	-EAP-FAST -Allow Trust Exceptions -Inner Identity -Proxy Type -Proxy Address, Port, Username, Password -Expiration (iOS 6+) -Certificate Authority Certificate Template	VPNs (iOS) <i>Settings vary based on connection type</i> -Display Name -Connection Type -User Authentication -Remote Address -Proxy Type -Expiration (iOS 6+)	Wi-Fi Networks (Android) -Resource Name -SSID -Hidden Network -Security Type -WPA/WPA2 Password -WEP Key -EAP Method -Phase2 Authentication -Certificate Authority -Certificate Template	VPNs (Android 4.0+) <i>Cisco AnyConnect or F5 SSL</i> -Display Name -Connection Type -Remote Address
---	--	---	---	---

Sample Add New Network Wizard

Configuring Other Resources

Access Point Names	Provisioning Profiles	SSO Configurations	Subscribed Calendars	Web Clips
-Access Point Name	-Display Name	-Name	-Display Name	-Label
-Proxy	-Provisioning Profile	-Realm	-Host Name	-URL
-Proxy Port	-Apply to Organization	-URL Prefix Matches	-Use SSL	-Icon
-Expiration (iOS 6+)	-Expiration (iOS 6+)	-App Identifier Matches	-Expiration (iOS 6+)	-Removable
		-Expiration (iOS 6+)		-Use Precomposed Icon
				-Launch in Full Screen
				-Expiration (iOS 6+)

Access Point Name Wizard

Provisioning Profile

Subscribed Calendar Wizard

Web Clip Wizard

Add New SSO Configuration [x]

Welcome

Single Sign On configurations assigned to users are pushed to the device during enrollment. Applications that connect to the corporate network can utilize the single sign on configuration and avoid prompting users for username/password.

Name: *

Realm: *

URL Prefix Matches: * **Add**

URL Prefix	Remove	Rename
<input type="text"/>	<input type="button" value="Remove"/>	<input type="button" value="Rename"/>
<input type="text"/>		

App Identifier Matches: **Add**

Application Identifier	Remove	Rename
<input type="text"/>	<input type="button" value="Remove"/>	<input type="button" value="Rename"/>
<input type="text"/>		

Expiration (iOS 6+) ▾

Finish

SSO Configuration

Assigning Resources to LDAP Groups and Folders

When the Administrative LDAP server is fully configured, corporate resources can be assigned to users via the LDAP group or folder to which they belong. User credentials are obtained from the LDAP server, thus saving the administrator from having to make resource assignments per individual user.

You can also assign resources directly from the User/Device Grid. See [Assigning Settings and Resources to LDAP Groups/Folders](#).

Note: These methods cannot be used to assign the SCEP server resource to users, because of the unique challenge code required for each user.

From the *Organization* view, select a resource from the *Android* or *iOS Corporate Resource* drop-down menu option. Click the option, **Assign to LDAP Groups/Folders**.

The screenshot shows the 'Exchange Servers' configuration page for 'Exchange 2013'. The 'Assign to LDAP Groups/Folders' option is highlighted in the top navigation bar. The configuration fields are as follows:

Exchange Server Name:	Exchange 2013	Expiration (iOS 6+):	Never
Exchange Server Address:	ex13.zmm.net		
Exchange port:	80		
Use SSL:	<input type="checkbox"/>		
Use S/MIME (iOS 5+):	<input type="checkbox"/>		
Allow Move (iOS 5+):	<input checked="" type="checkbox"/>		
Use Only in Mail (iOS 5+):	<input type="checkbox"/>		
Allow Recent Address Syncing (iOS 6+):	<input checked="" type="checkbox"/>		
Server Connectivity:	<input type="button" value="Test Now"/>		

1. Select an **LDAP Server** from the drop-down list.
2. Some resources have an option to **Use credentials from the LDAP Server**.
 - Keep the option checked to use credentials from LDAP.
 - Disable this option and enter the user authentication token(s) necessary for your Enterprise setup. Acceptable entries may include {domain}, {username}, or {emailaddress} or a combination of tokens such as, {domain}\{username}.
 - Disable this option to assign a resource to a group email address, then enter the shared User Name or shared User Name and Email Address. The assignment is made to that mail account only.
3. Click the *Groups* or *Folders* tab and navigate through the LDAP directory to select the groups or folders to which you will assign the resource.
4. Click the **Update Assignments** button.

The screenshot shows the 'Assign to LDAP Groups/Folders' dialog box. It contains the following elements:

- Header: Assign to LDAP Groups/Folders
- Message: Choose the folders/groups to which you wish to assign the resource Exchange 2013.
- Note: Users without an email address cannot be assigned this resource.
- LDAP Server: Exchange 2003
- Use credentials from LDAP Server:
- User Name:
- E-mail Address:
- Groups/Folders tabs: Groups (selected), Folders
- Table with columns: Assigned, Imported LDAP Groups
- Table content:

Assigned	Imported LDAP Groups
<input type="checkbox"/>	Domain Guests
<input type="checkbox"/>	HelpServicesGroup
<input type="checkbox"/>	
<input type="checkbox"/>	
- Update Assignments button

Assigning Network Resources to Local Groups

Several resources can be assigned to users via the local group to which they belong. For network resources (Wi-Fi networks and VPNs), user credentials are obtained from the *ZENworks Mobile Management* server, thus saving the administrator from having to make resource assignments per individual user.

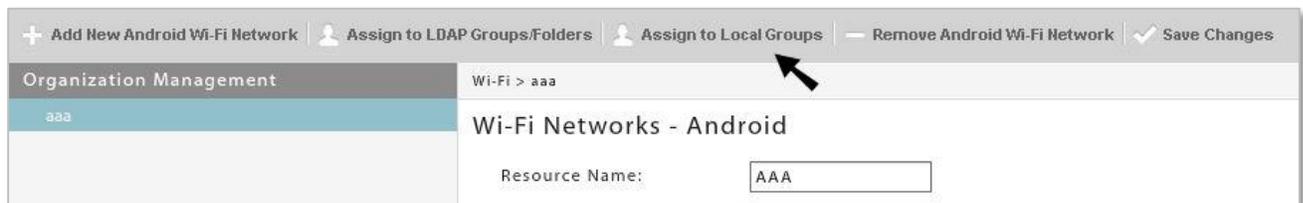
The following resources can be assigned to local groups:

- Android Wi-Fi
- iOS Wi-Fi
- iOS VPNs
- iOS Web Clips

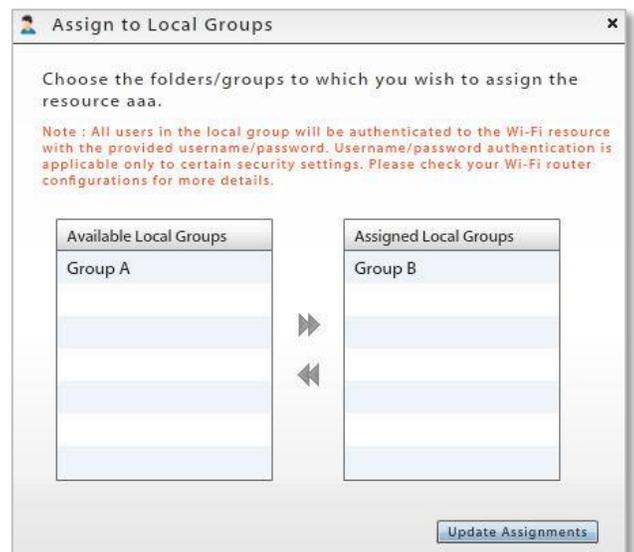
To Assign Android or iOS Wi-Fi Resources

Note: Wi-Fi network resources that have an enterprise security type cannot be assigned to a local group.

1. From the *Organization* view, select the Wi-Fi resource from either the *Android* or *iOS Corporate Resource* option. Click the option, **Assign to Local Groups**.

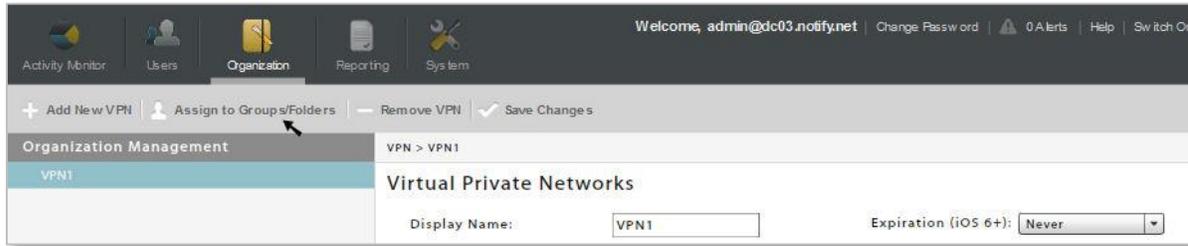


2. Click to select a local group from the *Available* column.
3. Click the right arrow to move that group to the *Assigned* column. Groups in this column will be assigned the resource.
4. Click the **Update Assignments** button.

