Organization Administration

ZENworks® Mobile Management 2.7.x

August 2013

Novell®

Legal Notices

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

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

Novell Trademarks

Third-Party Materials

Table of Contents

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***

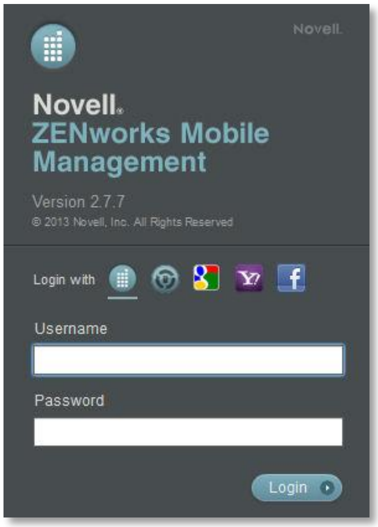
Example: https://my.ZENworks.server/dashboard

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.


Novell.
Novell.
ZENworks Mobile Management
Version 2.7.7
© 2013 Novell, Inc. All Rights Reserved
Login with
Username
Password
Login

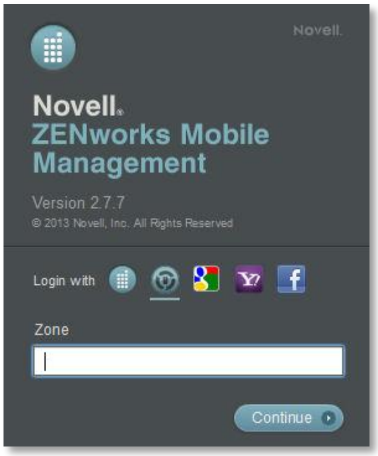
OpenID Login

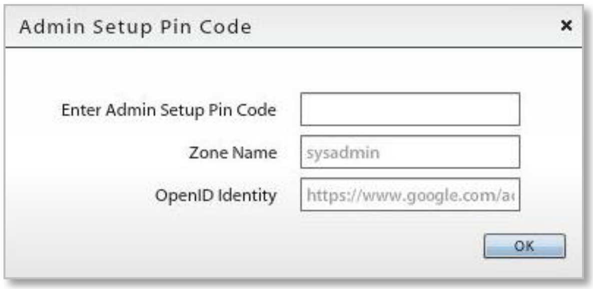
Use your OpenID credentials to log in.

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.

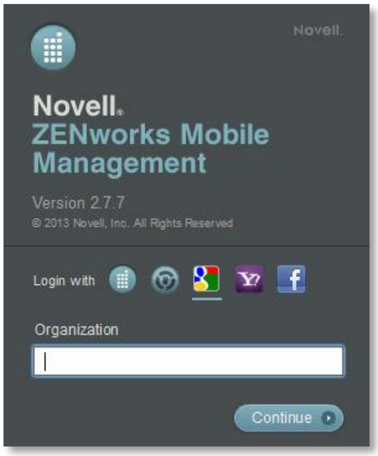

Novell.
Novell.
ZENworks Mobile Management
Version 2.7.7
© 2013 Novell, Inc. All Rights Reserved
Login with
Zone
Continue


Admin Setup Pin Code

Enter Admin Setup Pin Code

Zone Name sysadmin

OpenID Identity https://www.google.com/a


Novell.
Novell.
ZENworks Mobile Management
Version 2.7.7
© 2013 Novell, Inc. All Rights Reserved
Login with
Organization
Continue

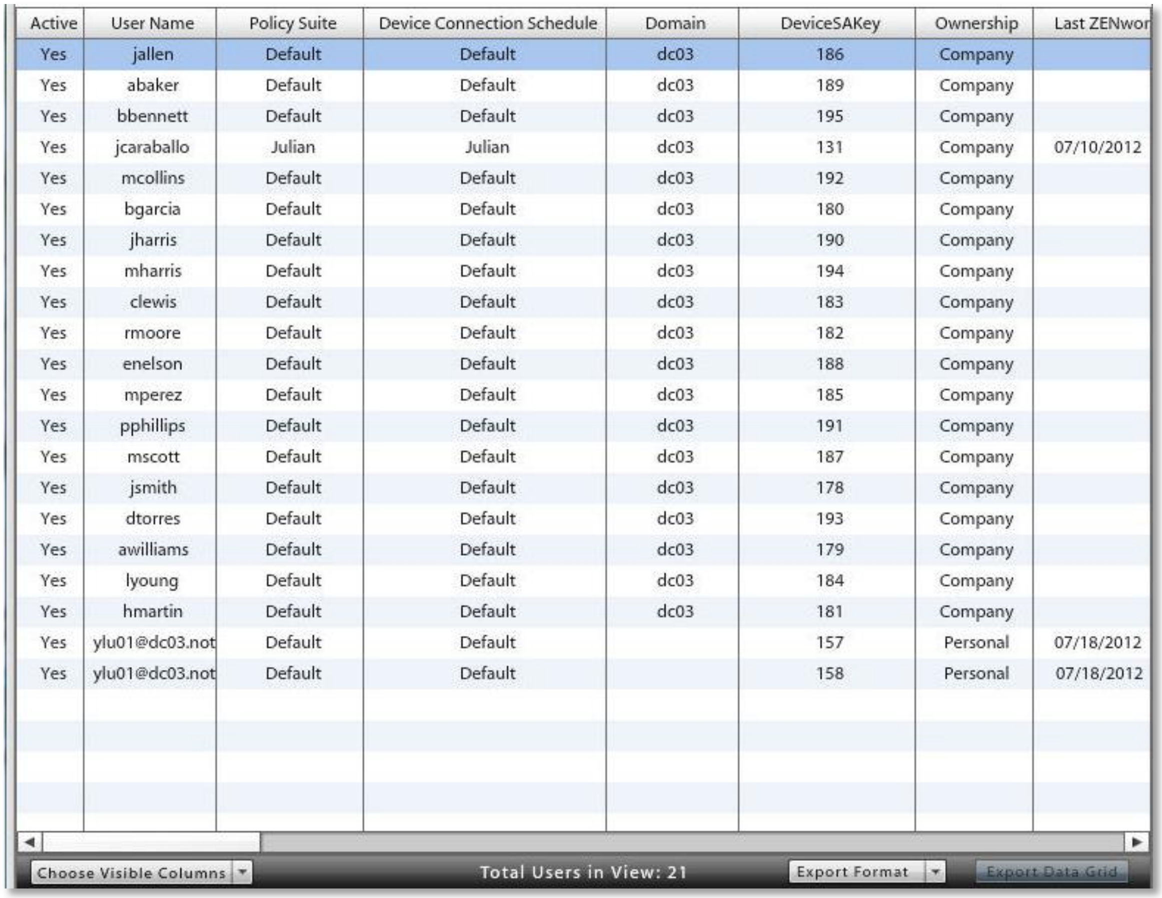
Managing Users

The User Grid

The ***Users*** view displays a list of all users currently in the *ZENworks Mobile Management* organization.

From this page, you can add a user, remove a user, email a user, move to a user profile view with a greater level of detail, and issue remote security commands to a user's device.

You can also customize the user list view or export data from the list.



Active	User Name	Policy Suite	Device Connection Schedule	Domain	DeviceSAKey	Ownership	Last ZENwor
Yes	jallen	Default	Default	dc03	186	Company	
Yes	abaker	Default	Default	dc03	189	Company	
Yes	bbennett	Default	Default	dc03	195	Company	
Yes	jcaraballo	Julian	Julian	dc03	131	Company	07/10/2012
Yes	mcollins	Default	Default	dc03	192	Company	
Yes	bgarcia	Default	Default	dc03	180	Company	
Yes	jharris	Default	Default	dc03	190	Company	
Yes	mharris	Default	Default	dc03	194	Company	
Yes	clewis	Default	Default	dc03	183	Company	
Yes	rmoore	Default	Default	dc03	182	Company	
Yes	enelson	Default	Default	dc03	188	Company	
Yes	mperez	Default	Default	dc03	185	Company	
Yes	pphillips	Default	Default	dc03	191	Company	
Yes	mscott	Default	Default	dc03	187	Company	
Yes	jsmith	Default	Default	dc03	178	Company	
Yes	dtorres	Default	Default	dc03	193	Company	
Yes	awilliams	Default	Default	dc03	179	Company	
Yes	lyoung	Default	Default	dc03	184	Company	
Yes	hmartin	Default	Default	dc03	181	Company	
Yes	ylu01@dc03.not	Default	Default		157	Personal	07/18/2012
Yes	ylu01@dc03.not	Default	Default		158	Personal	07/18/2012

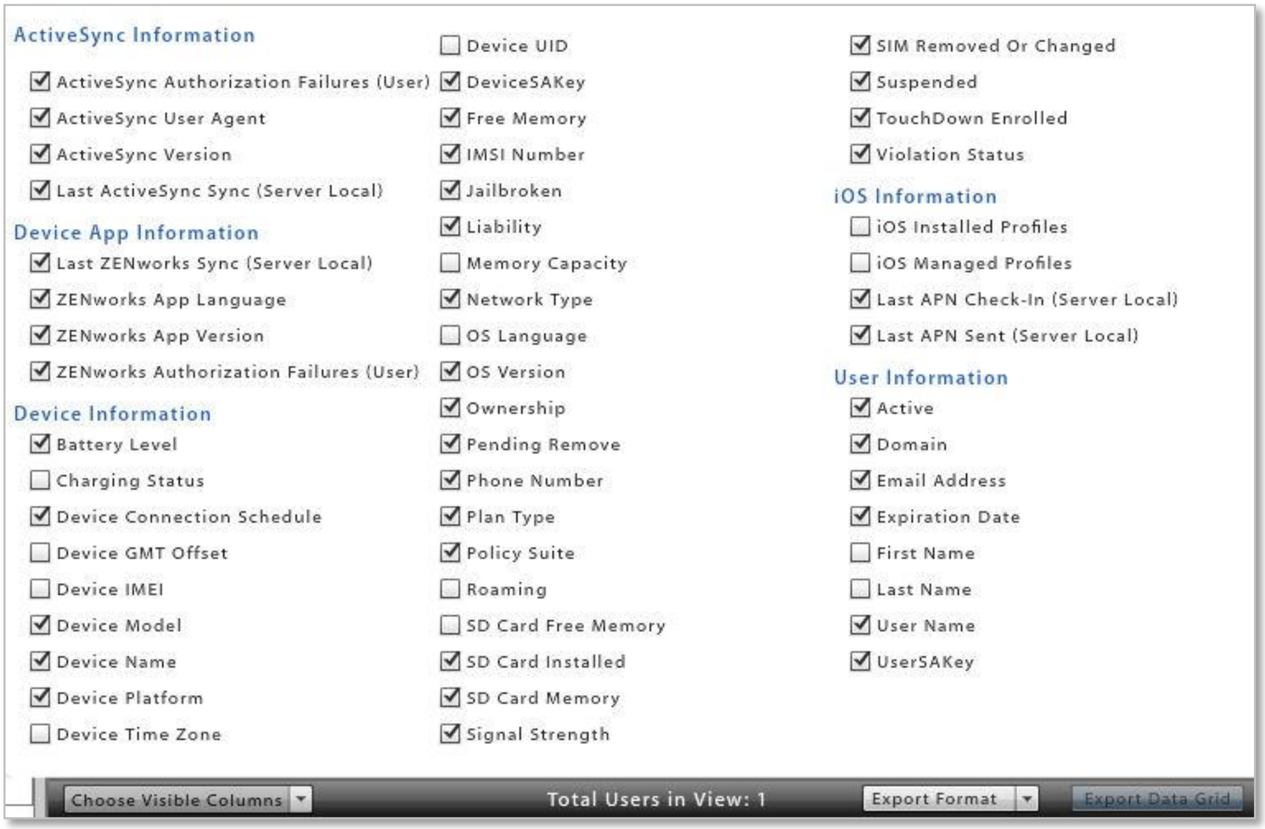
Total Users in View: 21

Customizing and Searching the User Grid

Customize the user list view by:

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

Choose the visible columns. Click the *Choose Visible Columns* button in the bottom left corner of the page and select or deselect the columns you want displayed or hidden. The dashboard saves the columns you choose to view.



ActiveSync Information

☑ ActiveSync Authorization Failures (User)
☑ ActiveSync User Agent
☑ ActiveSync Version
☑ Last ActiveSync Sync (Server Local)

Device App Information

☑ Last ZENworks Sync (Server Local)
☑ ZENworks App Language
☑ ZENworks App Version
☑ ZENworks Authorization Failures (User)

Device Information

☑ Battery Level
□ Charging Status
☑ Device Connection Schedule
□ Device GMT Offset
□ Device IMEI
☑ Device Model
☑ Device Name
☑ Device Platform
□ Device Time Zone
□ Device UID
☑ DeviceSAKey
☑ Free Memory
☑ IMSI Number
☑ Jailbroken
☑ Liability
□ Memory Capacity
☑ Network Type
□ OS Language
☑ OS Version
☑ Ownership
☑ Pending Remove
☑ Phone Number
☑ Plan Type
☑ Policy Suite
□ Roaming
□ SD Card Free Memory
☑ SD Card Installed
☑ SD Card Memory
☑ Signal Strength
☑ SIM Removed Or Changed
☑ Suspended
☑ TouchDown Enrolled
☑ Violation Status

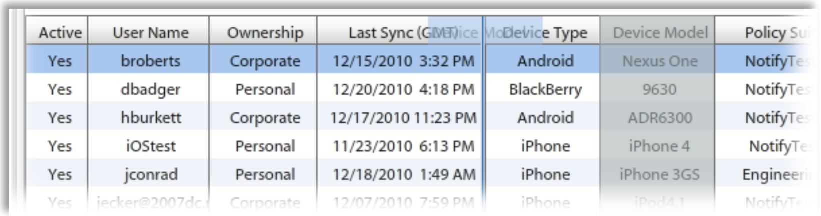
iOS Information

□ iOS Installed Profiles
□ iOS Managed Profiles
☑ Last APN Check-In (Server Local)
☑ Last APN Sent (Server Local)

User Information

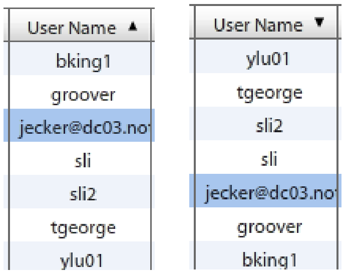
☑ Active
☑ Domain
☑ Email Address
☑ Expiration Date
□ First Name
□ Last Name
☑ User Name
☑ UserSAKey

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	NotifyTe
Yes	dbadger	Personal	12/20/2010 4:18 PM	BlackBerry	9630	NotifyTe
Yes	hburkett	Corporate	12/17/2010 11:23 PM	Android	ADR6300	NotifyTe
Yes	iOStest	Personal	11/23/2010 6:13 PM	iPhone	iPhone 4	NotifyTe
Yes	jconrad	Personal	12/18/2010 1:49 AM	iPhone	iPhone 3GS	Engineer
Yes	jecker@2007dc.	Corporate	12/07/2010 7:59 PM	iPhone	iPod4,1	NotifyTe

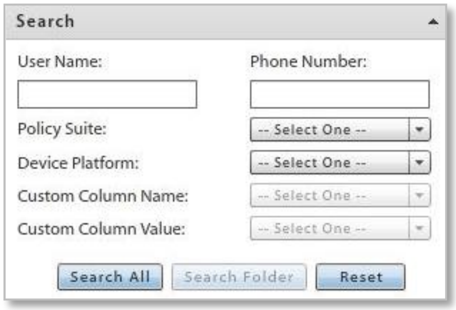
Sort columns. Click the heading of any column to sort the list by the information in that column. Sort in ascending or descending order.



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

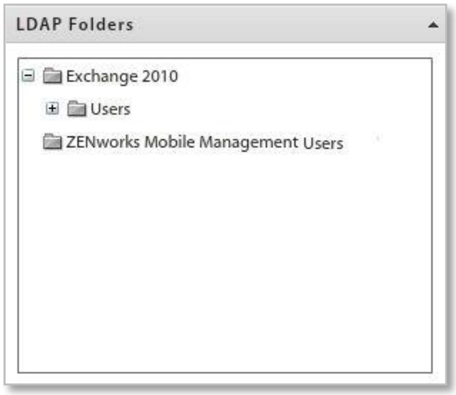
User Name ▼
ylu01
tgeorge
sli2
sli
jecker@dc03.no
groover
bking1

Search for and display a single user or category of users. Use the search criteria in the drop-down **Search** panel to search for users by user name, phone number, policy suite, device platform, or custom column name and value. Wildcards entries, using an asterisk, are supported.



LDAP Folders. Browse the LDAP folder directory in the drop-down **LDAP Folders** column and select a folder. This will limit the users displayed in the grid to the members of that folder.

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

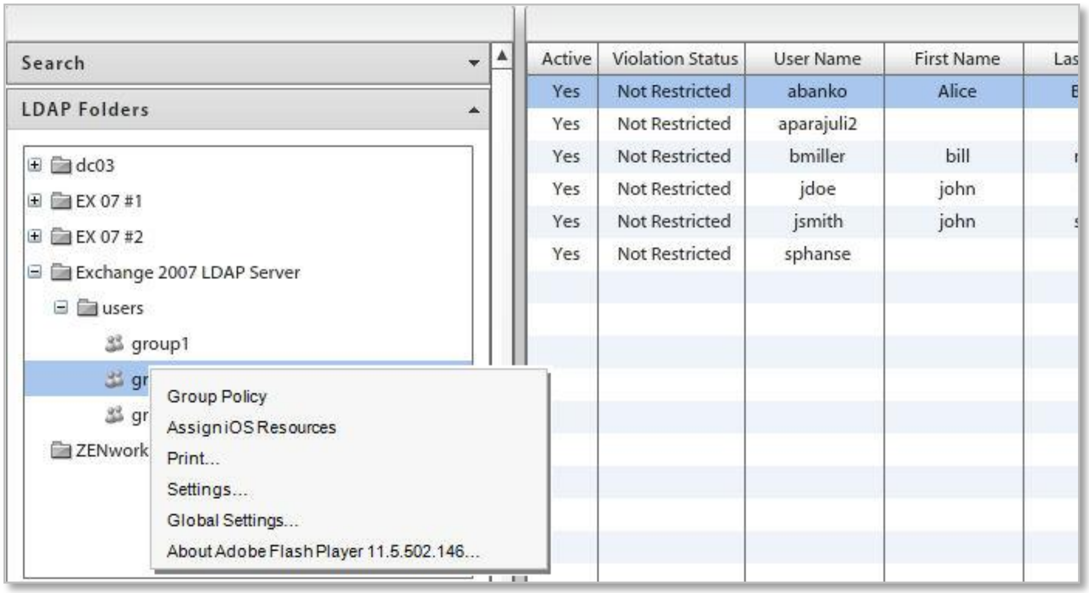


Assigning Settings and Resources to LDAP Groups/Folders

Settings such as Policy Suite, Connection Schedule, and Liability, as well as, iOS resources can be assigned to a group or folder directly from the user grid.

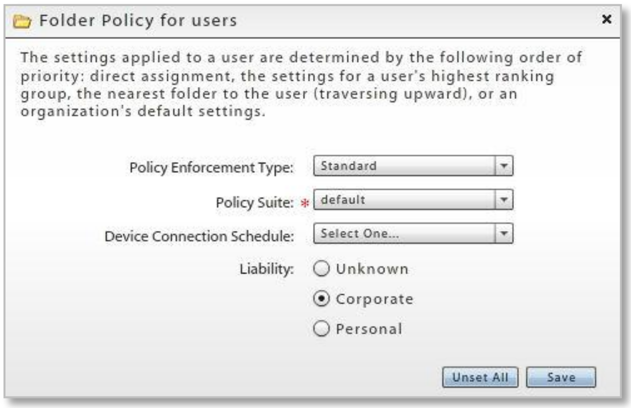
Expand the **LDAP Folders** panel and navigate to a group or folder. Right-click the group/folder.

- Select the **Group (Folder) Policy** option to assign settings for Policy Suite, Device Connection Schedule and Liability.
- Select the **Assign iOS Resource** option to assign resources.



Active	Violation Status	User Name	First Name	Las
Yes	Not Restricted	abanko	Alice	B
Yes	Not Restricted	aparajuli2		
Yes	Not Restricted	bmiller	bill	r
Yes	Not Restricted	jdoe	john	
Yes	Not Restricted	jsmith	john	s
Yes	Not Restricted	sphanse		

Setting Assignments. Choose the Policy Suite, Device Connection Schedule and Liability assignments for the group/folder. Click **Save**.



The settings applied to a user are determined by the following order of priority: direct assignment, the settings for a user's highest ranking group, the nearest folder to the user (traversing upward), or an organization's default settings.

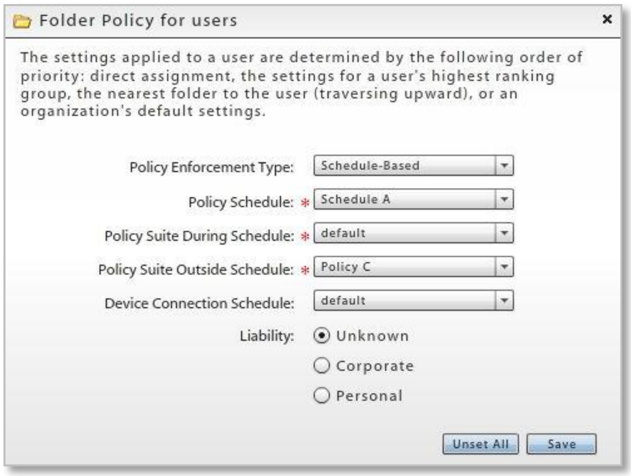
Policy Enforcement Type: Standard

Policy Suite: * default

Device Connection Schedule: Select One...

Liability: ○ Unknown ● Corporate ○ Personal

Standard Policy Enforcement



The settings applied to a user are determined by the following order of priority: direct assignment, the settings for a user's highest ranking group, the nearest folder to the user (traversing upward), or an organization's default settings.

Policy Enforcement Type: Schedule-Based

Policy Schedule: * Schedule A

Policy Suite During Schedule: * default

Policy Suite Outside Schedule: * Policy C

Device Connection Schedule: default

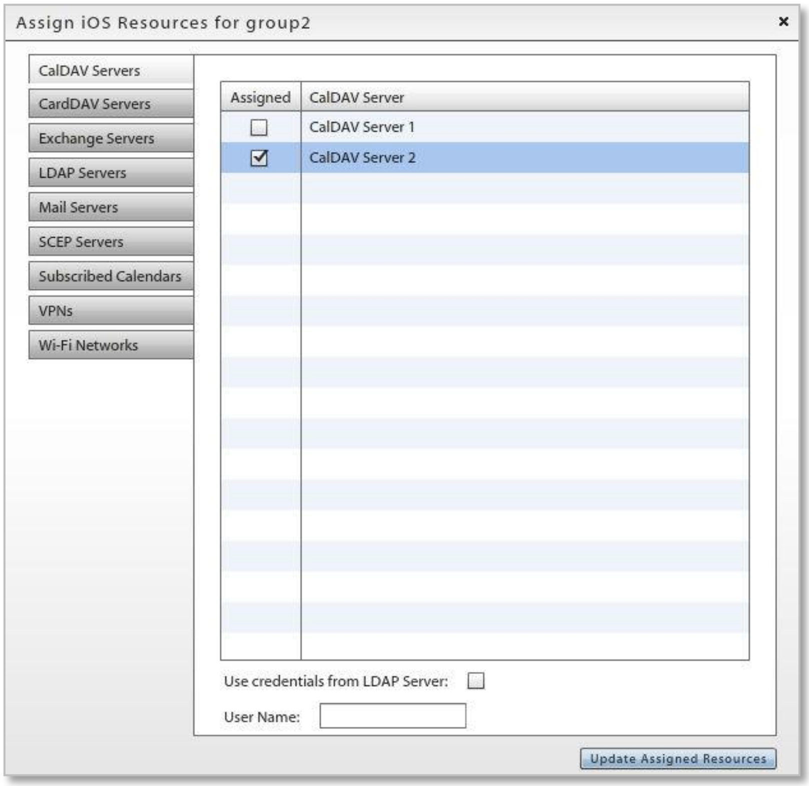
Liability: ● Unknown ○ Corporate ○ Personal

Schedule-Based Policy Enforcement

iOS Resource Assignments. Select a resource from the left panel.

- 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.

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



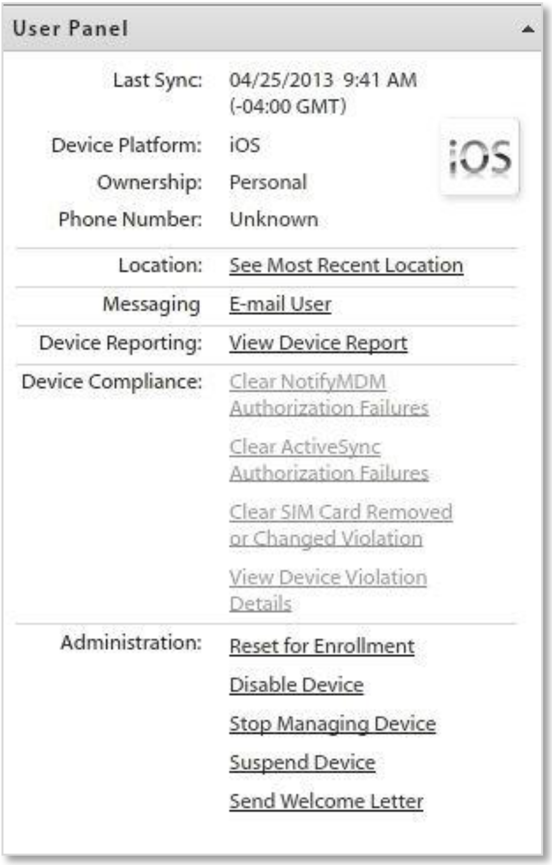
Assigned	CalDAV Server
☐	CalDAV Server 1
☑	CalDAV Server 2

Use credentials from LDAP Server: ☐

User Name:

The User Panel

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



User Panel

Last Sync: 04/25/2013 9:41 AM (-04:00 GMT)

Device Platform: iOS

Ownership: Personal

Phone Number: Unknown

Location: See Most Recent Location

Messaging: E-mail User

Device Reporting: View Device Report

Device Compliance: Clear NotifyMDM Authorization Failures
Clear ActiveSync Authorization Failures
Clear SIM Card Removed or Changed Violation
View Device Violation Details

Administration: Reset for Enrollment
Disable Device
Stop Managing Device
Suspend Device
Send Welcome Letter

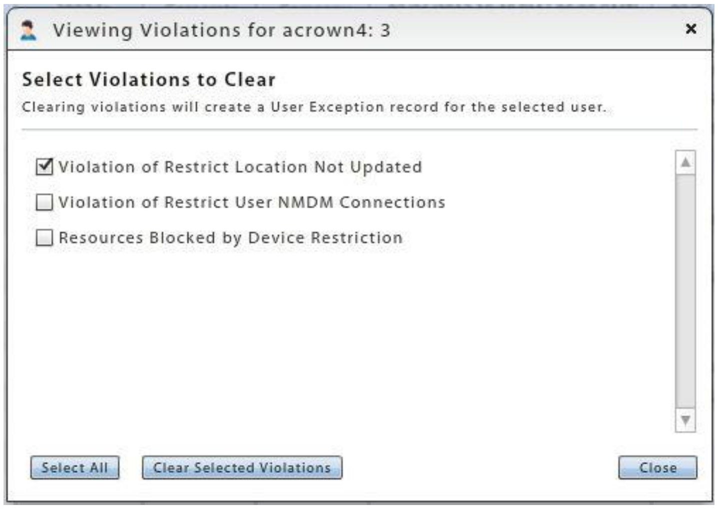
Panel Content

- **Quick Device Stats** - displays last sync time, device platform, ownership, and phone number
- **Pop-up Views** - provides the following links to pop-up views:
  - See Most Recent Location - Location statistics
  - E-mail User - Compose and send an email
  - View Device Report - Device statistics
- **Device Compliance** – allows the administrator to clear a violation restriction or view device violation details and create a User Exception for a violation. *See Monitoring Device Compliance for details.*
- **Security Commands** - Gives quick access to reactive security commands, such as *Full Wipe*. *See Remote Security Commands for functionality.* Security commands can also be issued through the User Self Administration Portal.
- **Show Recovery Password** - Allows the administrator to view the recovery password issued by a device. User can also view the recovery password through the User Self Administration Portal. See *Enabling Password Recovery*.
- **Send Welcome Letter** - Gives the ability to 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 ot reloading iOS profiles when a device experiences enrollment issues.
- **Clear Passcode** – The iOS device passcode is cleared. If the passcode is required by the user's policy, the user is prompted to enter a new passcode.

Monitoring Device Compliance from the User Panel

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

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



Viewing Violations for acrown4: 3

Select Violations to Clear

Clearing violations will create a User Exception record for the selected user.

☑ Violation of Restrict Location Not Updated

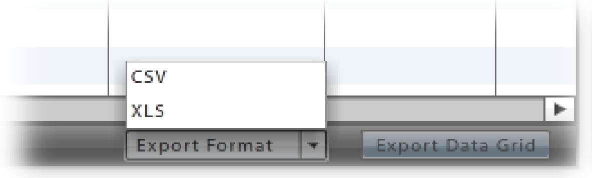
□ Violation of Restrict User NMDM Connections

□ Resources Blocked by Device Restriction

Violation Details Pop-up

Exporting Data from the User Grid

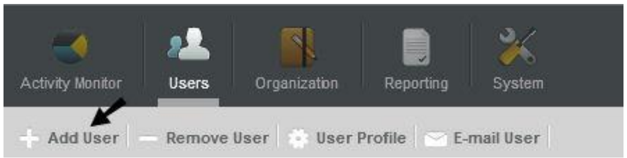
Exporting data from the list to a comma separated values (CSV) or Excel (XLS) file. Choose the *Export Format*, then click the *Export Data Grid* button to save the current grid to a file.



Adding / Removing / Disabling Users

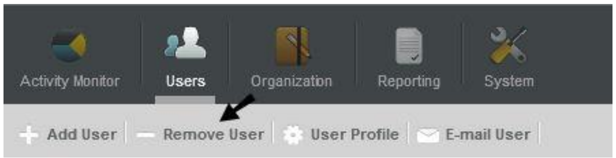
The ***Add User*** button launches a window that allows the manual addition of individual users or addition of users via batch import methods (.CSV file or an LDAP server).

For more documentation on adding users, see the Configuration Guide: Adding Users, Enrolling Devices.

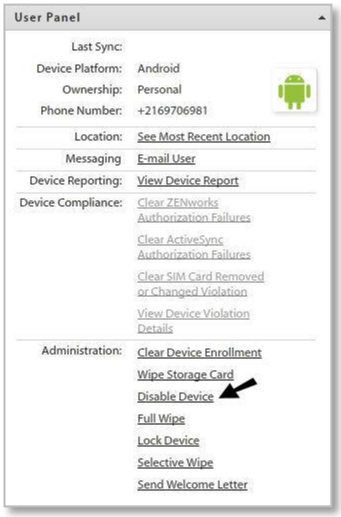


Add User button

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



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



User Panel

Last Sync:	
Device Platform:	Android
Ownership:	Personal
Phone Number:	+2169706981
Location:	See Most Recent Location
Messaging	E-mail User
Device Reporting:	View Device Report
Device Compliance:	Clear ZENworks Authorization Failures Clear ActiveSync Authorization Failures Clear SIM Card Removed or Changed Violation View Device Violation Details
Administration:	Clear Device Enrollment Wipe Storage Card Disable Device Full Wipe Lock Device Selective Wipe Send Welcome Letter

The User Profile

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

User Information

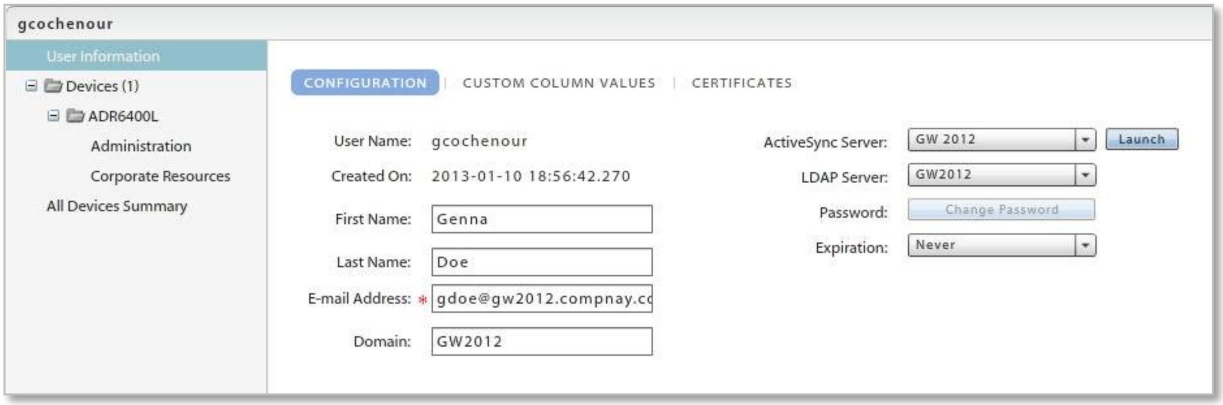
Select *User Information* from the left panel of the User Profile. There are three tabs that display the following user information*:*

- Configuration
- Custom Column Values
- Certificates

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.



User Name: gcochenour

Created On: 2013-01-10 18:56:42.270

First Name: Genna

Last Name: Doe

E-mail Address: * gdoe@gw2012.compnay.cc

Domain: GW2012

ActiveSync Server: GW 2012

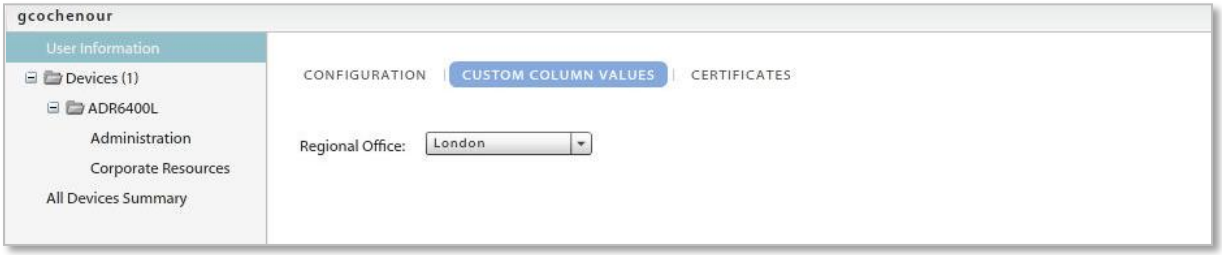
LDAP Server: GW2012

Password:

Expiration: Never

User Information: Custom Column Values

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



Regional Office: London

User Information: Certificates

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

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

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

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

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

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

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

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

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

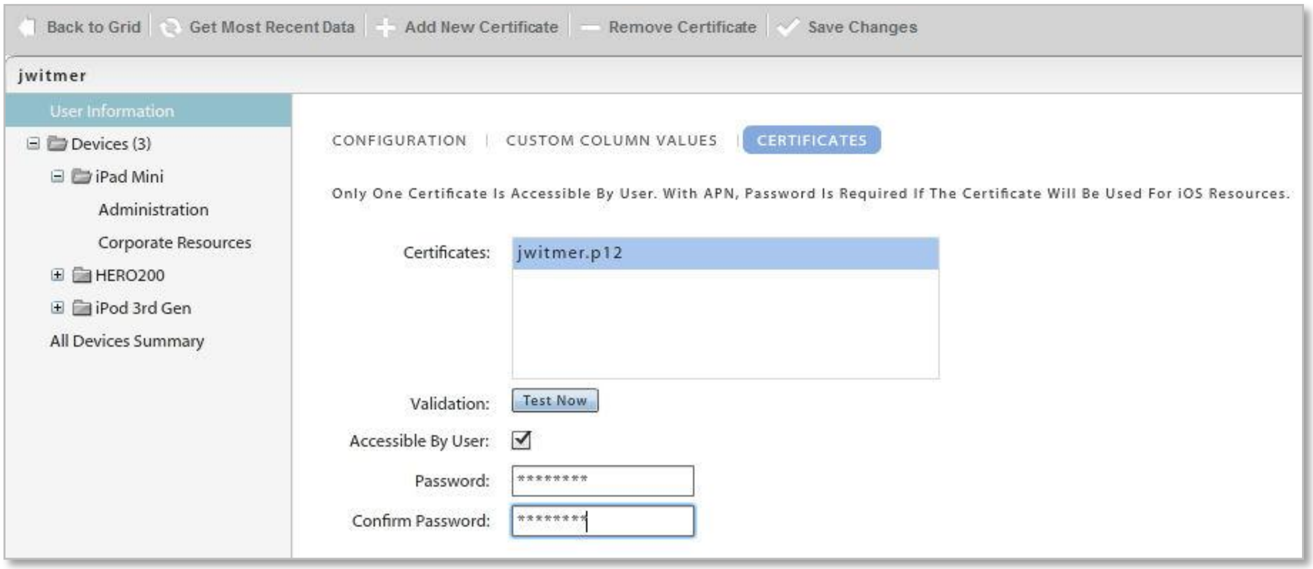
Upload the Certificate. When you have obtained a client certificate, upload it to the user's profile. You must have access to the certificate file itself and know any password associated with it.

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

To upload a certificate file:

1. Access the ***Users*** view of the dashboard. Select a user from the grids and click ***User Profile***.
2. Select ***User Information*** from the left panel, then select the ***Certificates*** tab.
3. Select the ***Add New Certificate*** button to browse and select the certificate file.

4. Check the box ***Accessible By User*** to designate this as the active certificate. It is possible to upload more than one certificate to the user's profile, however, only one certificate at a time can be active. One certificate can be used on multiple devices associated with a single user.
5. If the certificate is protected by a password, enter the ***Password*** and confirm it.
6. Click ***Save Changes***.



Only One Certificate Is Accessible By User. With APN, Password Is Required If The Certificate Will Be Used For iOS Resources.

Certificates: jwitmer.p12

Validation: Test Now

Accessible By User: ☑

Password: ********

Confirm Password: ********

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 *NotifySync*)	OS 4.5	
	OS 4.6	
	OS 5.0	
	OS 6.0	OS 6.0
	OS 7.0	OS 7.0
iOS	iOS 4.1	iOS 4.1
	iOS 4.3.5	iOS 4.3.5

	iOS 5+	iOS 5+
Symbian	OS 9.1	OS 9.1
	OS 9.2	OS 9.2
Windows Mobile	OS 6.1 Standard	OS 6.1 Standard
	OS 6.1 Professional	OS 6.1 Professional
	OS 6.5 Professional	OS 6.5 Professional

Device Administration

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

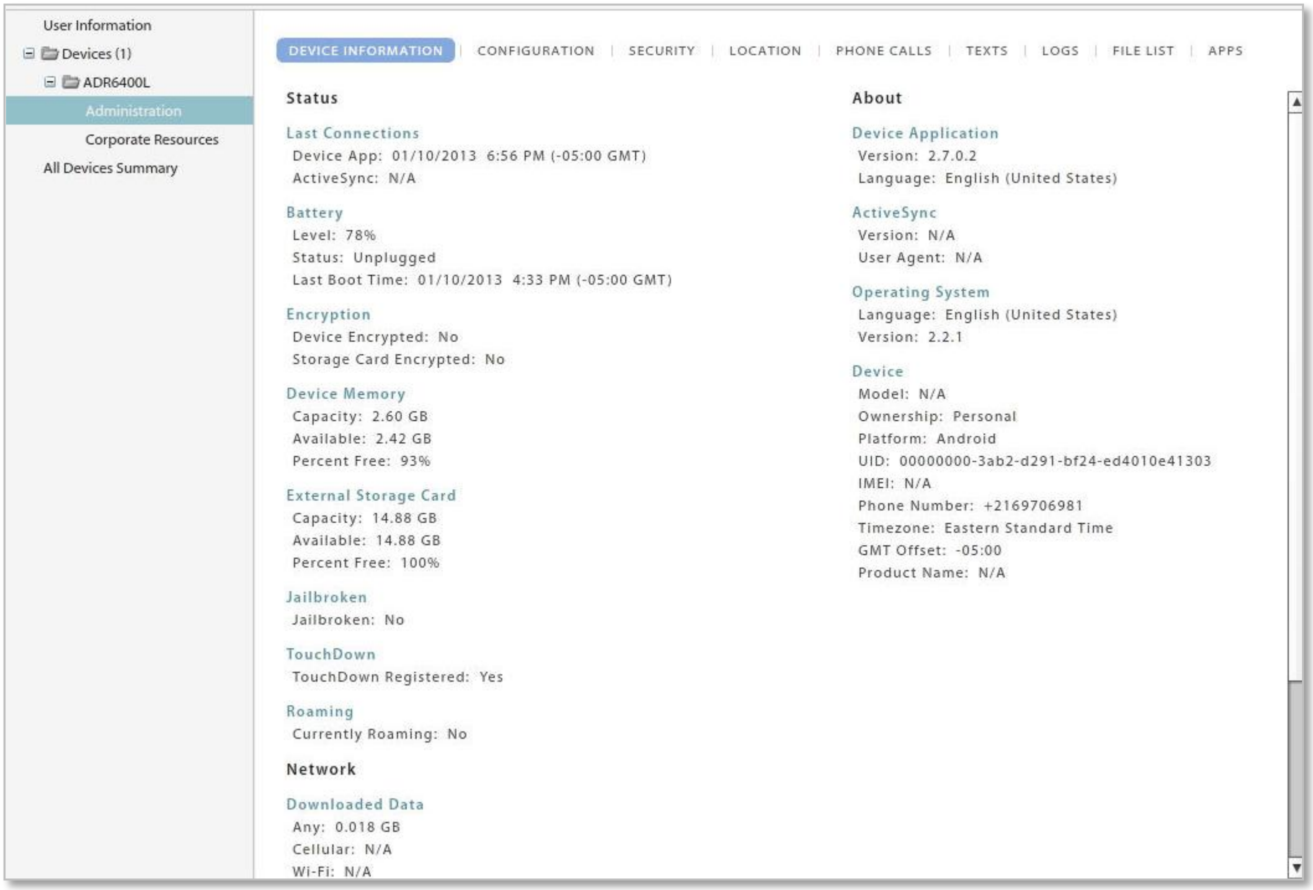
- Device Information
- Configuration
- Security
- Location
- Phone Calls and Texts
- Viewing Logs
- File List
- Applications

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.