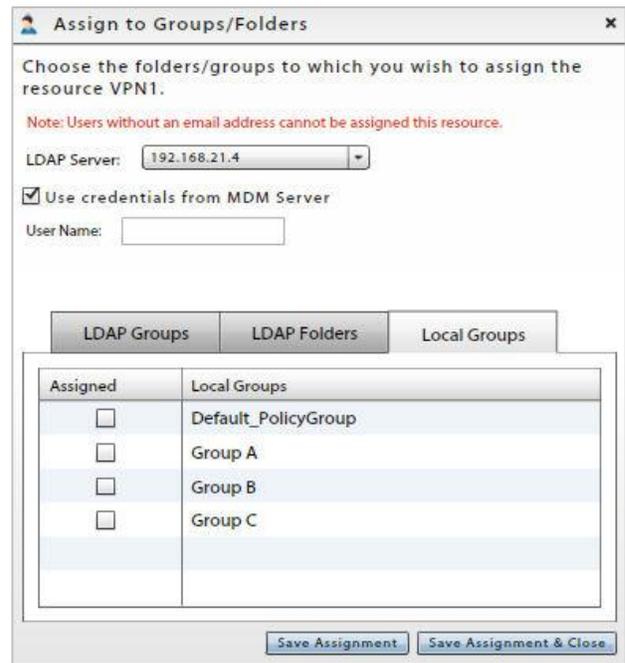


To Assign iOS VPN or iOS Web Clip Resources

1. From the *Organization* view, select the *VPN* or *Web Clips* resource from the *iOS Corporate Resource* option. Click the option, **Assign to Groups/Folders**.



2. If you are assigning a VPNs, check the box to **Use credentials from the MDM server** or enter an individual user in the **User Name** field.
3. Select the **Local Groups** tab.
4. Check the box beside each group to which you are assigning the resource.
5. Click **Save Assignment & Close**.



Simple Certificate Enrollment Protocol (SCEP) Servers

What is SCEP?

Simple Certificate Enrollment Protocol (SCEP) is a PKI communication protocol allowing administrators to securely issue certificates to large numbers of devices through an automatic enrollment technique. Devices must be SCEP-enabled and pre-registered to certification authority (CA) domain before they can request certificates. Device use this protocol to send a certificate request to the CA.

Benefits of a SCEP Server in your Environment

A SCEP server provides a way for you to deliver encrypted configuration profiles to iOS devices in your network. The encryption of the configuration profile is unique for each device. Only the device to which it is sent can read it. This provides another layer of security, in addition to SSL encryption, for sensitive corporate information included in iOS profiles. SCEP is supported only on Enterprise or Datacenter versions of Windows 2008 or 2008 R2. One of these versions must be used on the SCEP server.

SCEP Limitations

SCEP offers a convenient and efficient method of issuing authentication certificates to users and devices; however, there are limitations inherent to the overall SCEP model. The *ZENworks Mobile Management* server delivers the SCEP challenge and SCEP server address to the device securely by using an iOS profile. Although the SCEP challenge can only be used one time, the SCEP challenge does not uniquely identify the user/device for which it was intended and *ZENworks Mobile Management* has no means to control what is done with the information when it is received by the device. If it is compromised, the challenge can be used even though it was only intended to be used by the device user, because the SCEP server accepts the challenge with no user authentication.

SCEP was originally designed for use in a completely internal environment, but with external devices connecting to an external SCEP server to obtain a certificate, there are potential inroads.

If you use *ZENworks Mobile Management* to deliver challenge passwords to devices, ensure that the level of trust given to these certificates is appropriate.

If SCEP limitations pose too great a risk, you should deploy client authentication certificates directly from the *ZENworks Mobile Management* server. Each user is issued a unique certificate that can only be obtained by using *ZENworks Mobile Management* credentials.

SCEP Servers and the ZENworks Mobile Management System

When there is a SCEP server in an environment where *ZENworks Mobile Management* has been implemented, administrators can use *ZENworks Mobile Management* to efficiently provide digital certificates to users with iOS devices. The process is automated and requires very little user input.

Administrators can define the SCEP servers via the Organization view and then associate a user with the SCEP server and configure settings that allow devices to enroll automatically.

The initial configuration profile that the user accepts contains the address of the SCEP server. The device connects with both the *ZENworks Mobile Management* and SCEP servers to complete several configuration steps:

- The device loads the SCEP profile from *ZENworks Mobile Management*.
- The device obtains a certificate from the SCEP server.
- The device obtains a uniquely encrypted configuration profile from *ZENworks Mobile Management*, which can be read exclusively by the device.

Define a SCEP Server

From the dashboard, select **Organization > iOS Corporate Resources > SCEP Servers**. Click the **Add New SCEP Server** tab and fill in the server credentials to define a server.

Display Name (required)	Name identifying the SCEP server.
SCEP Name (required)	Common Name of the Certificate Authority
URL (required)	The base URL of the SCEP server. Must be accessible from the device browser. The server portion of the address might need to be changed to either the internal IP (Wi-Fi) or the external server address (cellular) in order for SCEP to work.
Subject	The CommonName (CN) and Organization (O) that you used when setting up the SCEP. For example: CN=iPhoneSCEP,O=YourCompany
Use Subject Alternative Name	Determines whether an alternative name is used.
Subject Alternative Name Type	Select the type of subject name alternative from the drop-down: RFC-822 Name, DNS Name, or Uniform Resource Identifier
Subject Alternative Name	Supply the alternate name for the SCEP server. Valid entries are an email address (RFC-822), the DNS name of the server, or the server's fully-qualified URL.
NT Principal Name	NT principal to be used in the request.
Key Size in Bits	The size of the key to be used: 1024 or 2048.
Use as Digital Signature	Select the box to use the key as a digital signature.
Use for Key Encipherment	Select the box if the certificate uses a protocol that encrypts keys.
Fingerprint	Hex string to be used as a fingerprint. Can be left blank.

The screenshot shows a wizard window titled "Add New SCEP Server Wizard". It has a "Welcome" sidebar on the left. The main content area contains the following fields and controls:

- Display Name: * [text input]
- SCEP Name: * [text input]
- URL: * [text input]
- Subject: [text input]
- Use Subject Alternative Name:
- Subject Alternative Name Type: RFC 822 Name (dropdown)
- Subject Alternative Name: [text input]
- NT Principal Name: [text input]
- Finish button

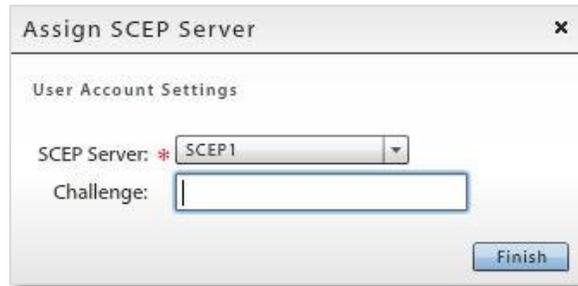
Now, use the *Corporate Resource* option in the **Device Profile** to associate users with a SCEP server.

Associating a User with a SCEP Server

From the dashboard, select the **Users** view and select a user to view his or her profile. Expand the menu under the user's device and select *Corporate Resources*. Choose the **SCEP Server** option and click *Assign New SCEP Server*.

Select a SCEP server for the user from the drop-down list.

To obtain a challenge password, browse to the SCEP URL. Enter the authentication credentials (by default Integrated Windows Authentication). Copy the *Enrollment Challenge Password* and paste it into the *Challenge* field.



The image shows a dialog box titled "Assign SCEP Server" with a close button (X) in the top right corner. Below the title bar, the text "User Account Settings" is displayed. There are two input fields: "SCEP Server: *" with a dropdown menu showing "SCEP1" and a "Challenge:" text input field. A "Finish" button is located at the bottom right of the dialog.



The image shows a table titled "Assigned SCEP Server" with four columns: "Display Name", "SCEP Name", "URL", and "Subject". The first row contains the values "SCEP1", "SCEP1", "123.456.7.89", and "test". Below the table, the text "User Account Settings" is displayed, followed by a "Challenge:" label and a text input field containing the value "123456789".

Display Name	SCEP Name	URL	Subject
SCEP1	SCEP1	123.456.7.89	test

User Account Settings
Challenge: 123456789

Tracking Data Usage

ZENworks Mobile Management can be configured to track usage of carrier data plans and assign data plan limits to users sharing a data plan. The *ZENworks Mobile Management* application gathers data usage statistics from the device and sends it to the server. Based on settings defined in the data plan assigned to the user, a notification alerting the user about the usage limit can be sent to the device when the data usage threshold has been reached.