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

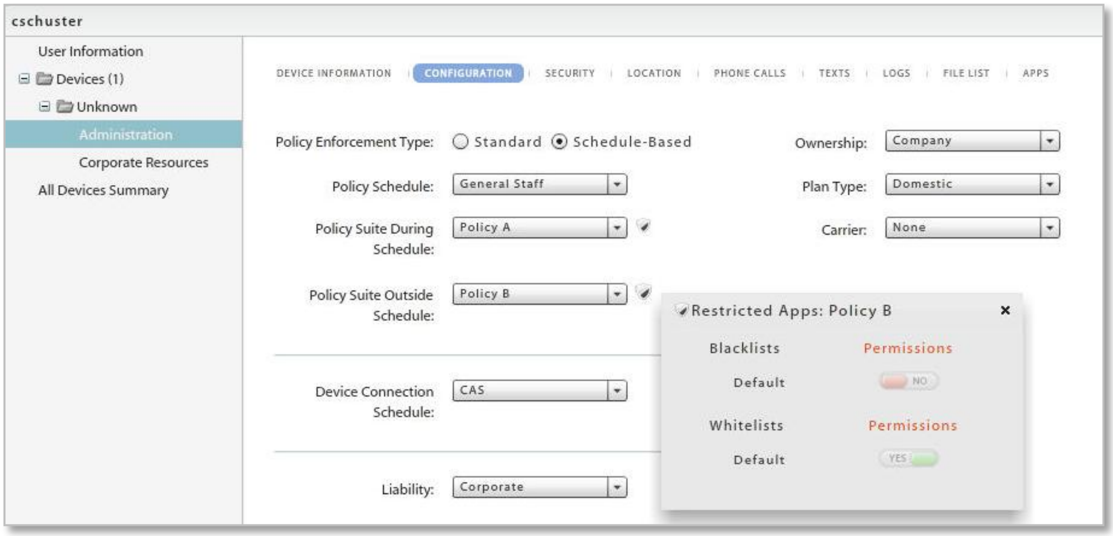
(*return to Device Administration menu*)

Select the ***Configuration*** tab to view the Policy Suite, Device Connection Schedule, and Liability assignments for the device. The source from which each assignment came is displayed in parentheses below the drop down box.

When the **Auto** check boxes are marked, the user receives assignments based upon his/her LDAP group/folder membership. Changes on the LDAP server update the user's assignments.

If you wish to override the assignments made automatically by LDAP association or organization defaults, remove the checkmark and select a new assignment from the drop-down list. When you override automatic assignments, changes on the LDAP server do not update the user's assignments.

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



Policy Enforcement Type: ○ Standard ● Schedule-Based

Policy Schedule: General Staff

Policy Suite During Schedule: Policy A

Policy Suite Outside Schedule: Policy B

Device Connection Schedule: CAS

Liability: Corporate

Ownership: Company

Plan Type: Domestic

Carrier: None

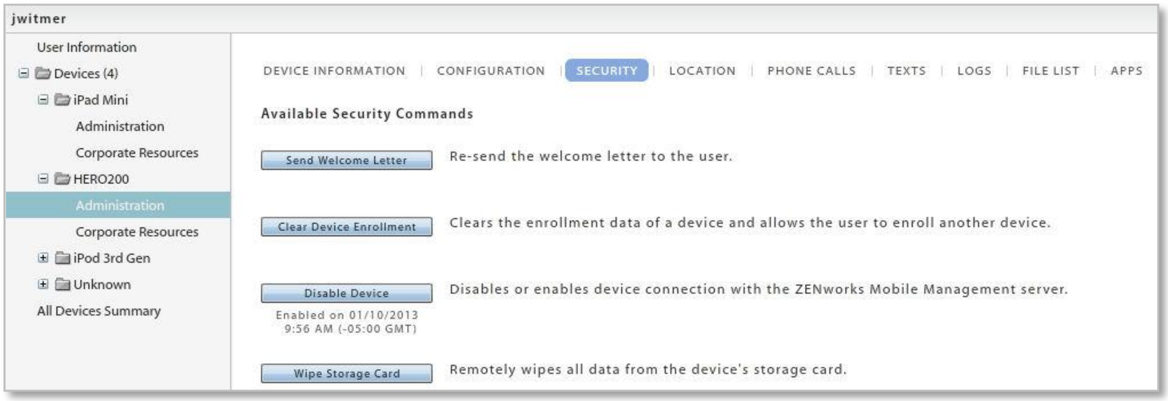
Restricted Apps: Policy B ×

Blacklists	Permissions
Default	NO
Whitelists	**Permissions**
Default	YES

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.



Available Security Commands

Send Welcome Letter — Re-send the welcome letter to the user.

Clear Device Enrollment — Clears the enrollment data of a device and allows the user to enroll another device.

Disable Device — Disables or enables device connection with the ZENworks Mobile Management server.
Enabled on 01/10/2013
9:56 AM (-05:00 GMT)

Wipe Storage Card — Remotely wipes all data from the device's storage card.

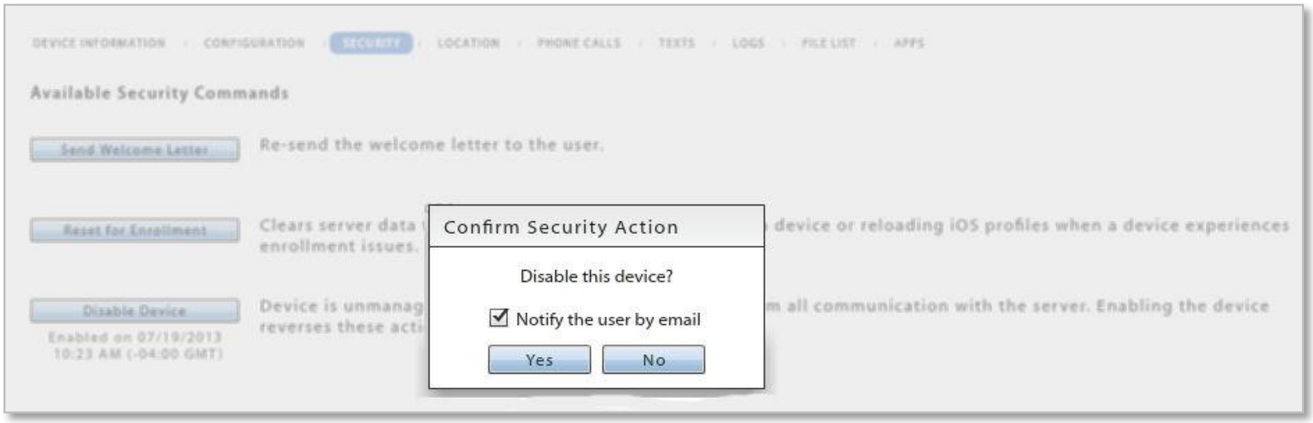
How Security Commands are Issued

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

Stop Managing Devices, 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 *Stop Managing Devices* 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.



Available Security Commands

Re-send the welcome letter to the user.

Clears server data … device or reloading iOS profiles when a device experiences enrollment issues.

Device is unmanag… m all communication with the server. Enabling the device reverses these acti…

Enabled on 07/19/2013 10:23 AM (-04:00 GMT)

Confirm Security Action

Disable this device?

☑ Notify the user by email

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	**S60**	Symbian S60 3rd edition devices
TD/A	*Android devices with TouchDown*	**WM**	Windows Mobile 6.1/6.5 devices
NS/BB	*NotifySync for BlackBerry*	**wOS**	webOS devices
iOS	iOS multitasking devices	**WP**	Windows Phone devices
TD/iOS	iOS multitasking devices with TouchDown	**BB10**	BlackBerry 10 devices

Action	Description	Devices that Support
Full Wipe	Administrators can issue a Full Wipe command. The device remains on the user grid. Functionality varies by device. (Administrators can issue the *Disable* or *Suspend Device* command as well, if the device needs to be temporarily blocked.) *Android w/ native ActiveSync account (requires OS v2.2 or greater):* 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. *Android w/TouchDown (requires OS v2.2 or greater):* The device returns to	**ZENworks Mobile Management app:** Anrd, NS/BB, iOS, TD/iOS, TD/A, WM, S60 **ActiveSync only:** BB10, wOS, WP

	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. *Android w/TouchDown using OS v2.0 or 2.1:* Full Wipe not available – use the *Stop Managing Device* option to wipe the data associated with TouchDown. *BlackBerry*: Requires the *NotifySync for BlackBerry* application. Removes all mail and PIM data associated with the NotifySync application and removes the NotifySync account. Locks the device if *Require Password* is enabled. Erases NotifySync data from the SD card. *iOS*: 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. *Full Wipe* is applied immediately. *Symbian*: The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Some models (N95 and 6120c) wipe only *Mail for Exchange* data. Erases the SD card. *WM*: The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Erases the SD card only on Professional devices. *webOS and WP:* 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.	
Stop Managing Device	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. Android (native): Devices with native mail app only wipe the ZENworks Mobile Management account. Mail/PIM is not wiped. 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.) Devices without ZENworks Mobile Management app: The only action performed is to remove device from the *ZENworks Mobile Management* server and dashboard grid. Mail/PIM is not wiped.	**ZENworks Mobile Management app:** Anrd, NS/BB, iOS, TD/iOS, TD/A, S60, WM **ActiveSync only:** BB10, wOS, WP
Remove User	Stops managing all devices associated with the user and subsequently removes the user from the *ZENworks Mobile Management* server and dashboard grid.	**ZENworks Mobile Management app:** Anrd, NS/BB, iOS, TD/iOS, TD/A, WM, S60 **ActiveSync only:** BB10, wOS, WP7
Wipe Storage Card	Remotely wipes all data from the device's storage card.	**ZENworks Mobile Management app:** Anrd, NS/BB, TD/A, WM
Lock Device	Remotely locks the device, requiring a password to be entered before the device can be used. *Android or Android w/TouchDown:* Requires OS v2.2 or greater. *iOS* allows for *Lock Device* to be applied immediately to iOS devices.	**ZENworks Mobile Management app:** Anrd, NS/BB, TD/A, iOS, TD/iOS, WM
Disable / Enable Device	Device is unmanaged while disabled and thus blocked from all communication with the server. It does not occupy a license seat in this state.	**ZENworks Mobile Management app:** Anrd, NS/BB, iOS, TD/iOS, TD/A, WM,

		S60 **ActiveSync only:** BB10, wOS, WP
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, Mobile 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, WM, S60 **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 *ZENworks Mobile Management* User Self-Administration portal. See *Enabling Password Recovery** below.	**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

*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.

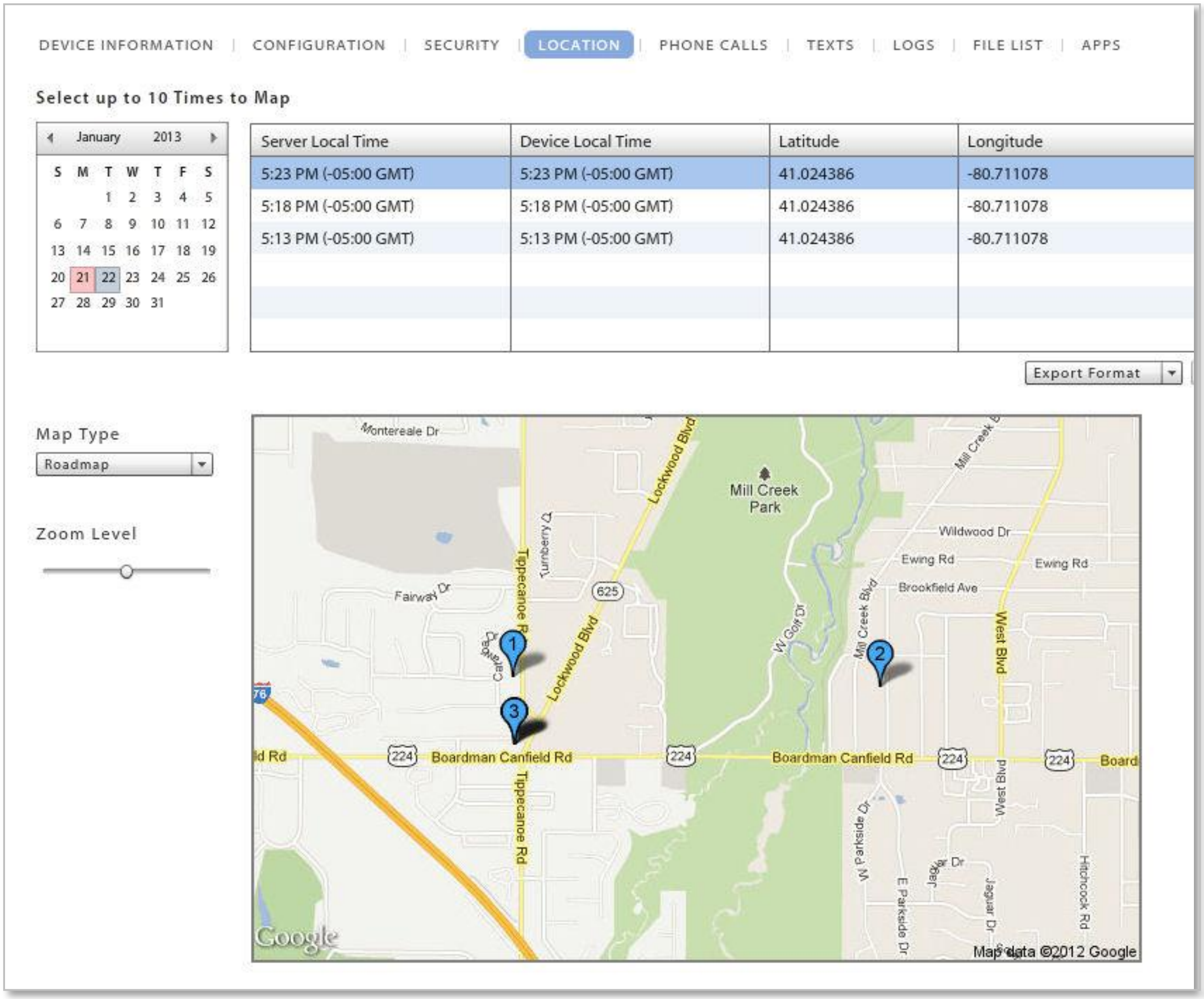
Device Administration: Location

(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*



Select up to 10 Times to Map

January 2013

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

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

Map Type: Roadmap

Zoom Level

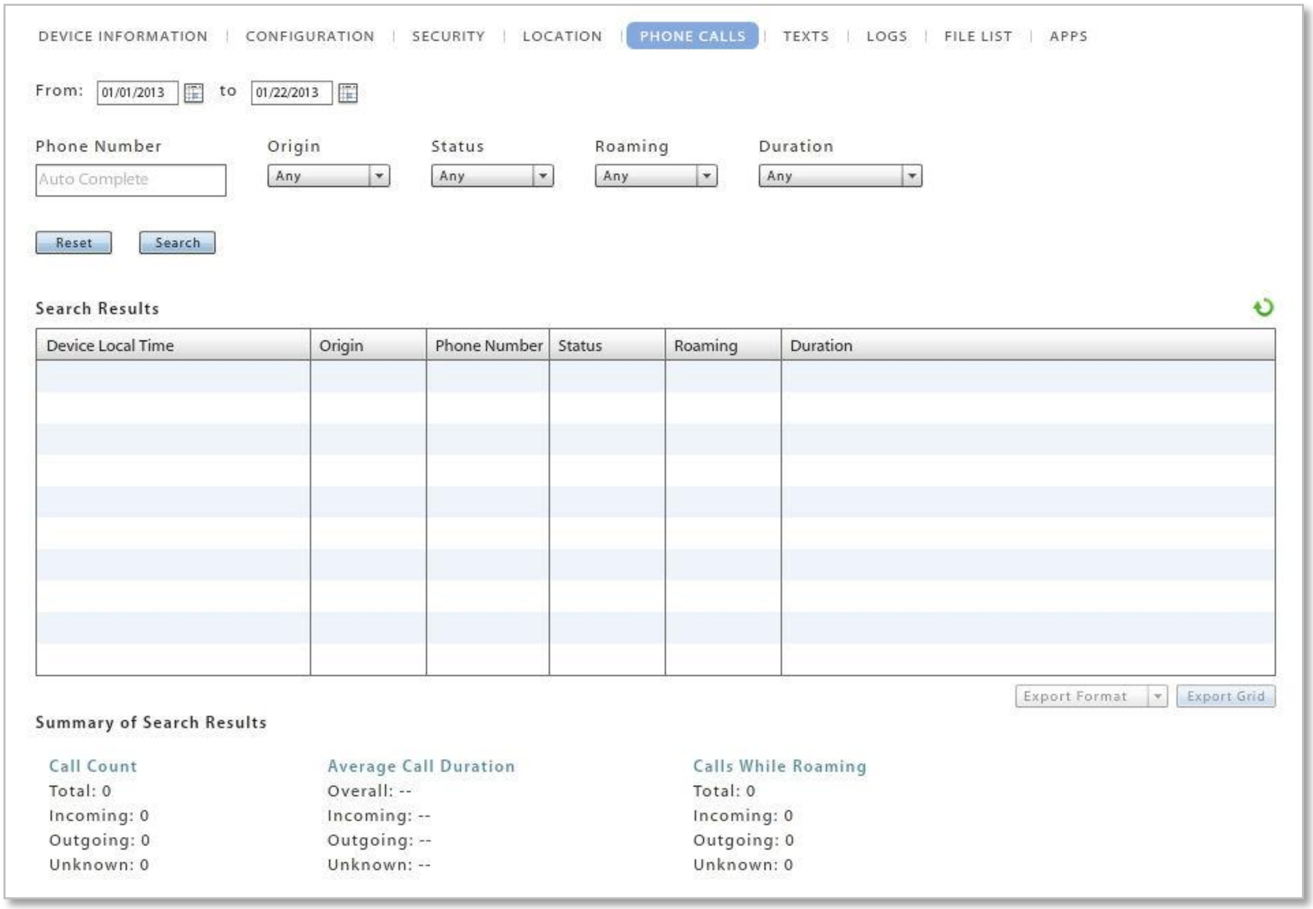
On the action bar, click the ***Get Most Recent Data*** button to refresh the location data.
Click the ***Locate on Google Maps*** button to view a Google Map and the location address.

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.



From: 01/01/2013 to 01/22/2013

Phone Number: Auto Complete

Origin: Any

Status: Any

Roaming: Any

Duration: Any

Search Results

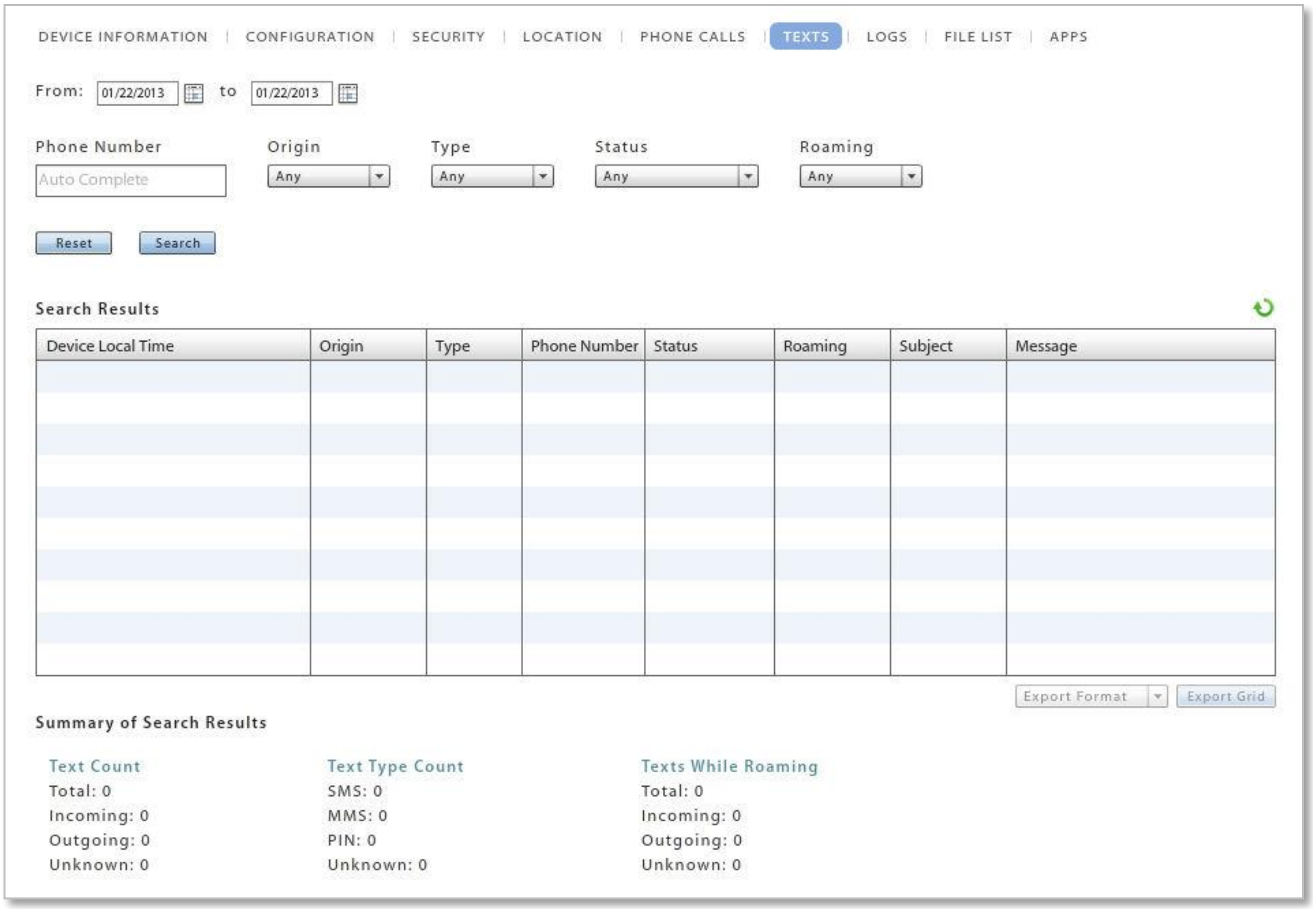
Device Local Time	Origin	Phone Number	Status	Roaming	Duration

Summary of Search Results

Call Count	Average Call Duration	Calls While Roaming
Total: 0	Overall: --	Total: 0
Incoming: 0	Incoming: --	Incoming: 0
Outgoing: 0	Outgoing: --	Outgoing: 0
Unknown: 0	Unknown: --	Unknown: 0

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

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


DEVICE INFORMATION | CONFIGURATION | SECURITY | LOCATION | PHONE CALLS | TEXTS | LOGS | FILE LIST | APPS
Reset
Search
Export Format
Export Grid

From: 01/22/2013 to 01/22/2013

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.
- **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.
- **Data Usage Log** – Track the amount of data being exchanged:
    - Between the device's *ZENworks Mobile Management* app and the *ZENworks Mobile Management server*
    - Between the device's ActiveSync client and the *ZENworks Mobile Management* server
    - As iOS MDM traffic between the device and the *ZENworks Mobile Management* servers
    - Between the *ZENworks Mobile Management* and ActiveSync servers
- **Device Log** – to request and view a log from a device running the *ZENworks Mobile Management* application.
- **Error Chain Log** – to view detailed messages for errors logged in the *iOS MDM Sync Log*. (iOS device specific)

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

Synchronization Logs

Synchronization logs give administrators the ability to view events associated with a particular device that have been logged during connections between servers and between the device and servers. There are three logs of this type.

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

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

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

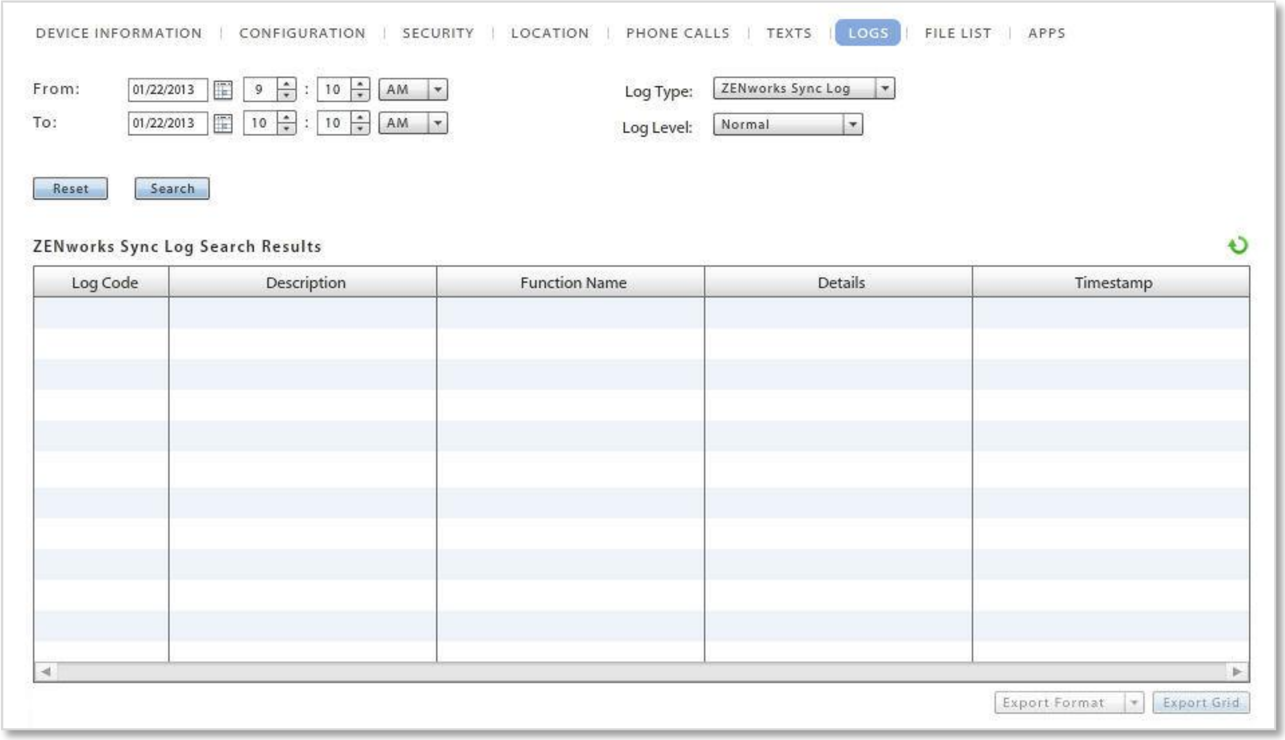
The logs display:

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

Select ***ActiveSync Log***, ***ZENworks Sync Log***, or ***iOS MDM Sync Log*** from the drop-down list.

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

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


DEVICE INFORMATION | CONFIGURATION | SECURITY | LOCATION | PHONE CALLS | TEXTS | LOGS | FILE LIST | APPS
Reset
Search
Export Format
Export Grid

From: 01/22/2013 9 : 10 AM

To: 01/22/2013 10 : 10 AM

Log Type: ZENworks Sync Log

Log Level: Normal

ZENworks Sync Log Search Results

Log Code	Description	Function Name	Details	Timestamp

Sample Synchronization Log Grid

Data Usage Log

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

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

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

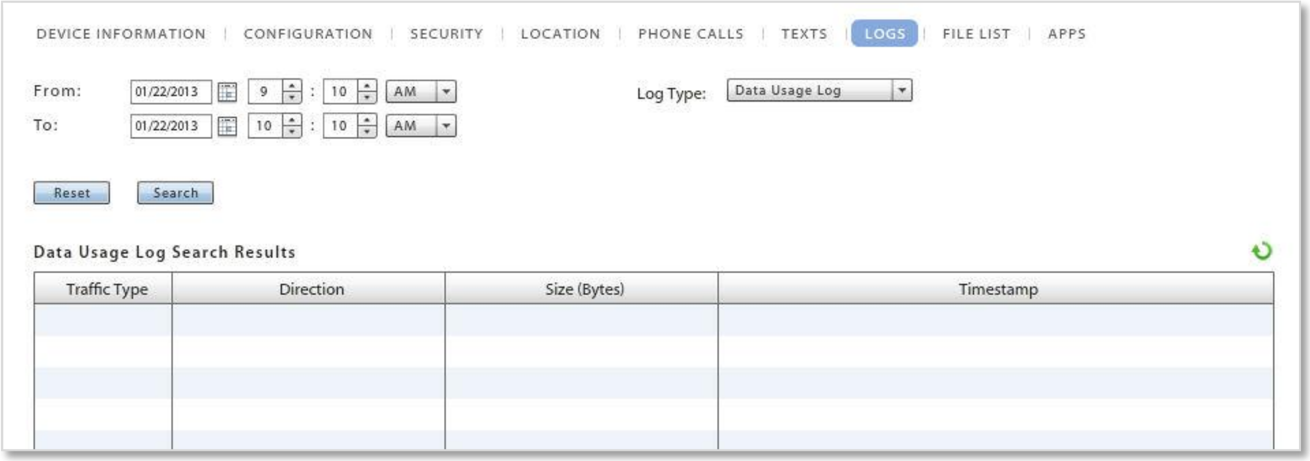
The log displays:

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

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

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

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



From: 01/22/2013 9 : 10 AM

To: 01/22/2013 10 : 10 AM

Log Type: Data Usage Log

Data Usage Log Search Results

Traffic Type	Direction	Size (Bytes)	Timestamp

Device Logs

The device logging option can be used to request a log from any device running the *ZENworks Mobile Management* application or a BlackBerry device running the *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. *ZENworks* logging must be enabled on the device (*Log Settings*). The *ZENworks* log is written to the SD card.
BlackBerry (with *NotifySync*)	BlackBerry devices must have logging enabled on the device (*Log Settings*) and must have an SD card.
iOS	No special requirements. Logging is always enabled on iOS devices.
Symbian S60, 3	*ZENworks* Logging must be enabled on the device (*Log Settings*).
Windows Mobile 6	*ZENworks* Logging must be enabled on the device (*Log Settings*).

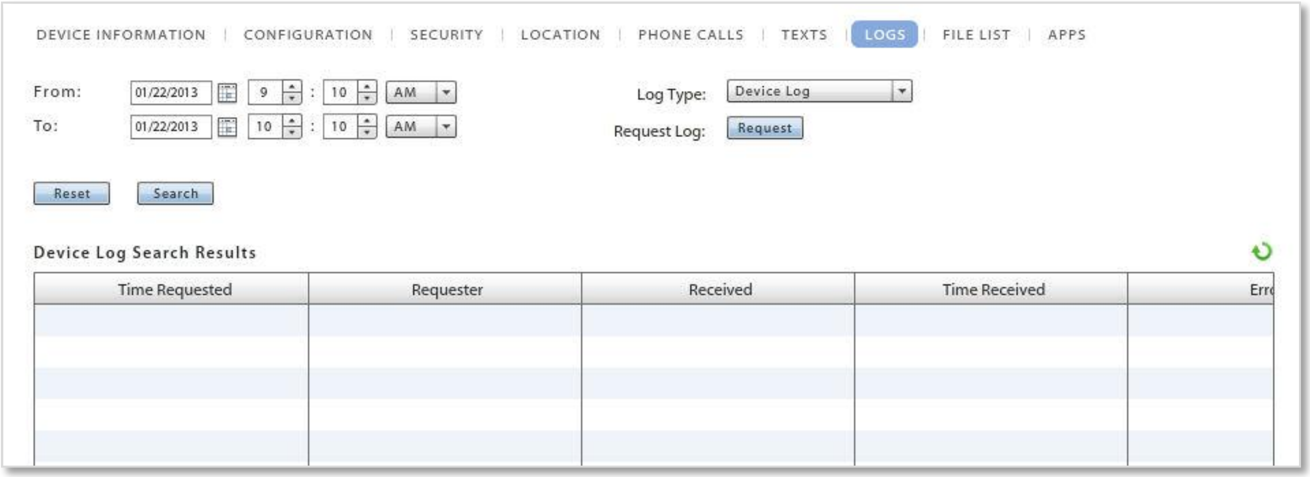
Select ***Device Log*** from the drop-down list.

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



From: 01/22/2013 9 : 10 AM
To: 01/22/2013 10 : 10 AM
Log Type: Device Log
Request Log:

Device Log Search Results

Time Requested	Requester	Received	Time Received	Err

Device Log Grid

When the log has been received, select the log file and click the **Download Log** button. Save the log file on the Desktop or in another designated folder. The file can be viewed in the .txt format.

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

Error Chain Log (iOS device specific)

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

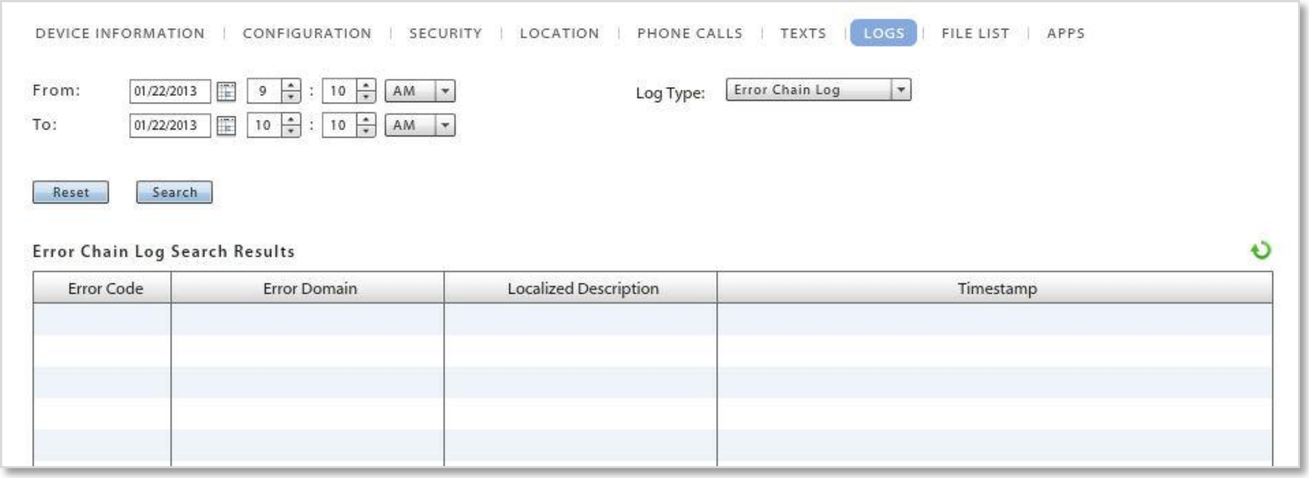
The log displays:

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

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

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

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



From: 01/22/2013 9 : 10 AM

To: 01/22/2013 10 : 10 AM

Log Type: Error Chain Log

Error Chain Log Search Results

Error Code	Error Domain	Localized Description	Timestamp

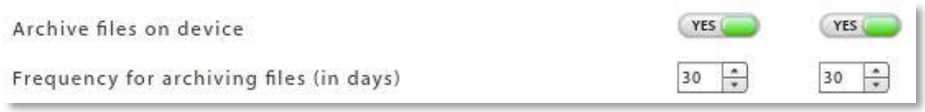
Error Chain Log Grid

Device Administration: File List

(return to Device Administration menu)

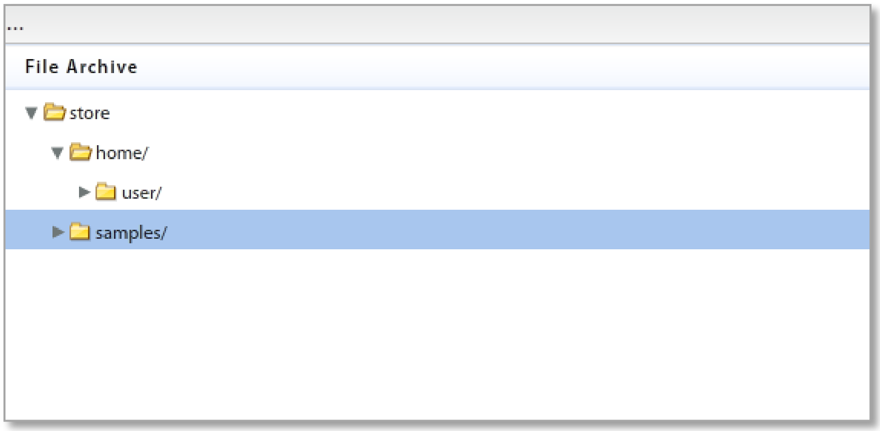
Select the ***File List*** tab to view the file list sent up from the device. The *Archive files on device* policy rule must be enabled in the policy suite to which the user belongs. When the rule is enabled, the device periodically sends a list of all folders and files stored on the device and the SD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

The *Archive files 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.



Archive files on device	YES	YES
Frequency for archiving files (in days)	30	30

The device file directory is displayed in the User Profile.



...

File Archive

- ▼ store
  - ▼ home/
    - ▶ user/
  - ▶ samples/

Device Administration: Applications

(return to Device Administration menu)

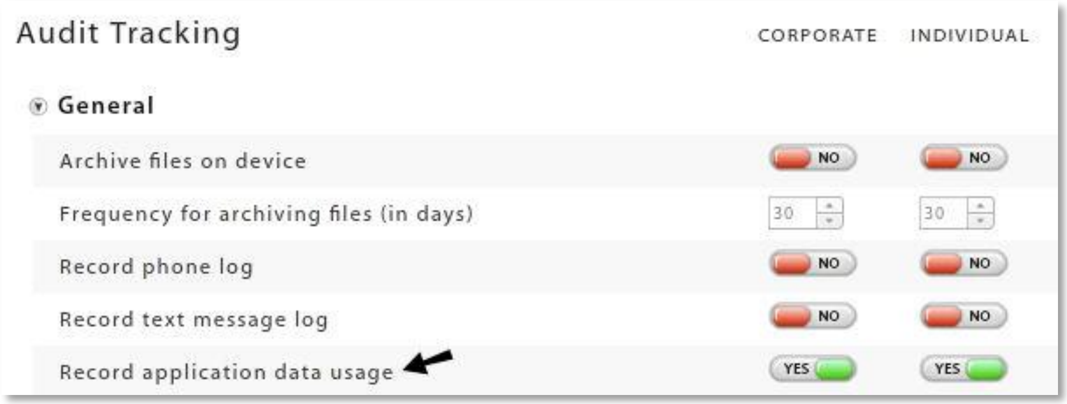
Select the ***Apps*** tab to view the lists of applications on the device. For iOS devices, you can view *Managed Apps* and *Installed Apps*.

Policies That Control Application Reporting and Management

ANDROID

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.

The ***Record application data usage*** policy rule is located in the ***Audit Tracking*** > ***General*** category of each policy suite.