Other features of the *ZENworks Mobile Management* data plan tracking system include:

- Reallocation of available data when a device is removed from a shared plan.
- Data usage report of each device in the data plan to assist administrators in choosing the correct plan for users.
- Alerts when tampering of data usage metrics is detected along with a subsequent compliance restriction.
- Assigned data plan and statistics visible from the Devices Grid.
- Graphic display of data usage statistics for the user through the *ZENworks Mobile Management* app and the User Self-Administration Portals.

Define a Data Plan

Define the data plans that have been procured by your organization for devices. After a data plan has been defined you can assign it to devices for usage tracking.

To Add a Data Plan:

1. From the dashboard, navigate to **Organization > Organization Control > Data Plans**.
2. Click the **Add Data Plan** button located in the action bar.
3. Enter an identifying **Name** for the data plan.

- Enter the data limit in the **Total Data in Plan (MB)** field. The default is 1000 MB.

- Enter additional information about the plan:

Quota Reset Day of the Month	The day on which the data plan is reset each month. The default is the 15 th day of the month.
Plan Type	Choose Domestic, International, Unknown, Domestic Roaming, International Roaming
Carrier	Select a carrier from the drop-down list.
Shared Plan	Check this box if the data plan is shared by multiple users. If the plan is not shared, it can be associated with only one user.
Warn at Usage Limit (%)	When data usage reaches this percentage of the total limit, an alert is sent to the device(s) and an email is sent to the email address designated to receive alerts. The default is 80%. Email address and message content can be defined once the plan is added.
Alert Increments (%)	Once the warning usage limit has been reached, alerts will be sent as usage percentage increases at increment designated here. The default is 10%, i.e. if an alert is initially sent at 80%, it repeats at 90% and 100% usage.
Alert Devices	Check this box if you want devices, in addition to an administrator, alerted when data usage reaches a percentage of the total limit.

- Click **Add** to save the data plan entry.

7. Once the plan has been added, you can designate the following:

- Email address to which alerts are sent.
- Subject for the email sent.
- Content for the email message.
- Content for the notification sent to the device(s).

Data Plans

Name:

Total Data in Plan (MB):

Quota Reset Day of the Month:

Plan Type:

Carrier:

Shared Plan:

Warn at Usage Limit (%):

Alert Increments (%):

Notes:

Send Email Alerts on Data Usage to the following:

Subject:

Message:

{USEDATA}% of the assigned data plan limit for {PLANNAME} has been used.

Alert Notification to Device:

{USEDATA}% of the assigned data plan limit has been used.

Note: Used in the alert message, the token {USEDATA} will display percentage of the total data plan used. {PLANNAME} will display the plan name.



Username	Phone Number	IMEI	Assigned Limit(MB)	Data Used(MB)

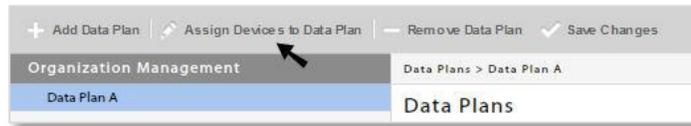
Assigning Devices to a Data Plan

Once a data plan has been defined, you can add a device (or devices for shared plans). On shared plans, when no specific limits are assigned, devices can consume any amount of data.

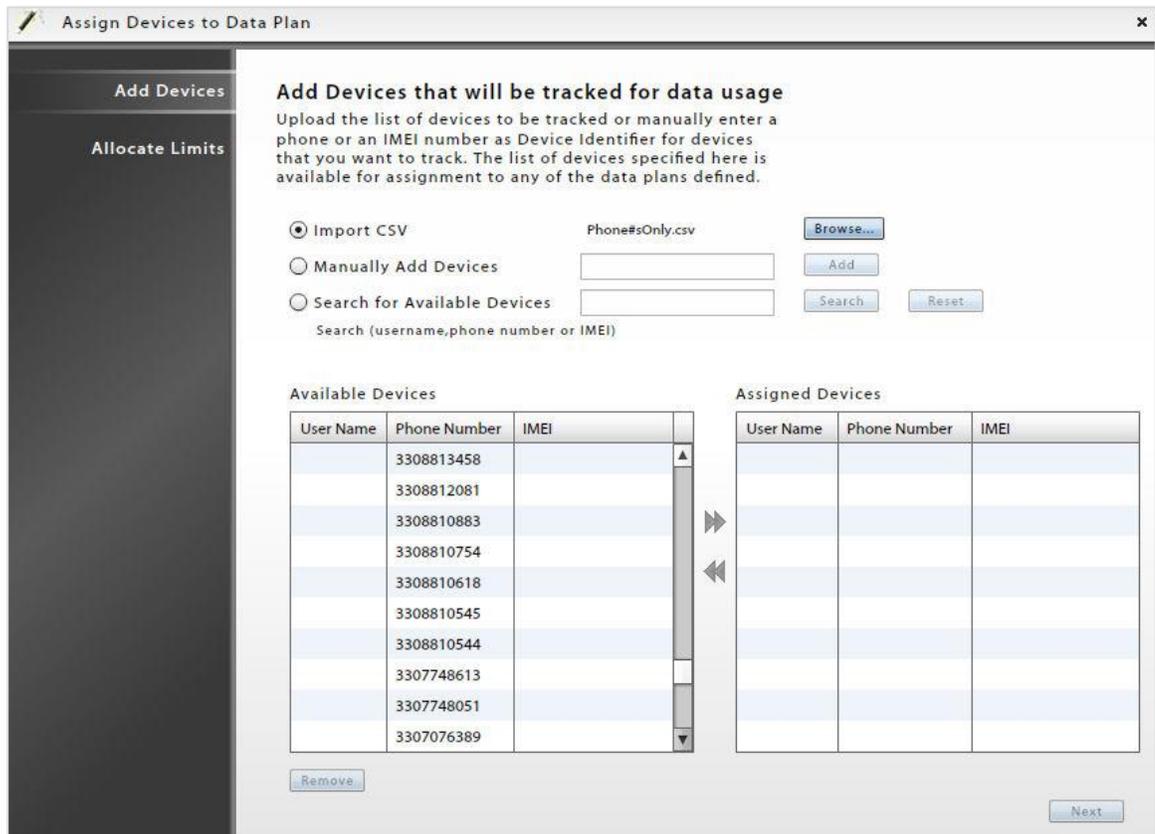
Adding a device or removing a device can be done from the Data Plan page or from the Device Profile. Adding or changing limits must be done from the Data Plan page.

Assign Devices to a Data Plan

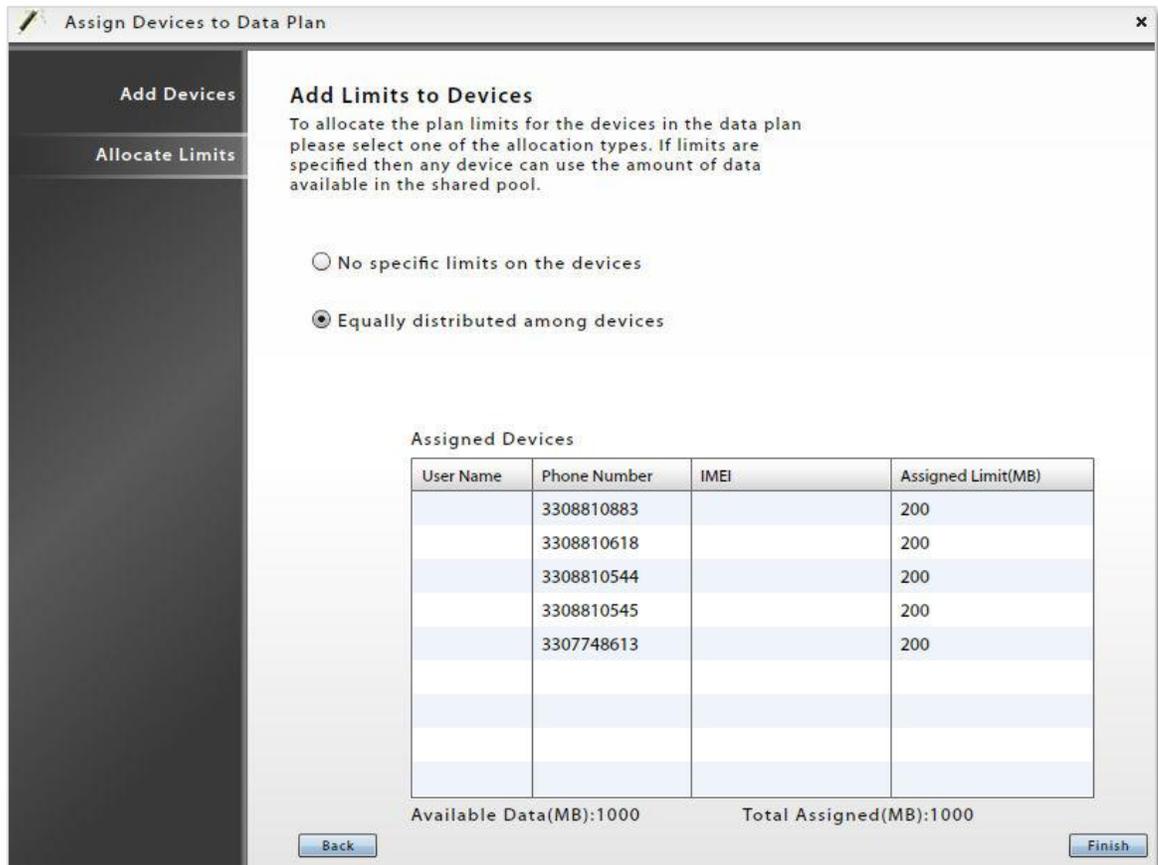
1. From the dashboard, navigate to **Organization > Organization Control > Data Plans**.
2. Click the **Assign Devices to a Data Plan** button located in the action bar.



3. Add devices to the *Available Devices* column.
 - Add a batch of devices using a .CSV file (2 columns labeled and listed in this order: Phone Number, IMEI)
 - Add a single device manually – enter the device phone number
 - Search for an available device on the *ZENworks Mobile Management Device Grid* – enter a string of characters from the username, phone number, or IMEI number associated with the device



4. Select one or more devices from the *Available Devices* column (CTRL+Click or SHIFT+Click for multiple device selection) and click the right arrow to move them to the *Assigned Devices* column.
5. Click **Next** to allocate data usage limits.



6. Select an allocation type:
 - a. No specific limits – devices sharing a plan have no specific limits assigned to them and can consume any amount of data up to the plan total
 - b. Equally distributed data – the data is equally distributed among all devices sharing the plan
7. Click **Finish** to save the data plan assignment.
8. The devices associated with the plan will display in a grid on the Data Plan main page.

Username	Phone Number	IMEI	Assigned Limit(MB)	Data Used(MB)
	3302722227		None	0
	3308812081		None	0
	3308813458		None	0
	3303603182		None	0
	3305065568		None	0
	3305069797		None	0

Remove Devices from a Data Plan

When a device with allocated limits is removed from a shared plan, the data allocated to the removed device is evenly distributed among the remaining devices. The device's unused data for the current billing cycle is distributed immediately and the full allocated amount is distributed evenly in subsequent billing cycles.

Devices can be manually removed from a plan via the *Assigned Devices* grid on the *Data Plan* page or from the Device Profile. They are also automatically removed when a full or selective wipe is issued.

To Manually Remove a Device from a Data Plan:

1. From the dashboard, navigate to **Organization > Organization Control > Data Plans**.
2. Select a data plan from the left panel.
3. Select a device from the grid at the bottom of the page and click the **Remove** button.
4. Click **Yes** to confirm the removal.

Username	Phone Number	IMEI	Assigned Limit(MB)	Data Used(MB)
	3301234567		250	0
	4403698741		250	0
	4401478523		250	0
	3309876543		250	0

Remove

File Share

File Share enables the administrator to create a directory of folders and files to be made available to users with devices that have installed a *ZENworks Mobile Management* device app or a BlackBerry 4.5-7.1 device with the *GO!NotifySync* application.

The first step is to create folders and add files to them. Each folder can be enable or disabled via the policy suites.

Next, enable the permissions in the policy suite. The file directories are not available to users until you enable the **File Share Permissions** for each folder you add to the list.

The user can then access the files from the *ZENworks* application on the device.

- Android users select **File Share** from the *ZENworks* main screen.
- BlackBerry (with *GO!NotifySync*) users select **Files** from the *GO!NotifySync* pop-up menu.
- iOS device users select the **Files** icon from the *ZENworks* main screen.

Adding Folders and Files to the Directory

To manage the file directory, select **Organization**. From the drop-down menu, select **Organization Control > File Share**.

Adding Folders

The parent folder for the directory is named **File Share Folders** by default. You can add subfolders to this parent folder to categorize the files you add.

1. In the left panel, highlight the parent folder to which you are adding a subfolder.
2. Click the **Add Folder** button.
3. Enter a name for the new folder.
4. Click **Create Folder**.



You can edit a folder label by highlighting a folder and clicking the **Change Folder Name** button.



If you want, highlight the new folder and add a *description* or *notes* about the purpose or content of the folder.

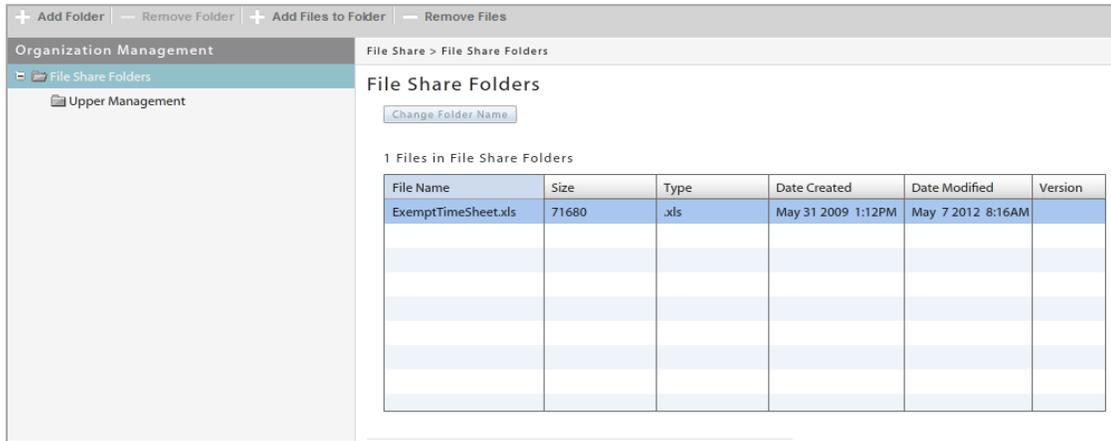


Adding Files

1. In the left panel, highlight the folder to which you are adding files.
2. Click **Add Files to Folder**.
3. A window for browsing and selecting a file pops up. Select a file or files and click **Open**.

The *Upload Status* shows the number of files that added successfully.





The addition of folders and files results in a directory tree. The tree is duplicated in the **File Share Permissions**, where you can allow or disallow access folder by folder.

Enabling the File Share Permissions

Make sure that you have enabled the **File Share Permissions** in the policy suites. From the *ZENworks Mobile Management* dashboard, select **Organization > Policy Management > Policy Suites > (select policy suites) > File Share Permissions**.



Group Notifications

Group Notifications gives the administrator the ability to select groups of users by criteria in order to send them an email or a message notification pushed via APN/GCM services.

Administrators can also search sent group email to view the message body and the date, time, subject and who sent the email (administrator login associated with the email).

Send Group Notifications

Administrators can send a notification to all or a selected group of iOS and/or Android devices via the APN/GCM push services.

Notes: You must upload a NPNS Certificate to the ZENworks Mobile Management server in order to send Group Notifications to iOS devices. (From the dashboard, select **System** > **Organization** and click the *Upload* button next to the **NPNS Certificate** field.)

Google Cloud Messaging must be enabled and Android users must be running OS 4.0.4+ or have a Gmail account registered on the device to receive messages.

Administrators can select a group of users with one or any combination of the following criteria:

- Device Platform
- Device Connection Schedule
- Liability
- ActiveSync Server
- Ownership
- Policy Suite

Notification messages are limited to 160 characters or less.

1. To send a group notification, select **Organization**. From the drop-down menu, select **Organization Control** > **Group Notifications**.
2. Select **Send Group Notifications** from the left panel.
3. Select the recipient criteria, compose your notification message (160 characters or less), and click **Send**.

Organization Management

Group Notifications > Send Group Notifications

Send Group Notifications

Send Group E-mail

Search Group E-mails

Send Group Notifications

Send a notification to targeted iOS/Android devices via the APN/GCM push services.
Note: GCM must be enabled and Android devices must be running OS 4.0.4+ or have a Gmail account to receive messages.

Recipient Criteria

Device Platform Liability Ownership ActiveSync Server

Select One... Select One... Select One... Select One...

Device Connection Schedule

Select One...

Policy Suite(s)

Default

Message (Limited to <= 160 characters)

Send Clear

Send Group E-mail

Administrators can select a group of the organization's users to email by using one or any combination of the following criteria:

- Device Platform
- Liability
- Ownership
- Device Connection Schedule
- ActiveSync Server
- Policy Suite

The sender can also elect to copy the organization contact and the organization administrators.

1. To send a group email, select **Organization**. From the drop-down menu, select Organization control > **Group Notifications**.
2. Select **Send Group E-mail** from the left panel.
3. Select the recipient criteria, compose your e-mail, and click **Send**.