Audit Tracking

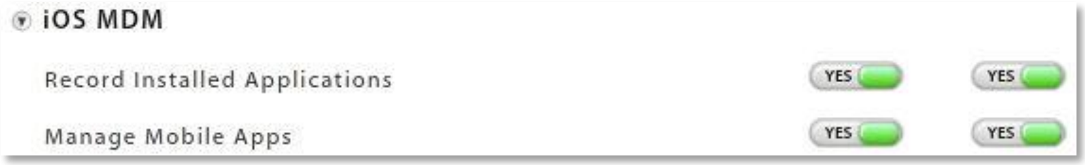
General

	CORPORATE	INDIVIDUAL
Archive files on device	NO	NO
Frequency for archiving files (in days)	30	30
Record phone log	NO	NO
Record text message log	NO	NO
Record application data usage	YES	YES

IOS

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 ***Manage Mobile Apps*** policy rules are located in the ***iOS Devices: iOS MDM*** category of each policy suite. Changes to these access rights will require iOS device users to reload a new APN profile.



iOS MDM

Record Installed Applications	YES	YES
Manage Mobile Apps	YES	YES

Managed Apps

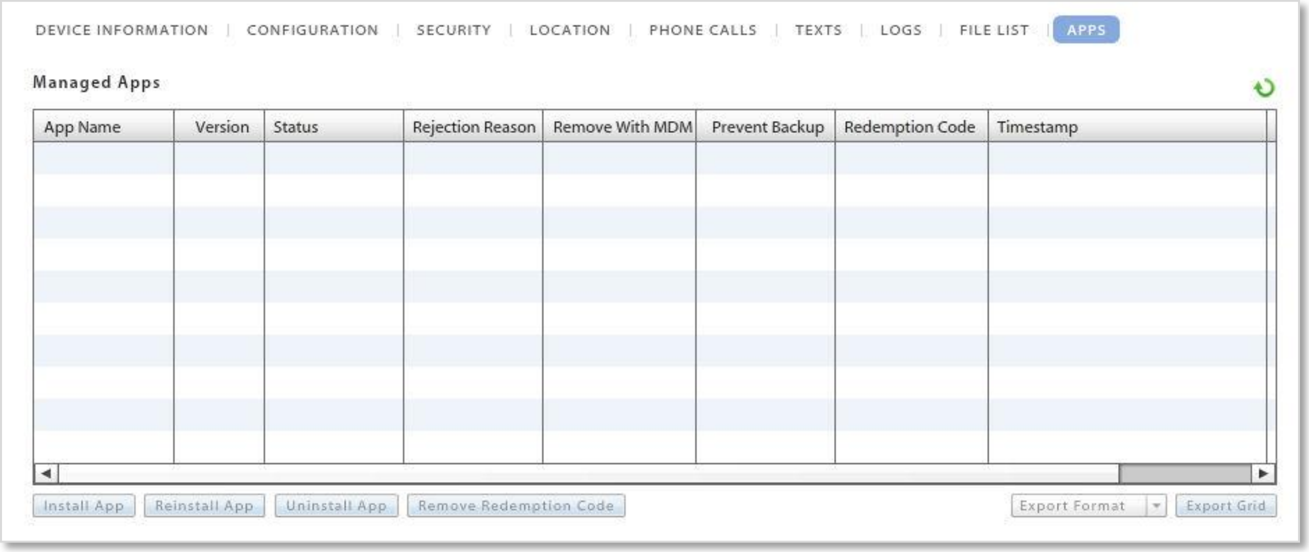
The ***Managed Apps*** grid lists all applications available to an Android or iOS 5+ user as determined by the *Mobile App Permissions* on the policy suite with which the user is associated.

When administrators add applications to the Android or iOS app permissions list via the policy suite, a user can access the list on the device and conveniently installed apps from the list. If the policy suite also has the *Manage Mobile Apps* 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. For iOS devices, administrators can also remove an invalid Redemption Code for a Volume Purchase Program (VPP) app.

A managed app is one that has been installed on the device through MDM by either the user, an administrator, or by a forced push of the application.

Applications that are not installed through MDM or those already existing on the device before the app was made available through MDM appear on the *Installed Apps* list and cannot be managed.

iOS Managed Apps Grid

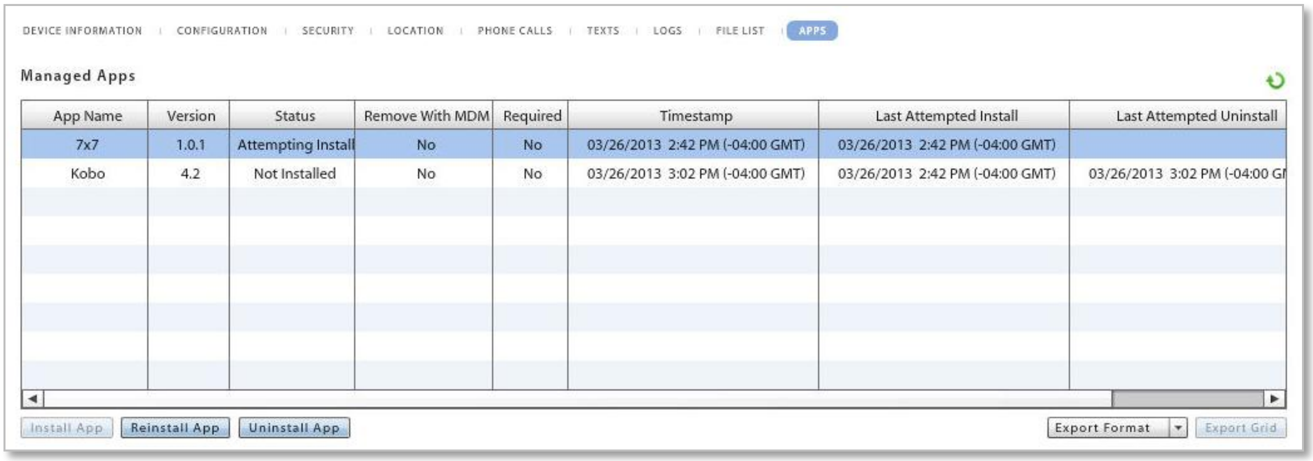


Managed Apps

App Name	Version	Status	Rejection Reason	Remove With MDM	Prevent Backup	Redemption Code	Timestamp

Information in the iOS Managed Apps Grid	
Status	The most common status messages include: • *Managed* – Indicates that the app is installed on the device • *Not Installed via MDM* – Indicates that the app is available through *ZENworks Mobile Management*, but is not required and has not been installed by *ZENworks*. • *Managed, but Uninstalled* – Indicates an app that is not installed; possibly because it was removed by the user or is not required. Other status messages give additional information about apps on the device.
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.
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 *Force Push* 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.

ANDROID MANAGED APPS GRID



Managed Apps

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

Information in the Android Managed Apps Grid	
Version	Application version number.
Status	Status messages include: • *Not Installed* – Application is not installed • *Pending Install* – Server has issued a *Force Push* for the application • *Attempting Install* – Device has received the *Force Push* and is in the process of installing the app • *Managed* – Application is installed and managed • *Pending Uninstall* – Server has pushed an uninstall command for the app • *Attempting Uninstall* – Device has received the uninstall command and is in the process of uninstalling the app
Remove with MDM	Whether this app is removed, along with its data, if the MDM profile is removed.
Required	Whether the application is one that has been Force Pushed to the device.
Timestamp	Date and time of the last update of the app’s status.
Last Attempted Install	Date and time of the last attempted installation of the app.
Last Attempted Uninstall	Date and time of the last attempted removal of the app.
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 *Force Push* option should be disabled first, so that the app does not get pushed back to the device after the user uninstalls it.

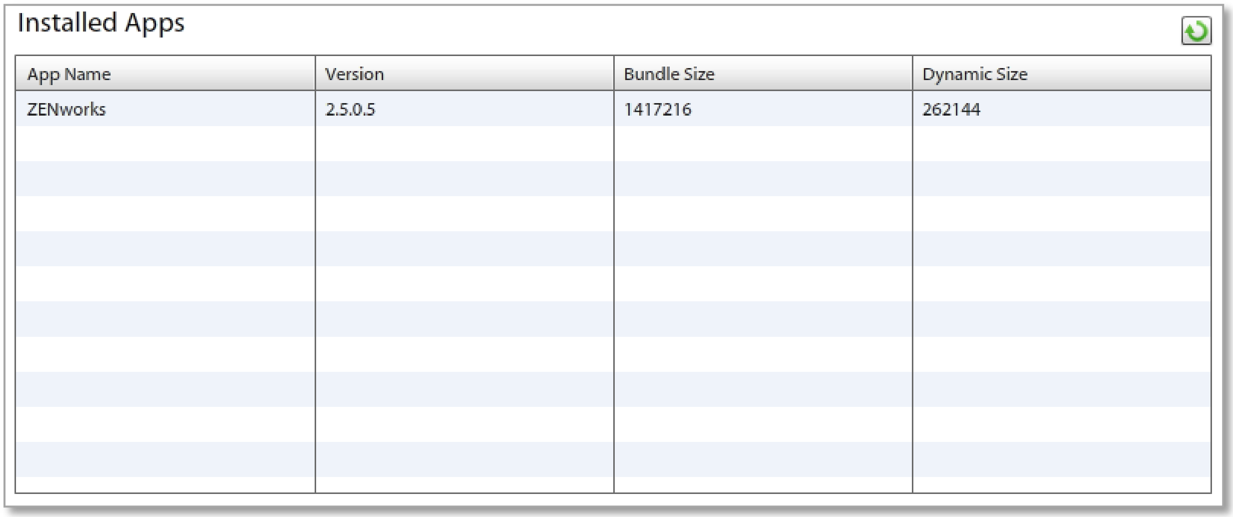
Installed Apps

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 application data usage* policy rule is 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.

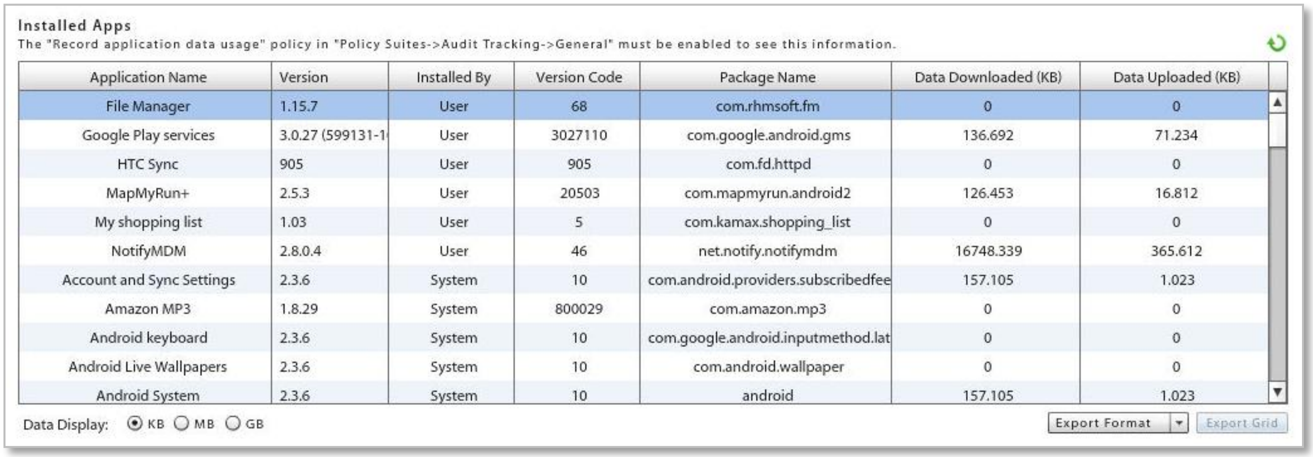
IOS INSTALLED APPS GRID



Installed Apps

App Name	Version	Bundle Size	Dynamic Size
ZENworks	2.5.0.5	1417216	262144

ANDROID INSTALLED APPS GRID



Installed Apps

The "Record application data usage" policy in "Policy Suites->Audit Tracking->General" must be enabled to see this information.

Application Name	Version	Installed By	Version Code	Package Name	Data Downloaded (KB)	Data Uploaded (KB)
File Manager	1.15.7	User	68	com.rhmsoft.fm	0	0
Google Play services	3.0.27 (599131-1	User	3027110	com.google.android.gms	136.692	71.234
HTC Sync	905	User	905	com.fd.httpd	0	0
MapMyRun+	2.5.3	User	20503	com.mapmyrun.android2	126.453	16.812
My shopping list	1.03	User	5	com.kamax.shopping_list	0	0
NotifyMDM	2.8.0.4	User	46	net.notify.notifymdm	16748.339	365.612
Account and Sync Settings	2.3.6	System	10	com.android.providers.subscribedfee	157.105	1.023
Amazon MP3	1.8.29	System	800029	com.amazon.mp3	0	0
Android keyboard	2.3.6	System	10	com.google.android.inputmethod.lat	0	0
Android Live Wallpapers	2.3.6	System	10	com.android.wallpaper	0	0
Android System	2.3.6	System	10	android	157.105	1.023

Data Display: ● KB ○ MB ○ GB

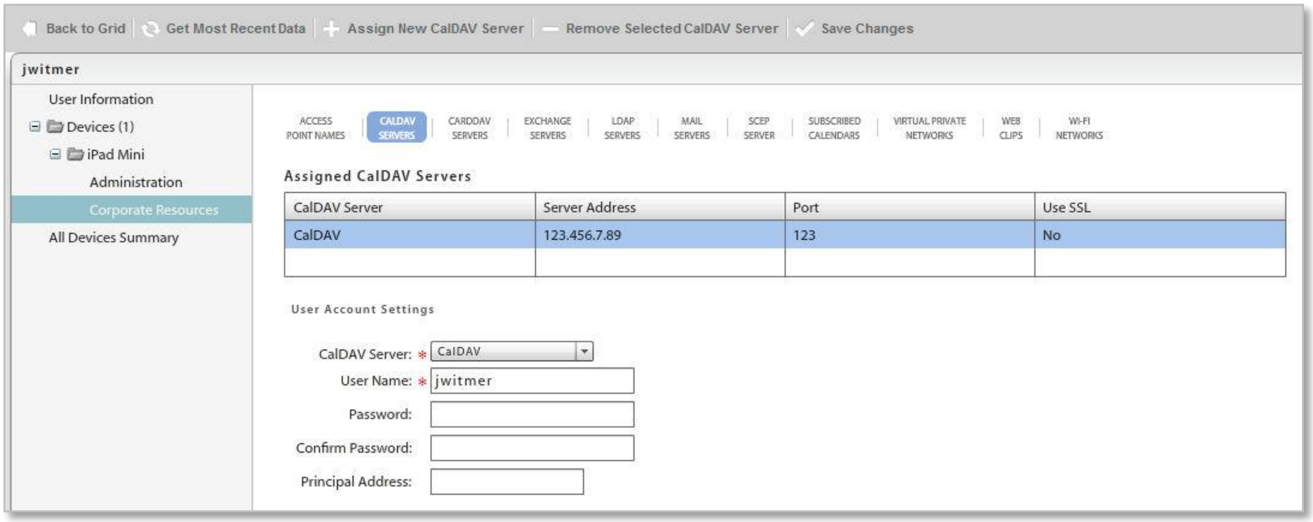
Corporate Resource Assignments

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 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 Subscribed Calendars, Web Clips, and an Access Point Name.

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

> **Note:** Configuration of these resources is done from the *Organization* view. See Managing Corporate Resources.

To assign a resource, select **Corporate Resources** from the left panel of the *User Profile*.
Click the tab of the resource you want to assign



Assigned CalDAV Servers

CalDAV Server	Server Address	Port	Use SSL
CalDAV	123.456.7.89	123	No

User Account Settings

CalDAV Server: * CalDAV
User Name: * jwitmer
Password:
Confirm Password:
Principal Address:

Sample iOS Resource Assignment

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 reasons for changing the Access Point Name.

Mail Servers*. Associate the user with a mail server and configure email account settings 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.

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.

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.

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

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.

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.

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.

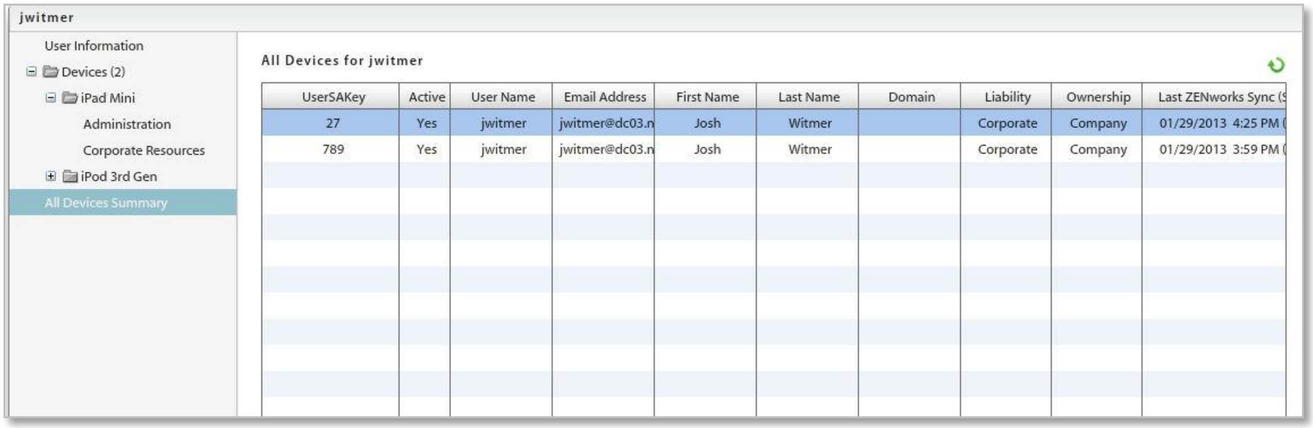
Mail Servers** and **Assign Exchange Servers have two options that can be enabled/disabled to govern how the mail account can be used by an iOS 5+ user. If they are set when the resource is created, however, they cannot be changed at the user level.

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

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

Device Summary

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



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

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:

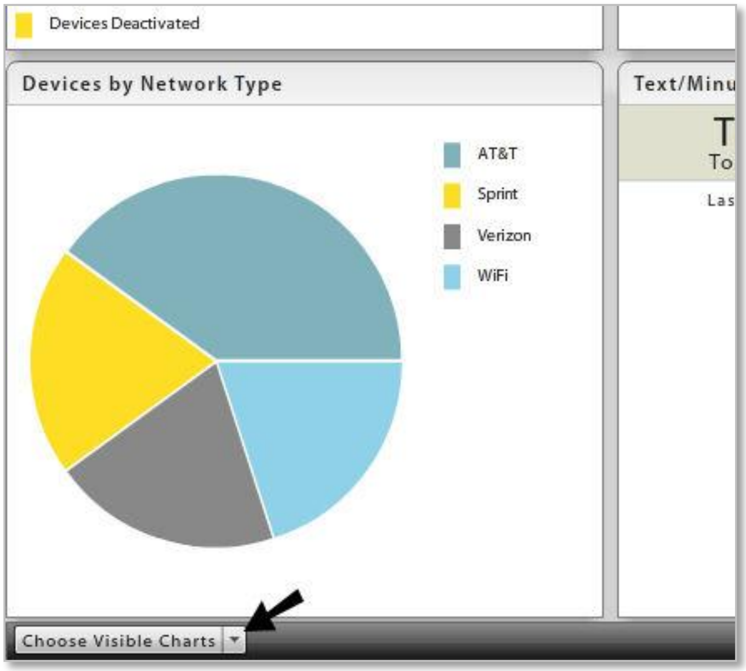
Configuration	
Activation/De-Activation History	Bar chart showing the number of devices activated and deactivated in the past seven days.
Active/Inactive Devices	Pie chart showing the percentage of active devices versus disabled devices.
Devices by Carrier	Pie chart showing the percentage of devices 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 *corporate* liable vs. *individual* 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 *ZENworks Mobile Management* 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 *ZENworks Mobile Management* 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.

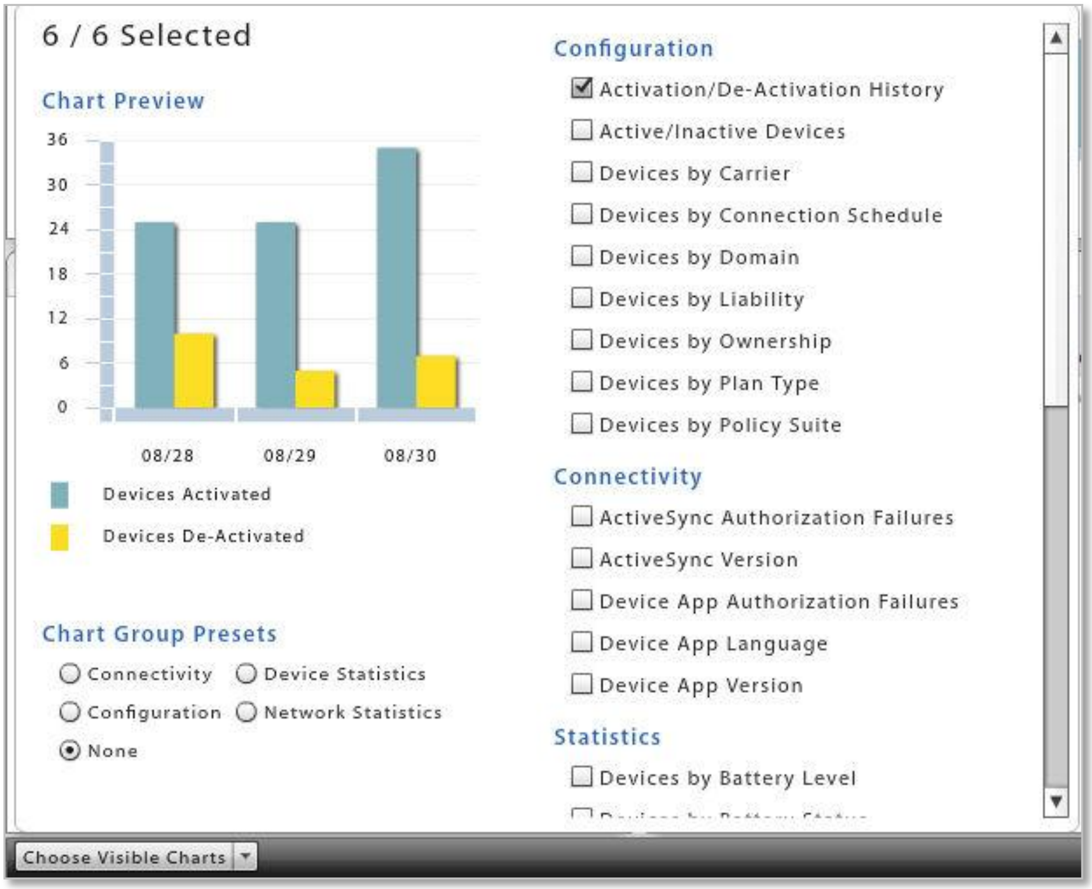
Select Graphs. Click the *Choose Visible Charts* button at the bottom left corner of the Activity Monitor screen. Select the six graphs you want to display on the grid.