The screenshot shows the 'Send Group E-mail' interface within the 'Organization Management' console. The breadcrumb trail is 'Group Notifications > Send Group E-mail'. The left sidebar contains 'Send Group Notifications', 'Send Group E-mail' (highlighted), and 'Search Group E-mails'. The main content area is titled 'Send Group E-mail' and includes a note: 'If no Recipient Criteria are specified, all users will receive the e-mail.' Below this, there are sections for 'Recipient Criteria' with dropdown menus for 'Device Platform', 'Liability', 'Ownership', 'ActiveSync Server', and 'Device Connection Schedule'. A 'Policy Suite(s)' section contains a text box with 'Default' and two checkboxes: 'Include organization contact' and 'Include administrators'. There are also input fields for 'Subject' and 'Message', and 'Send' and 'Clear' buttons at the bottom.

Search Group E-mail

The administrator can search the Group E-mail log by date, subject, or text in the message body. Results of the search are displayed in a list. Double-clicking on an email in the list reveals the message body and a list of users who failed to receive the email.

1. To search group email, select **Organization**. From the drop-down menu, select **Organization Control > Group Notifications**.
2. Select **Search Group E-mails** from the left panel.
3. Select a range of dates and click **Search**.

The screenshot displays the 'Search Group E-mails' interface. On the left, a navigation pane shows 'Organization Management' with options for 'Send Group Notifications', 'Send Group E-mail', and 'Search Group E-mails'. The main area is titled 'Group Notifications > Search Group E-mail' and 'Search Group E-mails'. It includes a date range selector set to '09/18/2014 to 09/18/2014' with 'Search' and 'Reset' buttons. A table shows 5 results found:

Time (Server Local)	Subject	Sent By
09/18/2014 8:04 AM (-04:00 GMT)	Maintenance this week	admin@dc03.notify.net
09/18/2014 8:04 AM (-04:00 GMT)	Maintenance this week	admin@dc03.notify.net
09/18/2014 8:03 AM (-04:00 GMT)	test	admin@dc03.notify.net
09/18/2014 8:02 AM (-04:00 GMT)	Maintenance this week	admin@dc03.notify.net
09/18/2014 8:02 AM (-04:00 GMT)	Maintenance this week	admin@dc03.notify.net

Double-click e-mails to see body and failed recipient(s)

The Activity Monitor

The *ZENworks Mobile Management* Activity Monitor provides snapshots of information regarding the wireless devices and users in the enterprise network. Pie charts, bar graphs, and tables display statistics at a glance. In addition, the view can be flipped to display a log of warnings and alerts.

The Activity Monitor is the default view for all logins; however, another view in the dashboard can be designated as the default by editing the login credentials. (See *System > Organization Administrators*)

The Activity Monitor will always display six graphs at a time.

You can choose which six to display from the following:

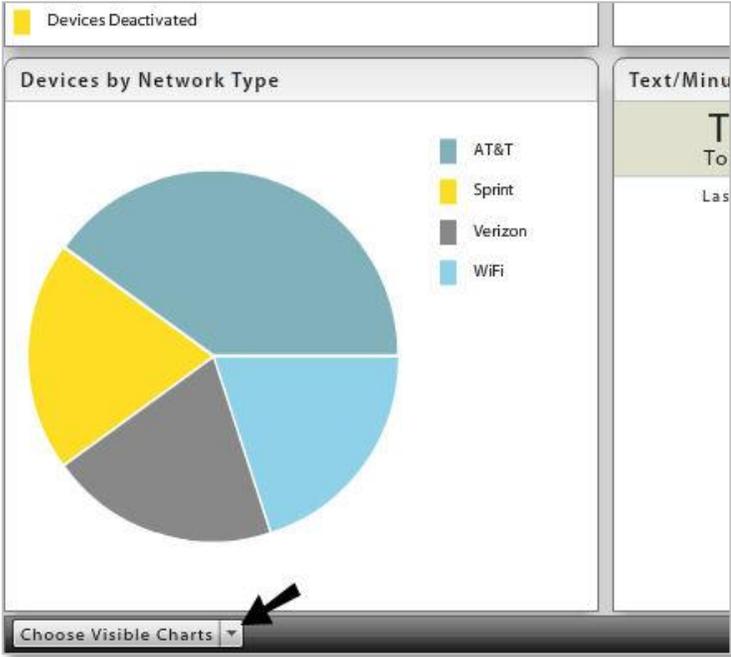
Configuration	
Activation/De-Activation History	Bar chart showing the number of devices activated and deactivated in the past seven days.
Active/Inactive Devices	Pie chart showing the percentage of active devices versus disabled devices.
Devices by Carrier	Pie chart showing the percentage of devices using a particular carrier.
Devices by Connection Schedule	Pie chart showing the percentage of devices operating under each device connection schedule.
Devices by Domain	Pie chart showing the percentage of devices operating under a particular domain.
Devices by Liability	Pie chart showing the percentage of devices designated as <i>corporate</i> liable vs. <i>individual</i> liable. (Liability refers to ownership of the data on the device.)
Devices By Ownership	Pie chart showing the percentage of devices owned by the company vs. the percentage of devices personally owned by individuals.
Devices by Plan Type	Pie chart showing the percentage of devices operating on an international vs. a domestic plan type.
Devices by Policy Suite	Pie chart showing the percentage of devices operating under each policy suite.
Connectivity	
ActiveSync Authorization Failures	Pie chart showing the percentage of devices passing invalid credentials for the ActiveSync accounts of known users to the server.
ActiveSync Version	Pie chart showing the percentage of devices operating with various ActiveSync protocol versions.

Device App Authorization Failures	Pie chart showing the percentage of devices passing invalid credentials for the <i>ZENworks Mobile Management</i> accounts of known users to the server.
Device App Language	Pie chart showing the percentage of devices by their language setting.
Device App Version	Pie chart showing the percentage of devices by the version of the <i>ZENworks Mobile Management</i> app installed.
Statistics	
Devices by Battery Level	Pie chart showing the percentage of devices that have battery levels at 0-20%, 21-40%, 41-60%, 61-80%, or 81-100%.
Devices by Battery Status	Pie chart showing the percentage of devices in various statuses of battery health: charging, not charging – battery health good, etc.
Devices by Free Memory	Bar chart showing the number of devices with 0-20%, 21-40%, 41-60%, 61-80%, or 81-100% free memory.
Devices by Memory	Pie chart showing the percentage of devices that have memory capacity of 256 MB, 512 MB, etc.
Devices by Network Type	Pie chart showing the percentage of devices operating under a particular carrier network.
Devices by Platform > OS > Model	Pie chart showing the percentage of each device platform in use. Click a Platform wedge to show the platform by device operating system version. Click an OS wedge to show the operating system version by model. Click the back arrow to return to the previous view.
Devices by SD Card Free Memory	Bar chart showing the number of devices with 0-20%, 21-40%, 41-60%, 61-80%, or 81-100% free SD card memory.
Devices by SD Card Installed	Pie chart showing the percentage of devices with an SD card installed versus those that do not have an SD card installed.
Devices by SD Card Memory	Pie chart showing the percentage of devices that have an SD card memory capacity of 256 MB, 512 MB, etc.
Devices by SIM Card Removed/Changed	Pie chart showing the percentage of devices on which the SD card has been changed or removed vs. those that have had no change in the SD card status.
Devices by Timezone	Pie chart showing the percentage of devices by the time zone in which they are used.
Devices by TouchDown Registered	Pie chart showing the percentage of Android devices that have registered the TouchDown app vs. those that do not have TouchDown.
Devices by Violation	Pie chart showing the percentage of devices that are restricted vs. those that are not restricted.
Jailbroken/Not Jailbroken	Pie chart showing the percentages of jailbroken devices vs. those that are not jailbroken. This includes jailbroken iOS devices as well as rooted Android devices.

Roaming/Not Roaming	Pie chart showing the percentages of roaming devices vs. those that are not roaming.
Texts/Minutes Usage	Table listing top consumers in regard to text and minutes usage in the last 30 days.
Trends	
Trend of Changing Carriers	Line graph showing the number of users who have changed carriers over a week's time.
Trend of Changing Device Models	Line graph showing the number of users who have changed device models over a week's time.
Trend of Changing Ownership	Line graph showing the number of users whose device ownership has changed over a week's time.
Trend of Changing Platforms	Line graph showing the number of users who have changed device platforms over a week's time.

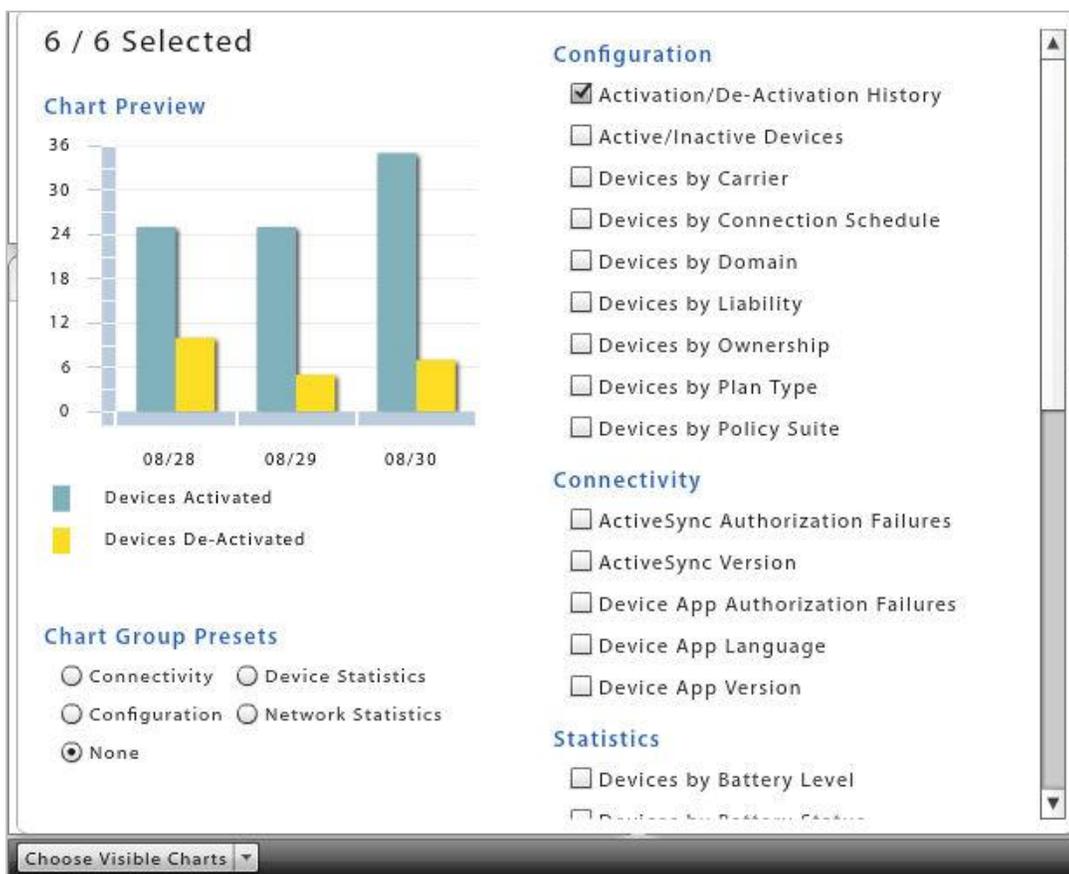
Select Graphs. Click the *Choose Visible Charts* button at the bottom left corner of the Activity Monitor screen. Select the six graphs you want to display on the grid.

The graphs you select and the grid arrangement are maintained for your dashboard login credentials.



When making or hovering over a selection, a preview of the chart appears. The information in the preview chart is sample data.

The Activity Monitor grid always displays six graphs. If fewer are chosen, the most recently deselected graphs will display along with your choices. You cannot select more than six graphs. You must deselect a graph before you can choose a different graph.

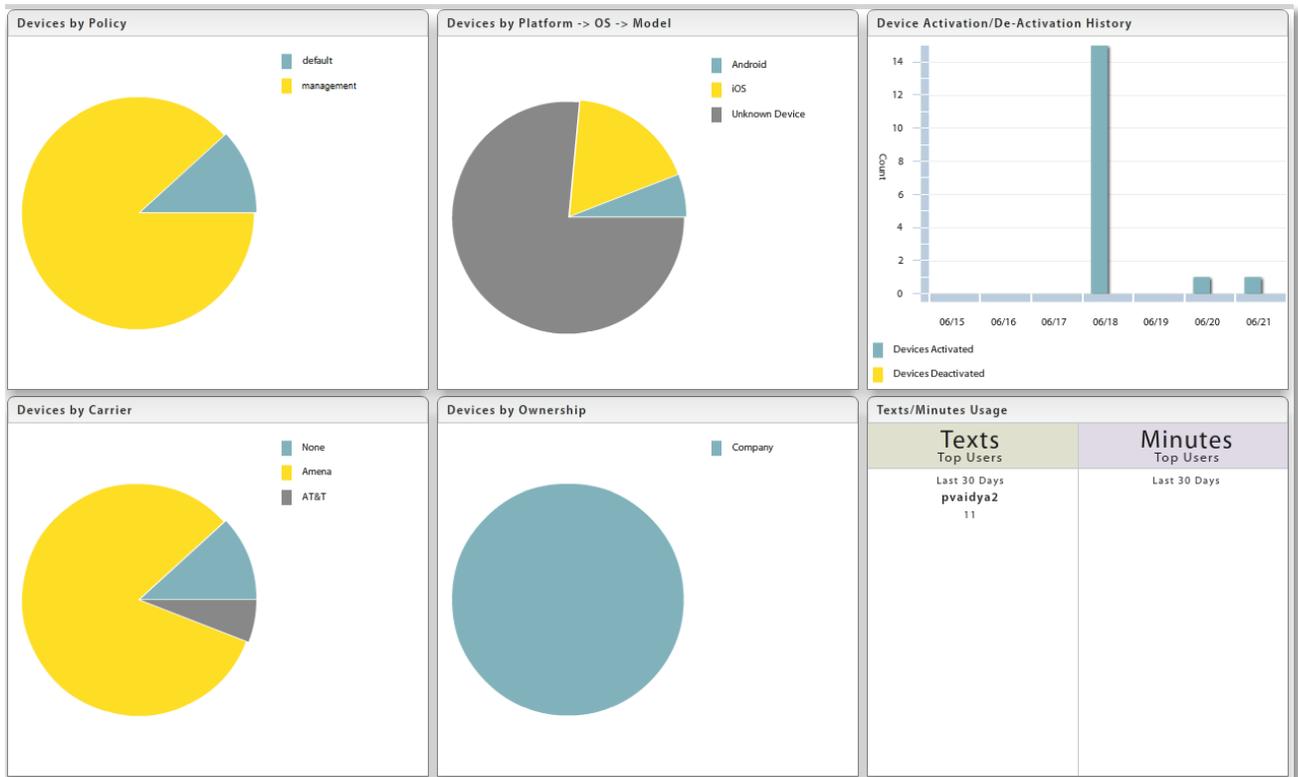


Click the *Choose Visible Charts* button when your selections are complete.

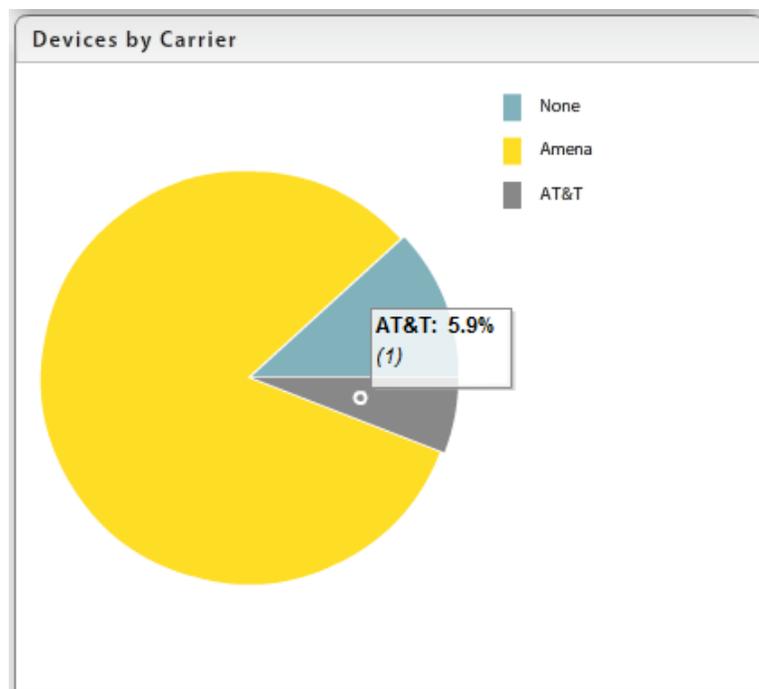
Chart Group Presets. You can choose a preset group of charts.