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.



6 / 6 Selected

Chart Preview

Chart Group Presets

○ Connectivity ○ Device Statistics
○ Configuration ○ Network Statistics
● None

Configuration

☑ Activation/De-Activation History
□ Active/Inactive Devices
□ Devices by Carrier
□ Devices by Connection Schedule
□ Devices by Domain
□ Devices by Liability
□ Devices by Ownership
□ Devices by Plan Type
□ Devices by Policy Suite

Connectivity

□ ActiveSync Authorization Failures
□ ActiveSync Version
□ Device App Authorization Failures
□ Device App Language
□ Device App Version

Statistics

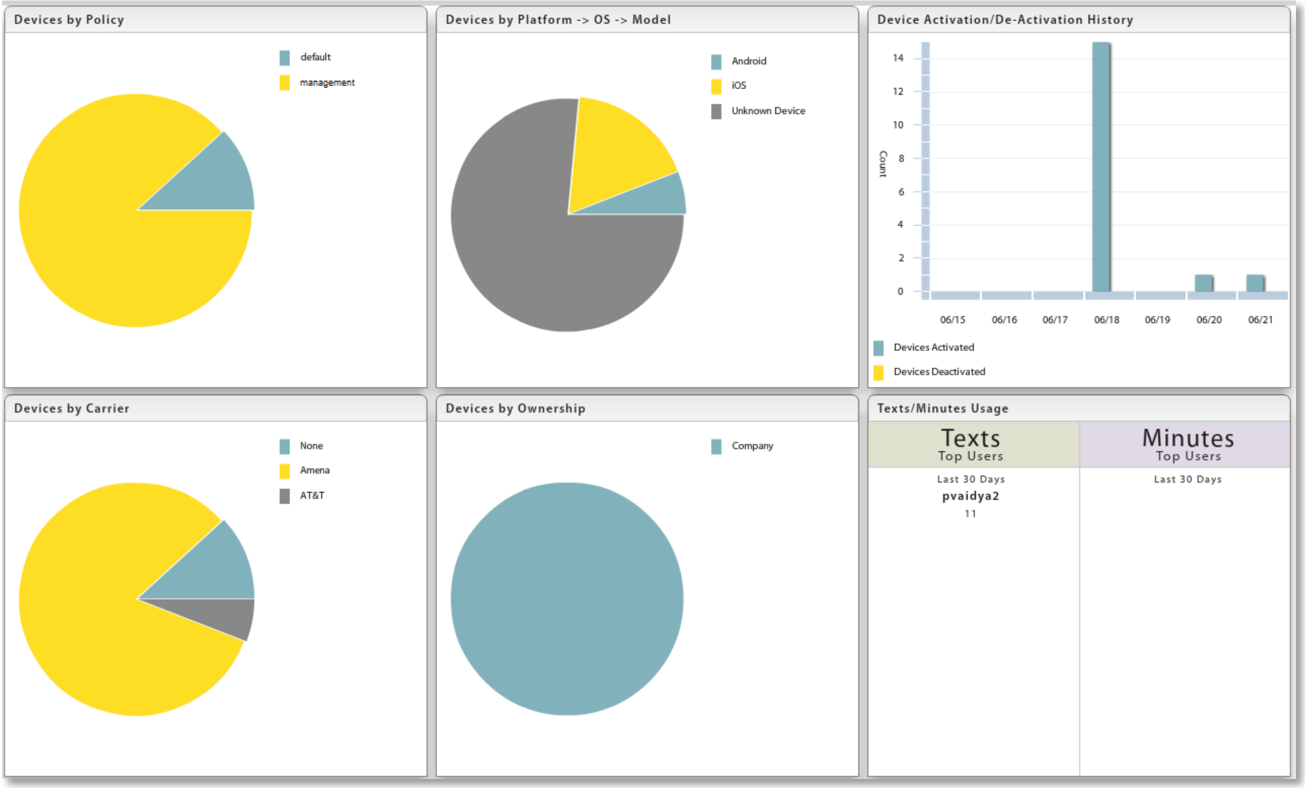
□ Devices by Battery Level

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

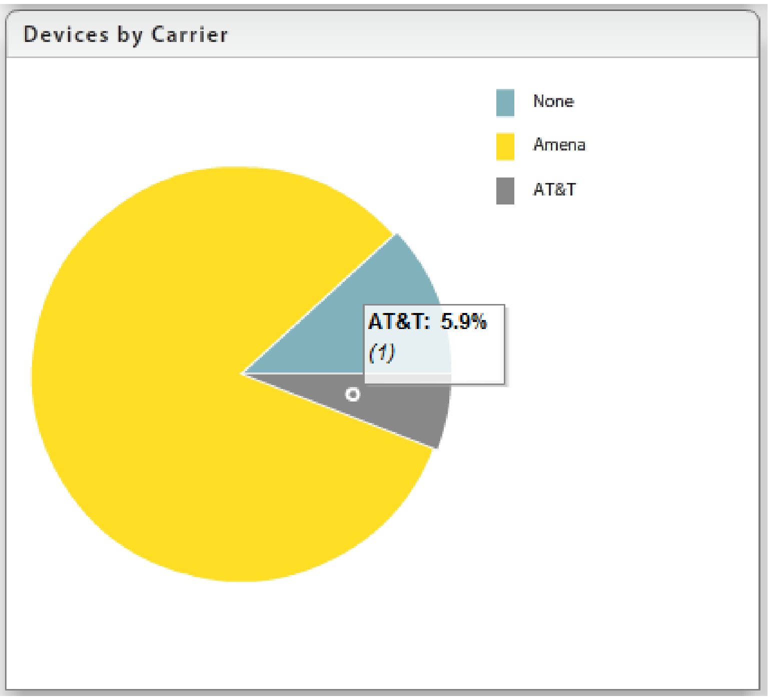
Chart Group Presets. You can choose a preset group of charts.

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

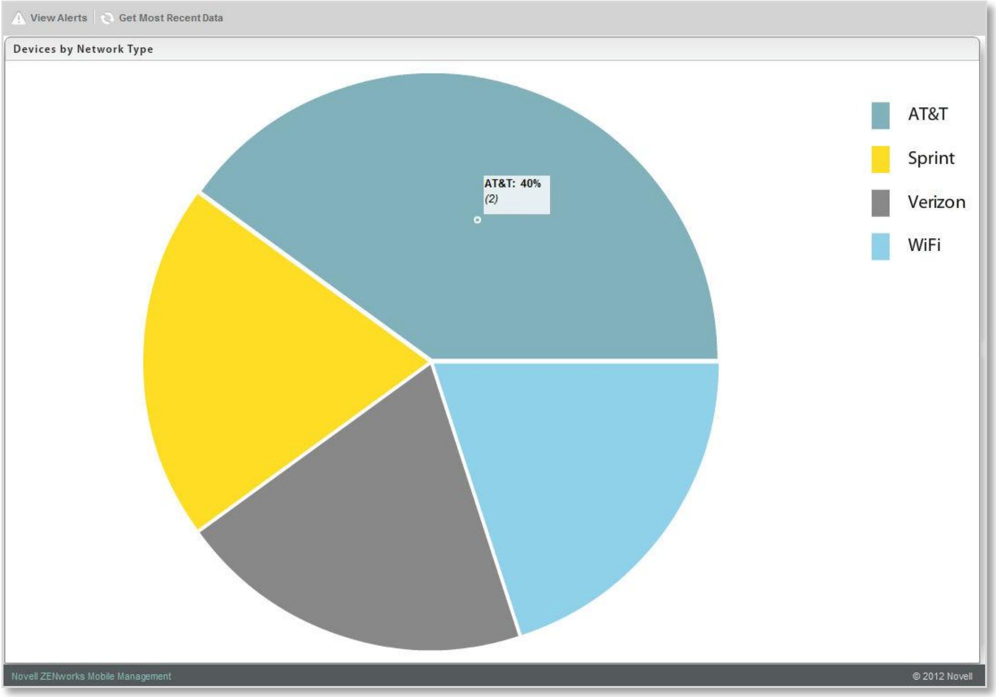
Rearrange Panels. You can rearrange the panels in the view by selecting a block and dragging it and dropping it where you prefer.



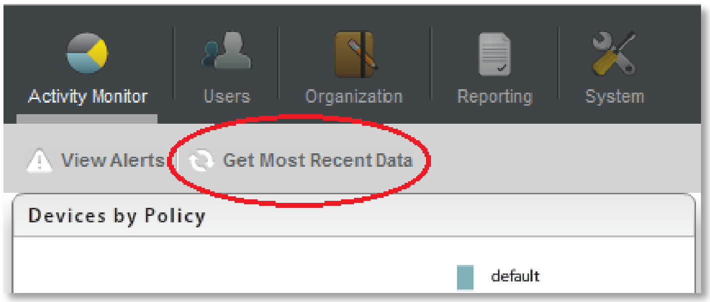
View Details. You can see detail of the statistics by hovering over a section of a graph or chart.



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.

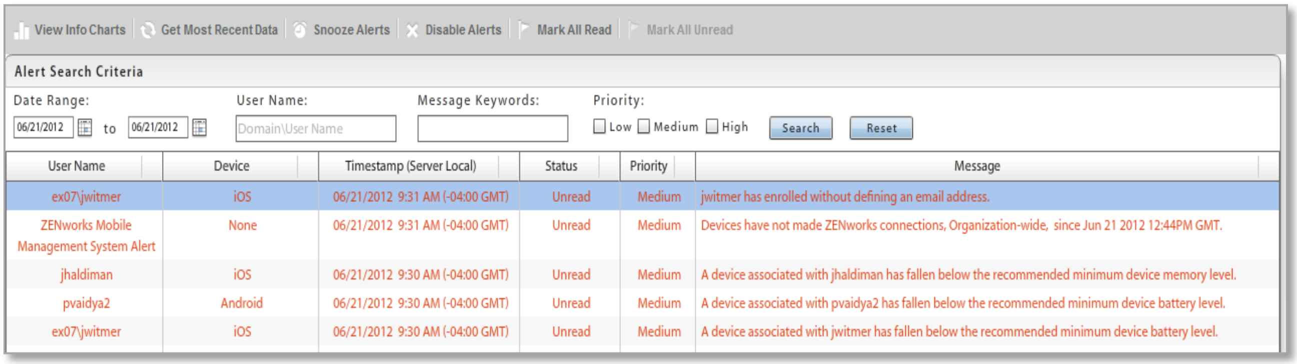


Refresh the View. You can refresh the Activity Monitor view with the most recent data by selecting *Get Most Recent Data* in the gray option bar.



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.



Alert Search Criteria

Date Range: 06/21/2012 to 06/21/2012

User Name: Domain\User Name

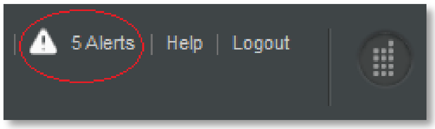
Message Keywords:

Priority: □ Low □ Medium □ High

Search Reset

User Name	Device	Timestamp (Server Local)	Status	Priority	Message
ex07\jwitmer	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.
jhaldiman	iOS	06/21/2012 9:30 AM (-04:00 GMT)	Unread	Medium	A device associated with jhaldiman has fallen below the recommended minimum device memory level.
pvaidya2	Android	06/21/2012 9:30 AM (-04:00 GMT)	Unread	Medium	A device associated with pvaidya2 has fallen below the recommended minimum device battery level.
ex07\jwitmer	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.

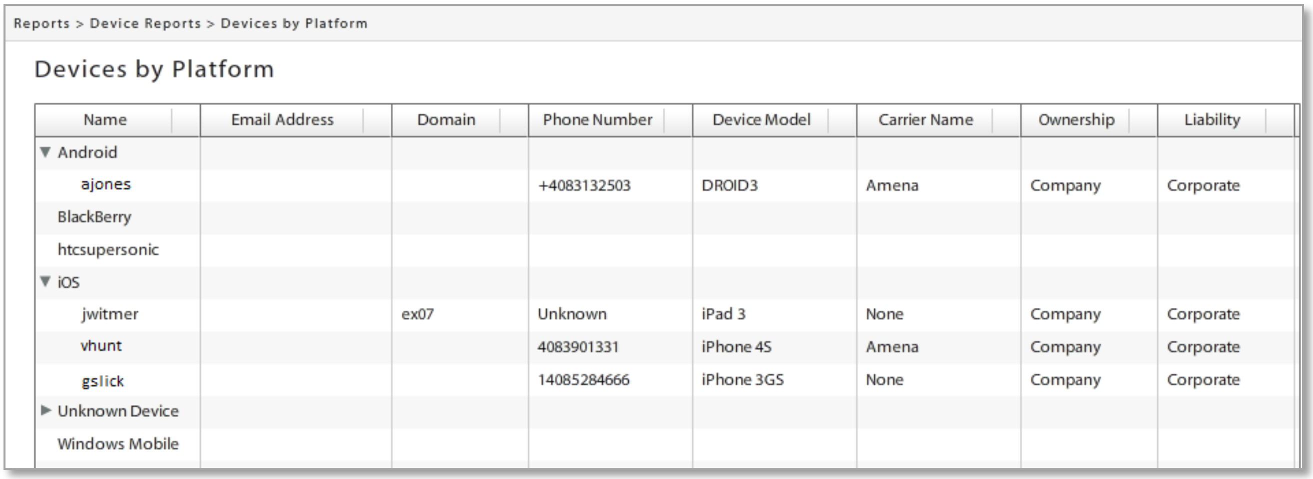
The reports are as follows:

Device Reports	**iOS Resource Reports**
• Data Usage by DeviceSAKey	• Resource by Assignment
• Devices by Liability	• Resource By Expiration Date
• Devices by Network Type	**Compliance Reports**
• Device by OS Version and Model	• Access Restriction Violations
• Device by OS Version and Platform	• Device Platform Restrictions by User
• Devices by Platform	• Exceptions by User
• Devices by Platform and Model	• Resource Restrictions by User
• Devices by Policy Suite	• User by Exceptions
User Reports	**Administrative Roles Reports**
• Data Usage by User	• Organization Administrators
• Users by Carrier	• Organization Roles
• Users by Ownership	• System Administrators
• Users by Expiration Date	• System Roles

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).

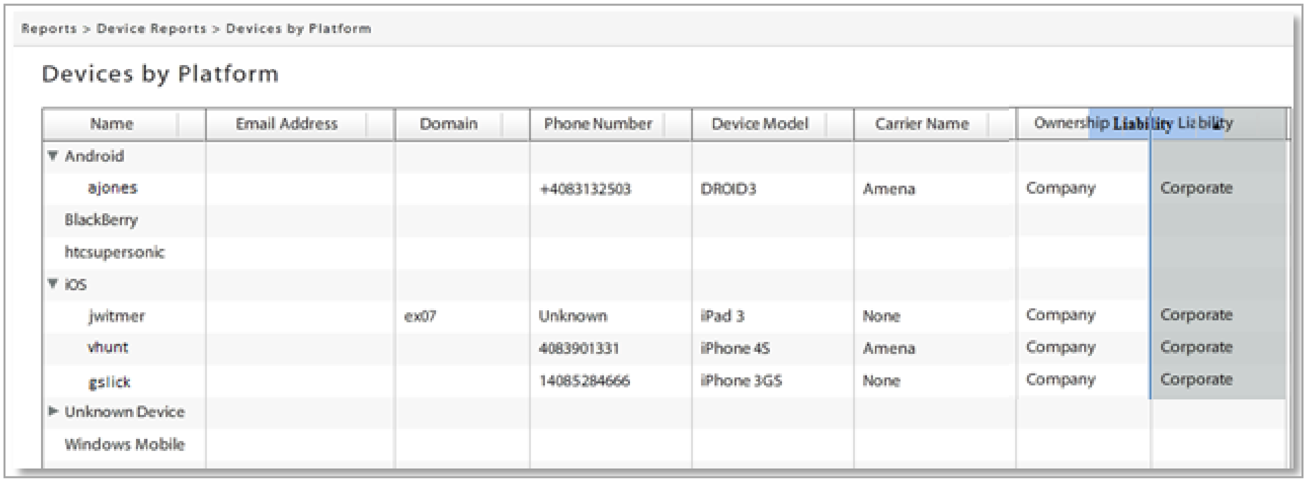


Reports > Device Reports > Devices by Platform

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.

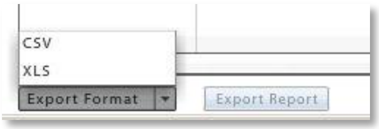


Reports > Device Reports > Devices by Platform

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.