Connectivity displays . . .	Configuration displays . . .	Device Statistics displays . . .	Network Statistics displays . . .
ActiveSync Authorization Failures	Devices by Connection Schedule	Device by Free Memory	Devices by Network Type
ActiveSync Version	Devices by Domain	Devices by SD Card Free Memory	Devices by Timezone
Device App Authorization Failures	Devices by Liability	Devices by TouchDown Registered	Roaming/Not Roaming
Device App Language	Devices by Ownership	Devices by Violation	Text/Minutes Usage
Device App Version	Devices by Policy Suite	Jailbroken/Not Jailbroken	Devices by SIM Card Removed/Changed
Devices by Network Type	Devices by Plan Type	Devices by Battery level	Devices by Carrier

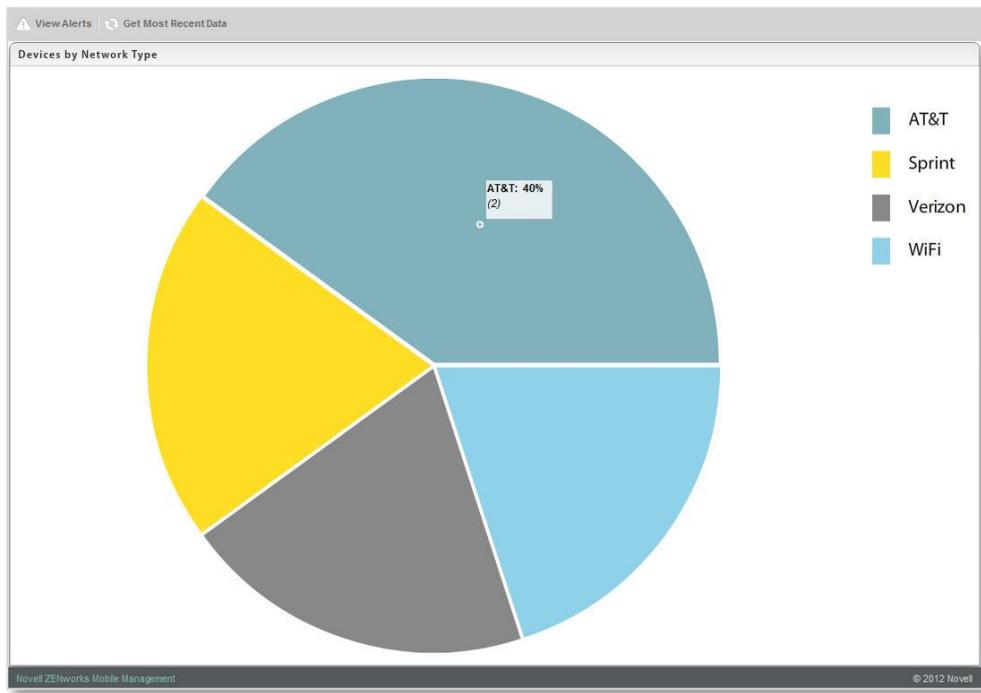
Rearrange Panels. You can rearrange the panels in the view by selecting a block and dragging it and dropping it where you prefer.



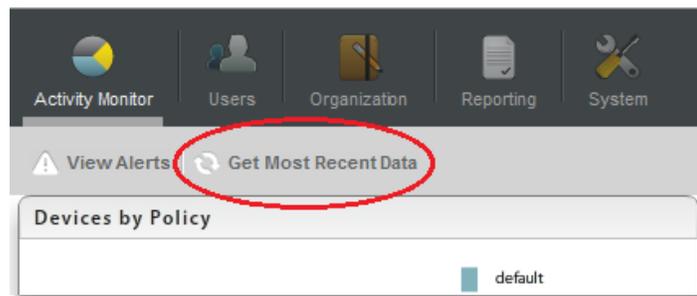
View Details. You can see detail of the statistics by hovering over a section of a graph or chart.



Zoom on a Panel. You can enlarge a panel to full view with full details by double-clicking it. Double-click on the enlarged view to return to the Activity Monitor view.



Refresh the View. You can refresh the Activity Monitor view with the most recent data by selecting *Get Most Recent Data* in the gray option bar.



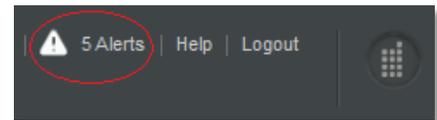
Flip to the View Alerts Grid. You can flip the Activity Monitor view to a table of alerts listed by user. Select **View Alerts** in the option bar. Select **View Info Charts** to return to the Activity Monitor view.

For an alert to trigger, **Alert Settings** in the *Compliance Manager* must be enabled. Alerts report violations of device access restrictions. They also monitor and report on device resource levels, connectivity, and administrator or user initiated events. For information on enabling the *Alerts Settings*, see [Configuration Guide: Compliance Manager](#).

The screenshot shows the 'View Alerts Grid' interface. At the top, there are navigation buttons: 'View Info Charts', 'Get Most Recent Data', 'Snooze Alerts', 'Disable Alerts', 'Mark All Read', and 'Mark All Unread'. Below this is the 'Alert Search Criteria' section with fields for 'Date Range' (06/21/2012 to 06/21/2012), 'User Name' (Domain\UserName), 'Message Keywords', and 'Priority' (Low, Medium, High). There are 'Search' and 'Reset' buttons. The main part of the interface is a table with the following columns: User Name, Device, Timestamp (Server Local), Status, Priority, and Message.

User Name	Device	Timestamp (Server Local)	Status	Priority	Message
ex07jwitmer	iOS	06/21/2012 9:31 AM (-04:00 GMT)	Unread	Medium	jwitmer has enrolled without defining an email address.
ZENworks Mobile Management System Alert	None	06/21/2012 9:31 AM (-04:00 GMT)	Unread	Medium	Devices have not made ZENworks connections, Organization-wide, since Jun 21 2012 12:44PM GMT.
jhalidman	iOS	06/21/2012 9:30 AM (-04:00 GMT)	Unread	Medium	A device associated with jhalidman has fallen below the recommended minimum device memory level.
pvaitya2	Android	06/21/2012 9:30 AM (-04:00 GMT)	Unread	Medium	A device associated with pvaitya2 has fallen below the recommended minimum device battery level.
ex07jwitmer	iOS	06/21/2012 9:30 AM (-04:00 GMT)	Unread	Medium	A device associated with jwitmer has fallen below the recommended minimum device battery level.

The total number of alerts is displayed at the bottom of the grid. An icon in the top right corner of the *ZENworks Mobile Management* dashboard gives the number of unread alerts in the grid. Unread alerts are displayed in red text. Alerts that have been read are displayed in black text. Only unread alerts display when you select **Hide Read Alerts**.



Search the Alert Grid. Search the View Alerts grid by:

- **Date Range**
- **User Name**
- **Keyword(s)**
- **Priority**

Snooze Alerts – You can select one or more alerts in the grid and click the **Snooze Alerts** button. This temporarily stops the alert from repeating, at the set interval, until you have had an opportunity to investigate. Choose to snooze for 1-60 Minutes, 1-24 Hours, or 1-60 Days.

Disable Alerts – You can select one or more alerts in the grid and click the **Disable Alerts** button. This disables the *Alert Setting*. All alerts of this type will cease to trigger. They no longer report on the *View Alerts* grid and do not send email and SMS notifications to designated administrators.

Reporting

The *Reporting* view provides statistical reports regarding devices, data usage, compliance rules, and administrator roles.

The reports are as follows:

Device Reports	Compliance Reports
<ul style="list-style-type: none"> • Devices by Liability 	<ul style="list-style-type: none"> • Access Restriction Violations
<ul style="list-style-type: none"> • Devices by Network Type 	<ul style="list-style-type: none"> • Device Platform Restrictions by User
<ul style="list-style-type: none"> • Device by OS Version and Model 	<ul style="list-style-type: none"> • Exceptions by User
<ul style="list-style-type: none"> • Device by OS Version and Platform 	<ul style="list-style-type: none"> • Resource Restrictions by User
<ul style="list-style-type: none"> • Devices by Platform 	<ul style="list-style-type: none"> • User by Exceptions
<ul style="list-style-type: none"> • Devices by Platform and Model 	Administrative Roles Reports
<ul style="list-style-type: none"> • Devices by Policy Suite 	<ul style="list-style-type: none"> • Organization Administrators
<ul style="list-style-type: none"> • Data Usage by Data Plan 	<ul style="list-style-type: none"> • Organization Roles
User Reports	<ul style="list-style-type: none"> • System Administrators
<ul style="list-style-type: none"> • Data Usage by User 	<ul style="list-style-type: none"> • System Roles
<ul style="list-style-type: none"> • Users by Carrier 	App Reports
<ul style="list-style-type: none"> • Users by Ownership 	<ul style="list-style-type: none"> • App Assignment
<ul style="list-style-type: none"> • Users by Expiration Date 	<ul style="list-style-type: none"> • App Statistics
iOS Resource Reports	<ul style="list-style-type: none"> • App Assigned to Users
<ul style="list-style-type: none"> • Resource by Assignment 	<ul style="list-style-type: none"> • App Statistics by Category
<ul style="list-style-type: none"> • Resource By Expiration Date 	

Using the Reports

Sort Report Columns. Most reports are initially sorted by user email address (or administrator/role) within each category mentioned in the report title. You can, however, click other column headings to change the order of the users within each main category.