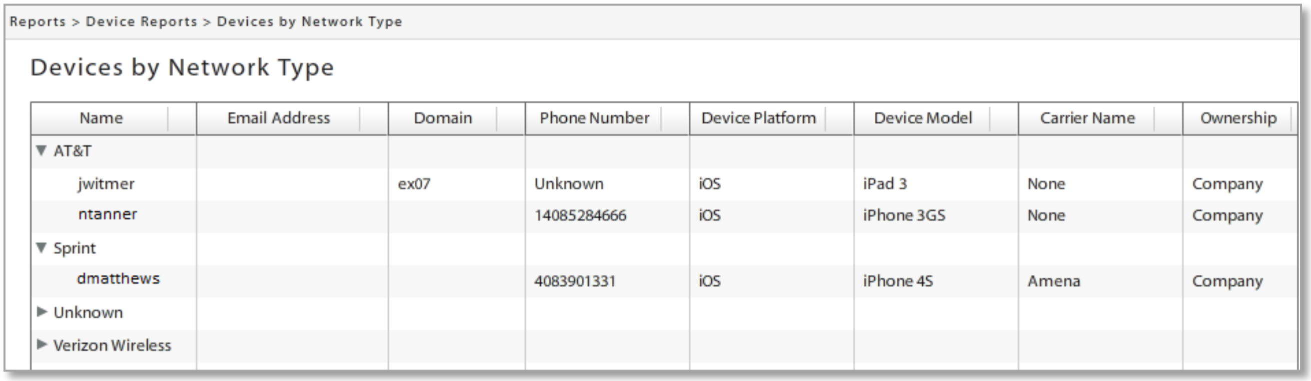


Sample Reports

Sample Device/User Reports

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

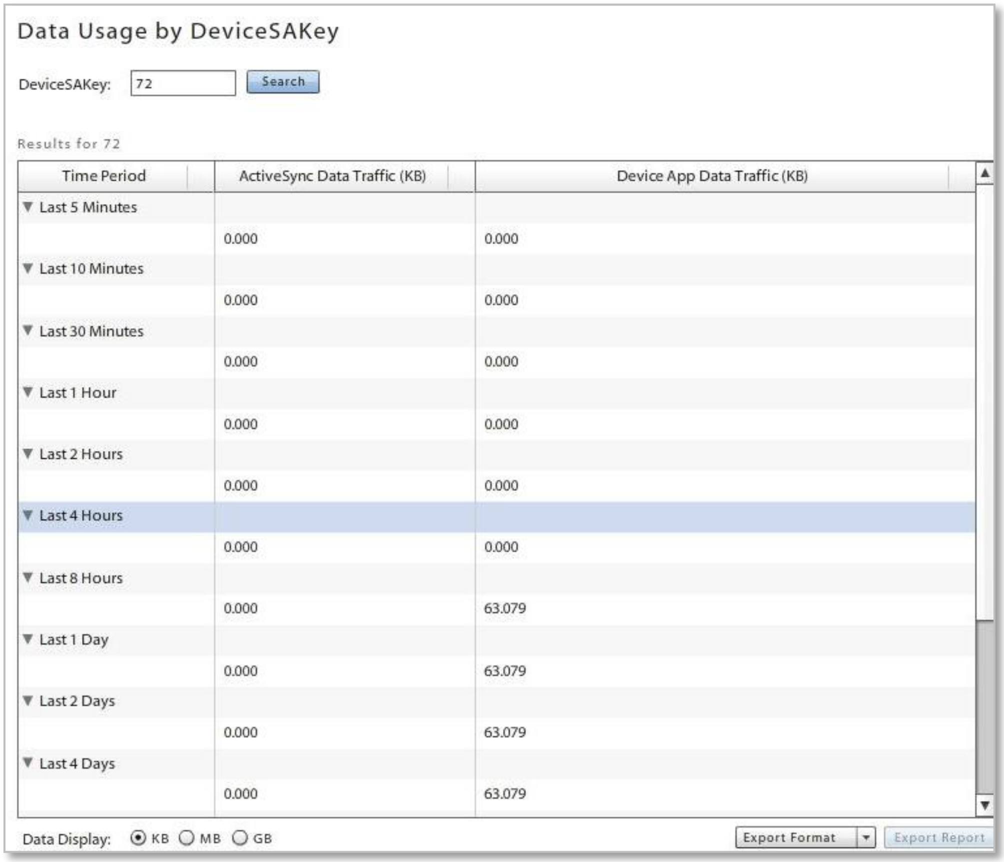
- User Name
- Email Address
- Domain
- Phone Number
- Device Platform
- Device Model
- Carrier Name
- Ownership
- Liability
- OS Version
- AS Version
- Policy Suite
- Device Connection Schedule
- Activation Date



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							



Data Usage by DeviceSAKey

DeviceSAKey: 72

Results for 72

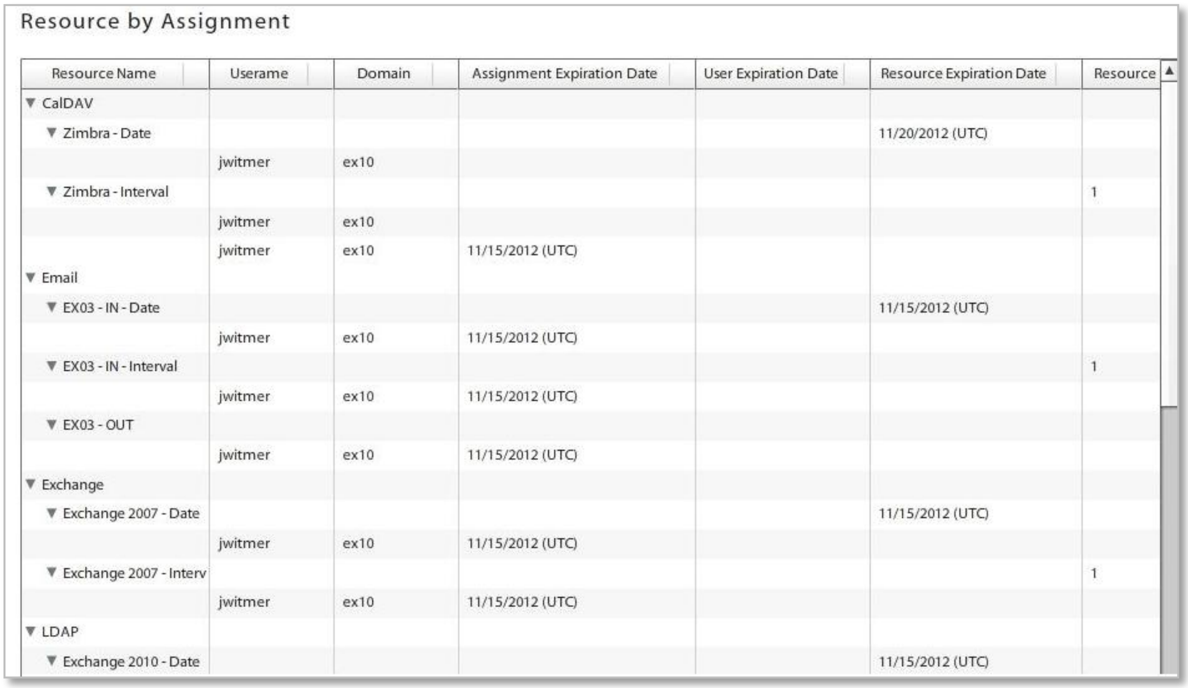
Time Period	ActiveSync Data Traffic (KB)	Device App Data Traffic (KB)
▼ Last 5 Minutes		
	0.000	0.000
▼ Last 10 Minutes		
	0.000	0.000
▼ Last 30 Minutes		
	0.000	0.000
▼ Last 1 Hour		
	0.000	0.000
▼ Last 2 Hours		
	0.000	0.000
▼ Last 4 Hours		
	0.000	0.000
▼ Last 8 Hours		
	0.000	63.079
▼ Last 1 Day		
	0.000	63.079
▼ Last 2 Days		
	0.000	63.079
▼ Last 4 Days		
	0.000	63.079

Data Display: ● KB ○ MB ○ GB

Sample iOS Resource Report

Information included in ***iOS Resource*** reports:

- Resource Name
- User Name
- Domain
- Expiration Dates



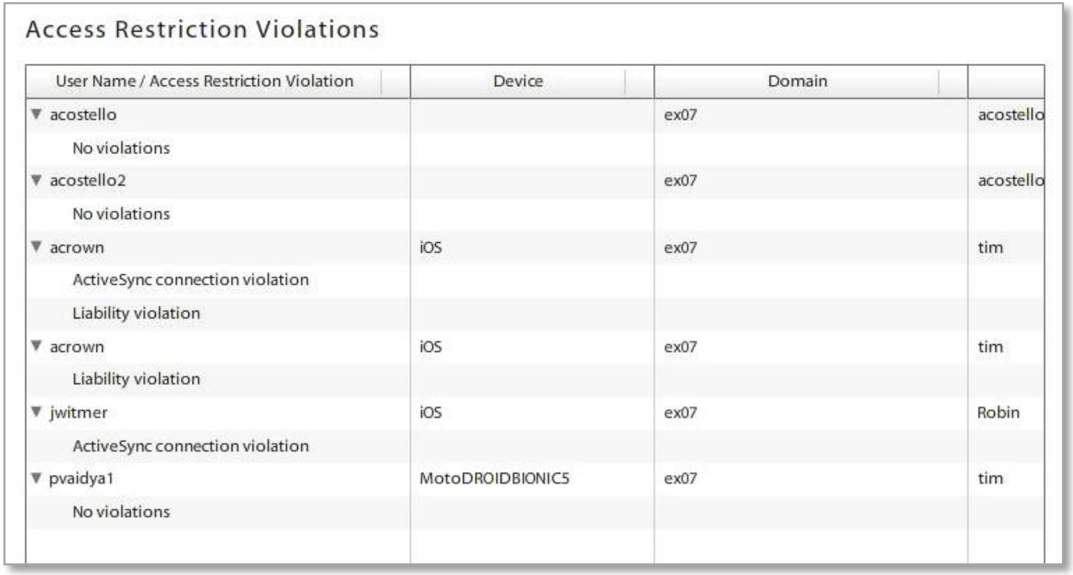
Resource by Assignment

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

Sample Compliance Report

Information included in ***Compliance*** reports:

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



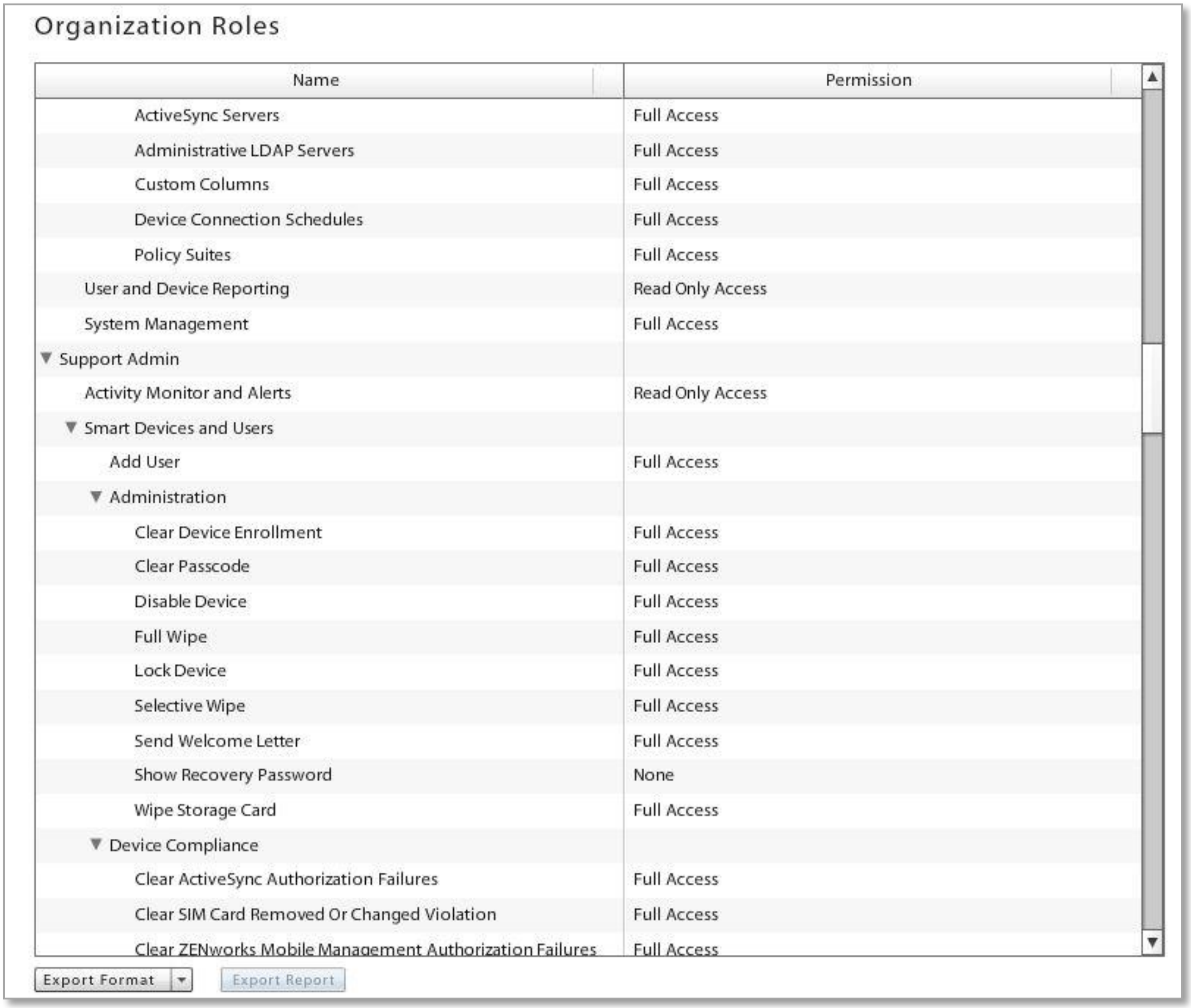
Access Restriction Violations

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			
▼ jwitmer	iOS	ex07	Robin
ActiveSync connection violation			
▼ pvaidya1	MotoDROIDBIONIC5	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

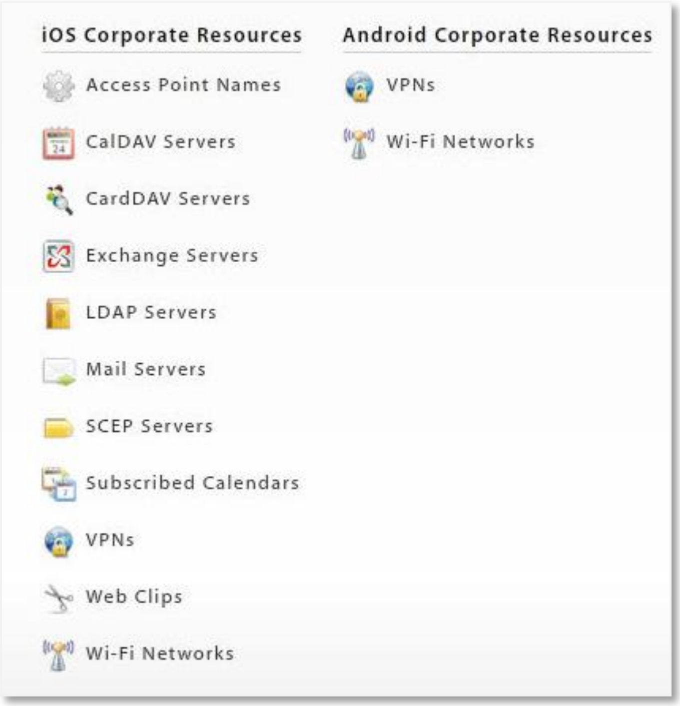
Managing Corporate Resources

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 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 *User 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

- Access Point Names
- CalDAV Servers
- CardDAV Servers
- Exchange Servers
- LDAP Servers
- Mail Servers
- SCEP Servers
- Subscribed Calendars
- VPNs
- Web Clips
- Wi-Fi Networks

Android Corporate Resources

- VPNs
- Wi-Fi Networks

Assigning Corporate Resources to Users

Corporate resources can be assigned to individual devices through the User 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 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

Server and Network Resource Configurations

You can define the following servers and networks:

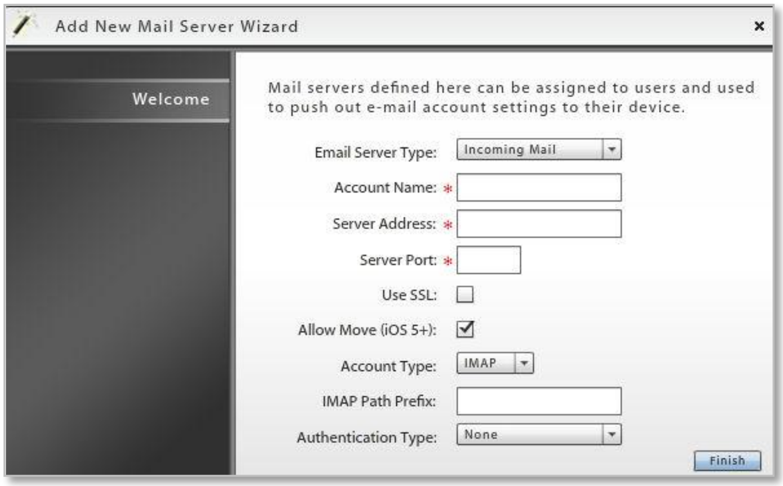
Resource	Description	Devices that Support
Access Point Names (APN)	The Access Point Name identifies the external cellular network a phone accesses for data. When you configure a new APN, you must have the correct settings for the carrier and type of account provisioning. Incorrect settings can result in a loss of functionality or additional charges. Reasons you may need to assign a new APN: • 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	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. 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.	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
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
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 from calendar-based services that support calendar subscriptions, including iCloud, Yahoo, Google, and the Mac OS x iCal application.	iOS
VPNs (Android)	Define your VPN networks. Instruct users to download and install the third party app, available through the Google Play Store (or add to your *Mobile Apps* 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. ***Note:*** Users installing Cisco AnyConnect should enable *External*	Android (OS 4.0+)

	Control in the app's settings prior to receiving a VPN assignment from the *ZENworks Mobile Management* server. If enabled after the assignment is sent, they must use the *VPN Settings* in the *ZENworks Mobile Management* settings to establish the connection.	
VPNs (iOS)	Define your VPN networks. Instruct users to download and install the third party app, available through the App Store or iTunes (or add to your *Mobile Apps* 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. ***Note:*** IPSec does not require a device application.	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.	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 **-**Account Name -Server Address -Server Port -Use SSL -Allow Move (iOS 5+) -Account Type -IMAP Path Prefix -Authentication Type -Expiration (iOS 6+)	-Exchange Server Name -Exchange Server Address -Exchange Port -Use SSL -Use S/MIME (iOS 5+) -Allow Move (iOS 5+) -Use Only in Mail (iOS 5+) -Allow Recent Address Syncing (iOS 6+) -Expiration (iOS 6+)	-LDAP Display Name -LDAP Server Address -LDAP Port -Use SSL -LDAP Searches -Expiration (iOS 6+)	-Display Name -Server Address -Server Port -Use SSL -Expiration (iOS 6+)	-Display Name -Server Address -Server Port -Use SSL -Expiration (iOS 6+)



Mail servers defined here can be assigned to users and used to push out e-mail account settings to their device.

Email Server Type: Incoming Mail

Account Name: *

Server Address: *

Server Port: *

Use SSL: □

Allow Move (iOS 5+): ☑

Account Type: IMAP

IMAP Path Prefix:

Authentication Type: None

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

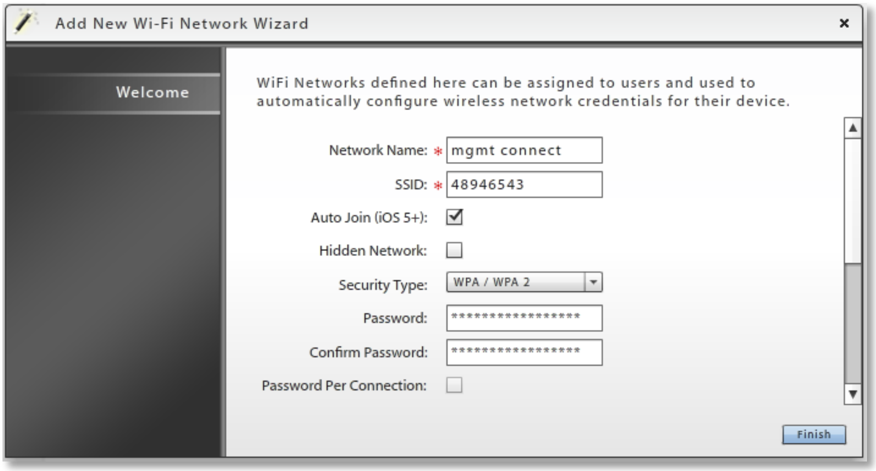
- **Allow Move (iOS 5+)** – When disabled, this option prevents an iOS 5+ device user from moving messages from corporate mail account folders to folders associated with other mailbox accounts. For example, a user could not move a message from the corporate mail account Inbox to a folder associated with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

  This prevents messages created outside of the device's native *Mail* application from being sent from the corporate account. For example, if the user sends a photo from the device *Photo* application, it is not 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)	-EAP-FAST	**VPNs (iOS)** *Settings vary based on connection type*	**Wi-Fi Networks (Android)**	-Allowed Pairwise Cipher	**VPNs (Android 4.0+)** *Cisco AnyConnect* or *F5 SSL*
-Resource Name -SSID -Auto Join (iOS 5+) -Hidden Network -Security Type -Password -Password Per Connection -Accepted EAP Types	-Allow Trust Exceptions -Inner Identity -Proxy Type -Proxy Address, Port, Username, Password -Expiration (iOS 6+)	**-**Display Name -Connection Type -User Authentication -Remote Address -Proxy Type -Expiration (iOS 6+)	**-**Resourcve Name -SSID -BSSID -Hidden Network -Allowed Authentication -Allowed Group Cipher -Allowed Key Management	-Allowed Protocol -Pre-Shared Key -WEP Key	**-**Display Name -Connection Type -Remote Address


Add New Wi-Fi Network Wizard

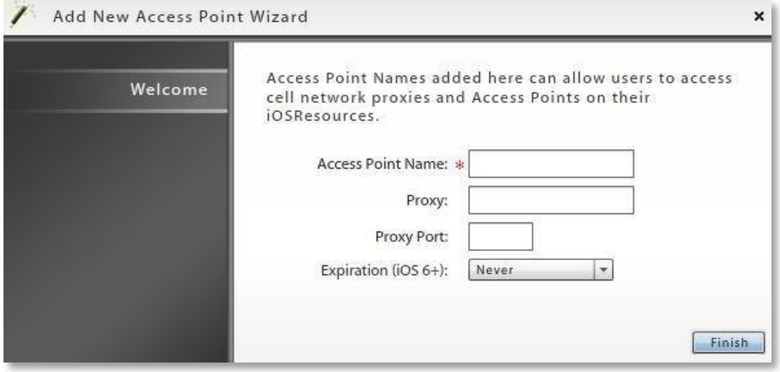
WiFi Networks defined here can be assigned to users and used to automatically configure wireless network credentials for their device.