By clicking multiple column headings you can create a nested sort. For example: Device Platform (the main category), sorted by Carrier Name (first sorting category), sorted by Phone Number (second sorting category).

Reports > Device Reports > Devices by Platform

Devices by Platform

Name	Email Address	Domain	Phone Number	Device Model	Carrier Name	Ownership	Liability
▼ Android							
ajones			+4083132503	DROID3	Amena	Company	Corporate
BlackBerry							
htcsupersonic							
▼ iOS							
jwitmer		ex07	Unknown	iPad 3	None	Company	Corporate
vhunt			4083901331	iPhone 4S	Amena	Company	Corporate
gslick			14085284666	iPhone 3GS	None	Company	Corporate
► Unknown Device							
Windows Mobile							

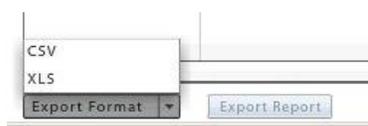
Rearrange Report Columns. The columns can be rearranged by clicking and dragging a column heading to a new position. Column width can be adjusted by clicking and dragging a column's left dividing line at the header position.

Reports > Device Reports > Devices by Platform

Devices by Platform

Name	Email Address	Domain	Phone Number	Device Model	Carrier Name	Ownership	Liability
▼ Android							
ajones			+4083132503	DROID3	Amena	Company	Corporate
BlackBerry							
htcsupersonic							
▼ iOS							
jwitmer		ex07	Unknown	iPad 3	None	Company	Corporate
vhunt			4083901331	iPhone 4S	Amena	Company	Corporate
gslick			14085284666	iPhone 3GS	None	Company	Corporate
► Unknown Device							
Windows Mobile							

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



Sample Reports

Sample Device/User Reports

Information included in most **Device** and **User** reports:

- User Name
- Email Address
- Domain
- Phone Number
- Device Platform
- Device Model
- Carrier Name
- Ownership
- Liability
- OS Version
- AS Version
- Policy Suite
- Device Connection Schedule
- Activation Date

The reports listed below also include discovered devices and display these additional columns: **MDM Status** (Discovered/Enrolled) and **ActiveSync Server Name**.

- Devices by OS Version and Model
- Devices by OS Version and Platform
- Devices by Platform and Model
- Devices by Platform

Reports > Device Reports > Devices by Network Type

Devices by Network Type

Name	Email Address	Domain	Phone Number	Device Platform	Device Model	Carrier Name	Ownership
▼ AT&T							
jwitmer		ex07	Unknown	iOS	iPad 3	None	Company
ntanner			14085284666	iOS	iPhone 3GS	None	Company
▼ Sprint							
dmatthews			4083901331	iOS	iPhone 4S	Amena	Company
▶ Unknown							
▶ Verizon Wireless							

The **Data Usage by Data Plan** report includes the following information:

- Plan Name
- Total Limit (MB)
- User Name
- Data Used (MB)
- Data Used (%)
- Phone Number
- IMEI
- Removed

Data Usage by Data Plan

Plan Name	Total Limit (..)	Username	Data Used(MB)	Data Used(%)	Phone Number	IMEI
Plan A	1000.000					
▼ Plan Q	1000.000					
		arivera	0.000	0.00		012621000894
Plan Z	1000.000					

Sample iOS Resource Report

Information included in **iOS Resource** reports:

- Resource Name
- Domain
- User Name
- Expiration Dates

Resource by Assignment						
Resource Name	Username	Domain	Assignment Expiration Date	User Expiration Date	Resource Expiration Date	Resource
▼ CalDAV						
▼ Zimbra - Date					11/20/2012 (UTC)	
	jwtmer	ex10				
▼ Zimbra - Interval						1
	jwtmer	ex10				
	jwtmer	ex10	11/15/2012 (UTC)			
▼ Email						
▼ EX03 - IN - Date					11/15/2012 (UTC)	
	jwtmer	ex10	11/15/2012 (UTC)			
▼ EX03 - IN - Interval						1
	jwtmer	ex10	11/15/2012 (UTC)			
▼ EX03 - OUT						
	jwtmer	ex10	11/15/2012 (UTC)			
▼ Exchange						
▼ Exchange 2007 - Date					11/15/2012 (UTC)	
	jwtmer	ex10	11/15/2012 (UTC)			
▼ Exchange 2007 - Interv						1
	jwtmer	ex10	11/15/2012 (UTC)			
▼ LDAP						
▼ Exchange 2010 - Date					11/15/2012 (UTC)	

Sample Compliance Report

Information included in **Compliance** reports:

- User Name
- Domain
- Device (platform)
- Policy Suite

Access Restriction Violations			
User Name / Access Restriction Violation	Device	Domain	
▼ acostello		ex07	acostello
No violations			
▼ acostello2		ex07	acostello
No violations			
▼ acrown	iOS	ex07	tim
ActiveSync connection violation			
Liability violation			
▼ acrown	iOS	ex07	tim
Liability violation			
▼ jwtmer	iOS	ex07	Robin
ActiveSync connection violation			
▼ pvaidya1	MotoDROIDBIONICS	ex07	tim
No violations			

Sample Administrative Roles Report

Information included in **Administrative Roles** reports:

- Administrator Name
- Administrative Role Name
- Permissions

Organization Roles	
Name	Permission
ActiveSync Servers	Full Access
Administrative LDAP Servers	Full Access
Custom Columns	Full Access
Device Connection Schedules	Full Access
Policy Suites	Full Access
User and Device Reporting	Read Only Access
System Management	Full Access
▼ Support Admin	
Activity Monitor and Alerts	Read Only Access
▼ Smart Devices and Users	
Add User	Full Access
▼ Administration	
Clear Device Enrollment	Full Access
Clear Passcode	Full Access
Disable Device	Full Access
Full Wipe	Full Access
Lock Device	Full Access
Selective Wipe	Full Access
Send Welcome Letter	Full Access
Show Recovery Password	None
Wipe Storage Card	Full Access
▼ Device Compliance	
Clear ActiveSync Authorization Failures	Full Access
Clear SIM Card Removed Or Changed Violation	Full Access
Clear ZENworks Mobile Management Authorization Failures	Full Access

Export Format ▼ Export Report

Sample App Reports

Information included in the **App Assignment** report:

- Name
- Email Address
- Domain
- Phone Number
- Device Model
- Carrier Name
- Ownership
- Liability
- OS Version
- AS Version
- Policy Suite
- Device Connection Schedule
- Activation Date
- Container ID

App Assignment							
Name	Email Address	Domain	Phone Number	Device Model	Carrier Name	Ownership	Liability
▼ Android							
▼ AIM							
None							
▼ Info Week							
None							
▼ TouchDown							
None							
▼ iOS							
▼ Doc Scan - Scanner to Scan PDF							
None							
▼ Skype for iPhone							
None							
▼ World Clock-Time Zones							
acrown		ex07	+13303984898	iPhone 4S		Personal	Individual

Information included in the **App Statistics** report:

- Name
- Download Count
- Download Limit
- Categories
- Version
- VPP
- Bundle ID
- App Store ID
- Package Name
- Available Redemption Codes
- Available Licenses

App Statistics						
Name	Download Count	Download Limit	Version	VPP	Bundle ID	
▼ Android						
AIM	0	<Unlimited>	5.2	N/A		0
Info Week	0	<Unlimited>	7.8.1	N/A		0
TouchDown	0	<Unlimited>	8.1.00012	N/A		0
▼ iOS						
Doc Scan - Scanner to Scan PDF, Pri	0	<Unlimited>	8.4	No	com.ifunplay.DocScan	453
Skype for iPhone	0	<Unlimited>	4.17.3	No	com.skype.skype	3048
UPS Mobile	0	<Unlimited>	2.4.1	No	com.ups.m.iphone	3362
World Clock-Time Zones	0	<Unlimited>	1.6.5	No	com.timeanddate.worldclock	4036

Information included in the **App Assigned to Users** report:

- Name
- Version
- Status
- Required
- Rejection Reason
- Last Attempted Install
- Container ID

Name	Version	Status	Required	Rejection Reason	Last Attempted Install
▼ acrown					
▼ iOS					
World Clock-Time Zones	1.6.5	Not installed via MDM	No		

Information included in the **App Statistics By Category** report:

- Name
- Download Count
- Download Limit
- Categories
- Version
- VPP
- Bundle ID
- App Store ID
- Package Name
- Available Redemption Codes
- Available Licenses

Name	Download Count	Download Limit	Categories	Version	VPP	
News & Magazines						
Newsstand						
Personalization						
Photo & Video						
Photography						
▼ Productivity						
▼ iOS						
Skype for iPhone	0	<Unlimited>	Productivity, Social Networ	5.2.1	No	com.skype
World Clock-Time Zones	0	<Unlimited>	Productivity, Travel	1.6.5	No	com.timea
Reference						

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
```