Network Name: * mgmt connect
SSID: * 48946543
Auto Join (iOS 5+): ☑
Hidden Network: □
Security Type: WPA / WPA 2
Password: *****************
Confirm Password: *****************
Password Per Connection: □

Sample Add New Network Wizard

Configuring Other Resources

Access Point Names	Subscribed Calendars	Web Clips
-Access Point Name	-Display Name	-Label
-Proxy	-Host Name	-URL
-Proxy Port	-Use SSL	-Icon
-Expiration (iOS 6+)	-Expiration (iOS 6+)	-Removable
		-Use Precomposed Icon
		-Launch in Full Screen
		-Expiration (iOS 6+)



Add New Access Point Wizard

Access Point Names added here can allow users to access cell network proxies and Access Points on their iOSResources.

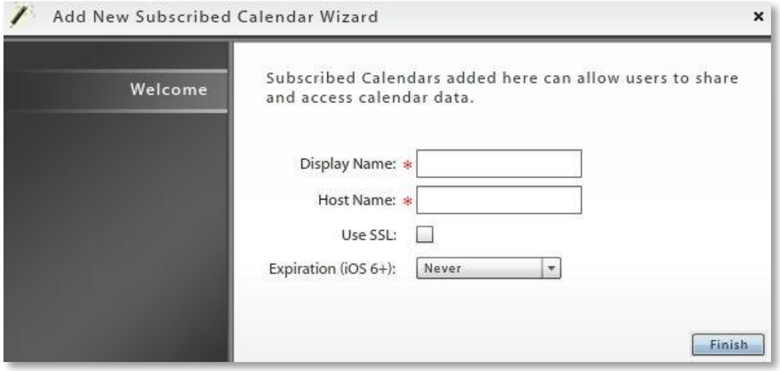
Access Point Name: *

Proxy:

Proxy Port:

Expiration (iOS 6+): Never

Access Point Name Wizard



Add New Subscribed Calendar Wizard

Subscribed Calendars added here can allow users to share and access calendar data.

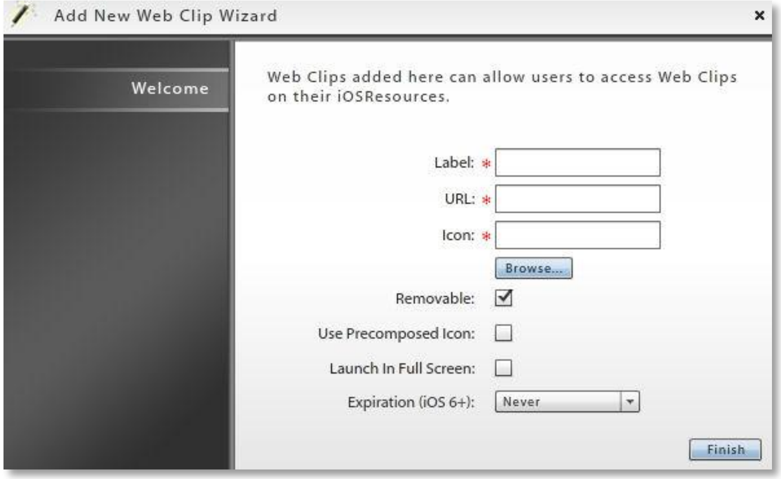
Display Name: *

Host Name: *

Use SSL: □

Expiration (iOS 6+): Never

Subscribed Calendar Wizard



Add New Web Clip Wizard

Web Clips added here can allow users to access Web Clips on their iOSResources.

Label: *

URL: *

Icon: *

Removable: ☑

Use Precomposed Icon: □

Launch In Full Screen: □

Expiration (iOS 6+): Never

Web Clip Wizard

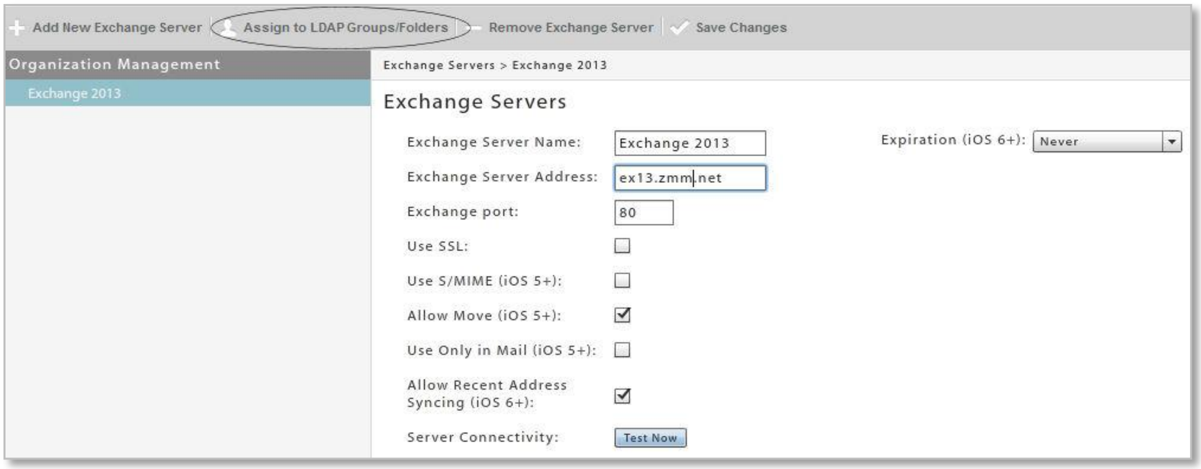
Assigning Resources to LDAP Groups and Folders

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 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 the resource you wish to assign and click the option, **Assign to LDAP Groups/Folders**.



Exchange Server Name: Exchange 2013

Expiration (iOS 6+): Never

Exchange Server Address: ex13.zmm.net

Exchange port: 80

Use SSL: □

Use S/MIME (iOS 5+): □

Allow Move (iOS 5+): ☑

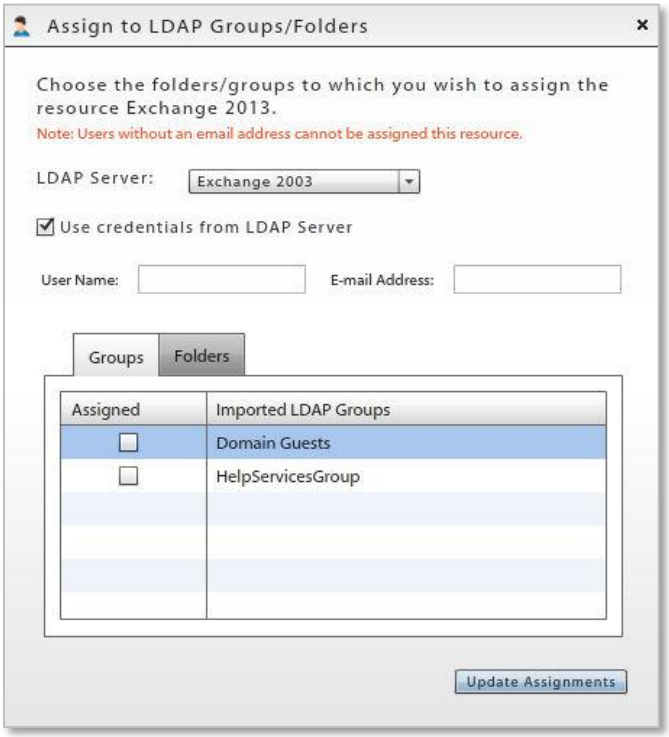
Use Only in Mail (iOS 5+): □

Allow Recent Address Syncing (iOS 6+): ☑

Server Connectivity: 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 this option enabled unless you want to assign a resource to a group email address.

   If you disable the option, you must 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 of folders to which you will assign the resource.
4. Click the **Update Assignments** button.



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:

Assigned	Imported LDAP Groups
□	Domain Guests
□	HelpServicesGroup

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. See ***Certificates***.

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.

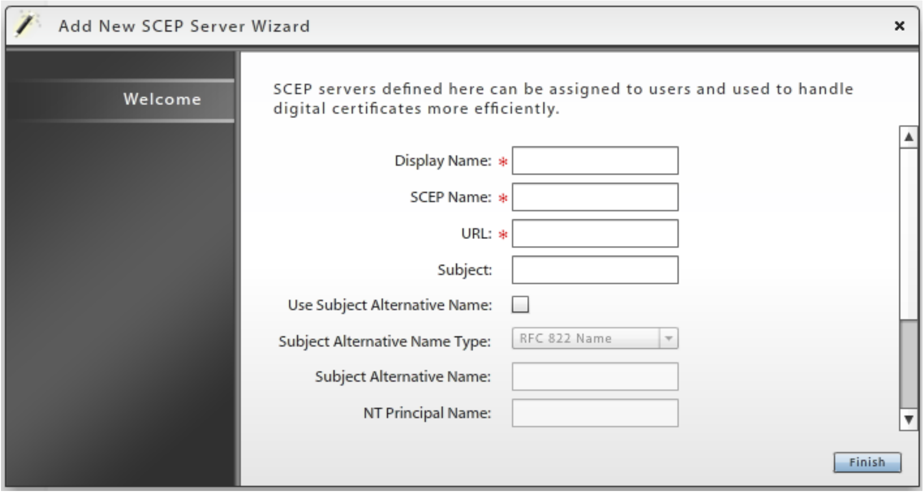
The initial configuration profile that the user accepts contains the address of the SCEP server. The device connects with both the *ZENworks Mobile Management* and SCEP servers to complete several configuration steps:

- 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*** > ***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.



SCEP servers defined here can be assigned to users and used to handle digital certificates more efficiently.

Display Name: *
SCEP Name: *
URL: *
Subject:
Use Subject Alternative Name: □
Subject Alternative Name Type: RFC 822 Name
Subject Alternative Name:
NT Principal Name:

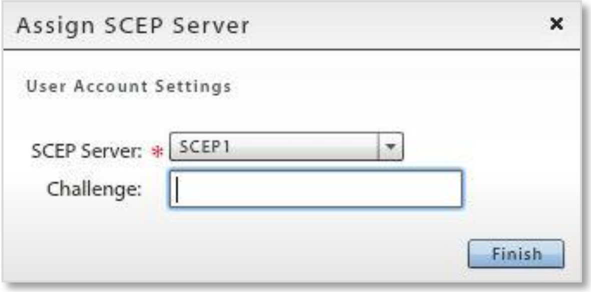
Now, use the *Corporate Resource* option in the **User Profile** to associate users with a SCEP server.

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.

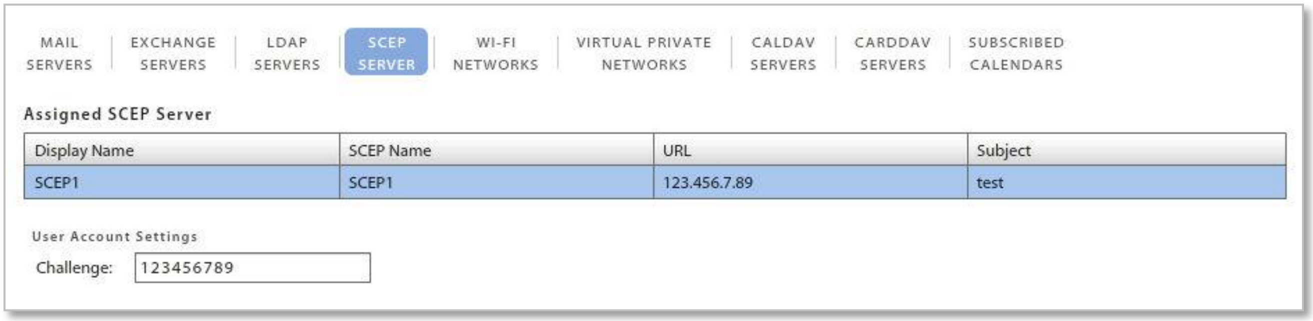
To obtain a challenge password, browse to the SCEP URL. Enter the authentication credentials (by default Integrated Windows Authentication). Copy the *Enrollment Challenge Password* and paste it into the *Challenge* field.



User Account Settings

SCEP Server: * SCEP1

Challenge:



Assigned SCEP Server

Display Name	SCEP Name	URL	Subject
SCEP1	SCEP1	123.456.7.89	test

User Account Settings

Challenge: 123456789

Organization Control

Organization Dashboard View

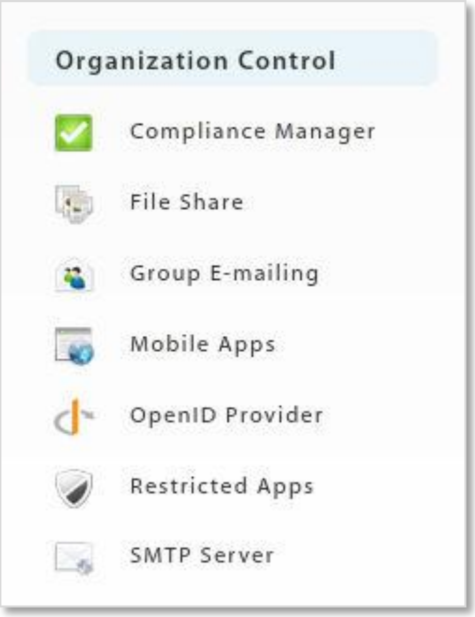
Organization Control settings are located in the *Organization* view of the dashboard. They consist of a variety of options that give you the ability to maintain organization configurations, communicate information to users, and manage the file share and application lists.

Email and File/Application Management Options
(documented in this guide)

- Group E-mailing
- File Share
- Mobile Apps
- Restricted Apps

Configuration Options
(see *Configuration Guides*)

- Compliance Manager
- SMTP Server
- OpenID Provider



Group E-mailing

Group E-mailing gives the administrator the ability to select groups of users by criteria in order to send them an email.

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 E-mail

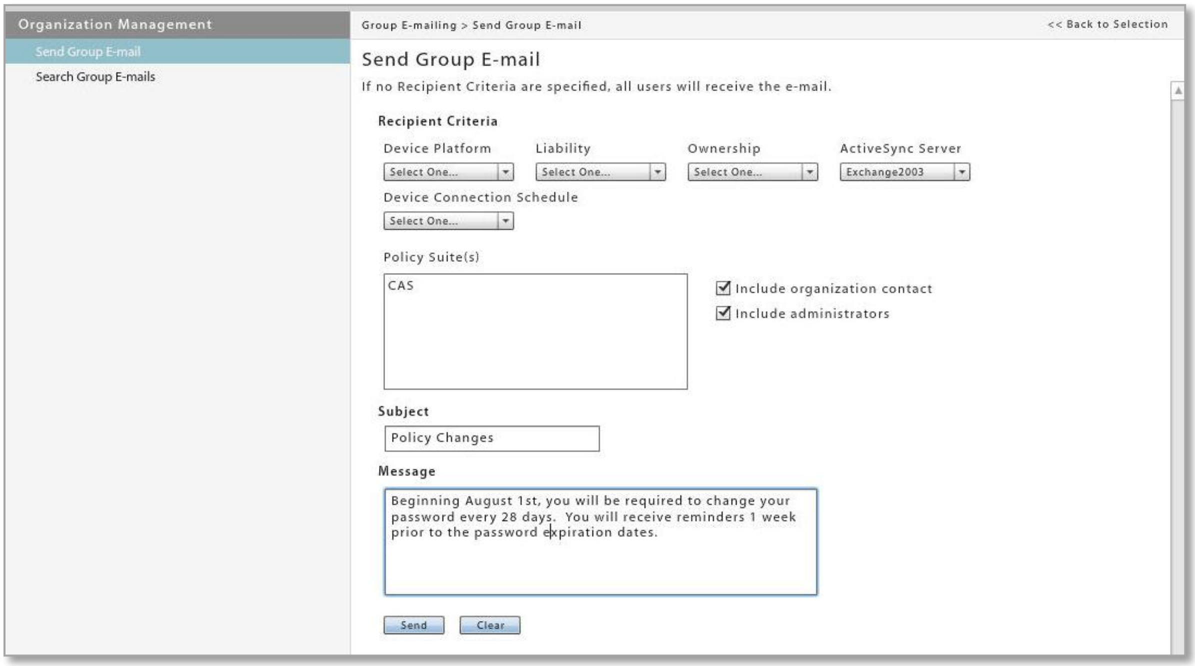
Administrators can select a group of the organization's users to email by using one or any combination of the following criteria:

- 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.

To send a group email, select ***Organization*** > ***Group E-mailing*** > ***Send Group E-mail***



Send Group E-mail

If no Recipient Criteria are specified, all users will receive the e-mail.

Recipient Criteria

Device Platform: Select One...
Liability: Select One...
Ownership: Select One...
ActiveSync Server: Exchange2003
Device Connection Schedule: Select One...

Policy Suite(s): CAS

☑ Include organization contact
☑ Include administrators

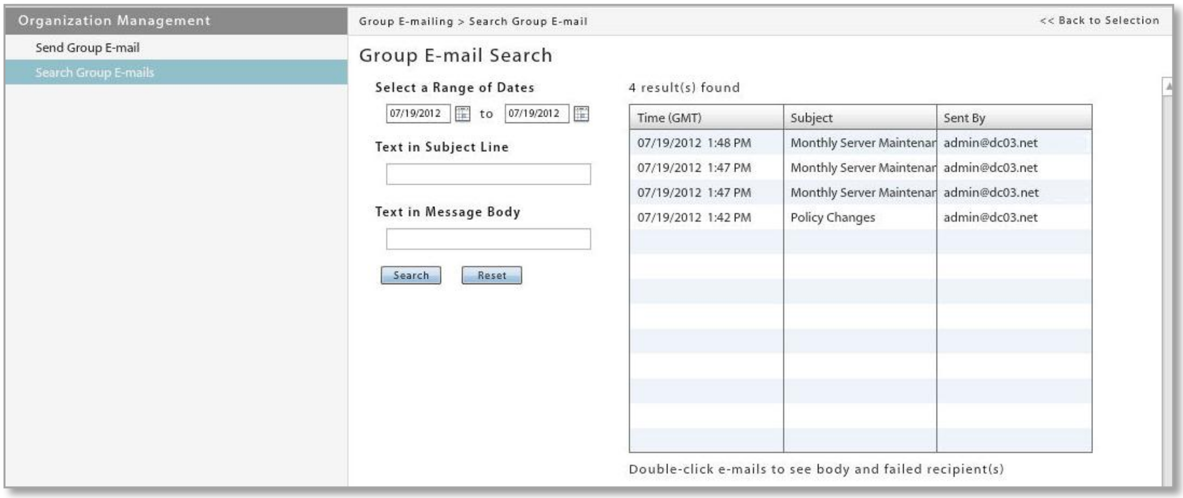
Subject: Policy Changes

Message: Beginning August 1st, you will be required to change your password every 28 days. You will receive reminders 1 week prior to the password expiration dates.

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.

To search group email, select ***Organization*** > ***Group E-mailing*** > ***Search Group E-mails***



Group E-mail Search

Select a Range of Dates: 07/19/2012 to 07/19/2012

Text in Subject Line

Text in Message Body

4 result(s) found

Time (GMT)	Subject	Sent By
07/19/2012 1:48 PM	Monthly Server Maintenar	admin@dc03.net
07/19/2012 1:47 PM	Monthly Server Maintenar	admin@dc03.net
07/19/2012 1:47 PM	Monthly Server Maintenar	admin@dc03.net
07/19/2012 1:42 PM	Policy Changes	admin@dc03.net

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

Restricted Apps

Blacklists enable the administrator to create a list of 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.

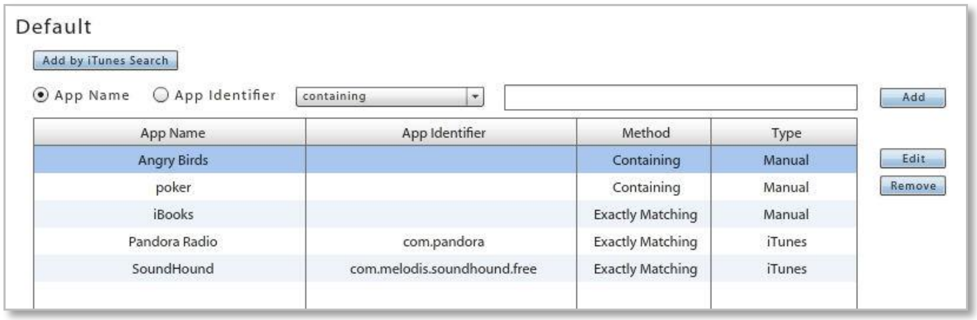
So that they are informed about which apps should not be installed, users can view the blacklist and whitelist filters via the *ZENworks Mobile Management* app on their device or the Self-Administration portals.

Add Strings to the Blacklist/Whitelist

First, create the list of strings. Select *Organization* > *Restricted Apps* > *Blacklists* or *Whitelists*.

Choose to add a filter string to 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.



Default

Add by iTunes Search

● App Name ○ App Identifier containing

Add

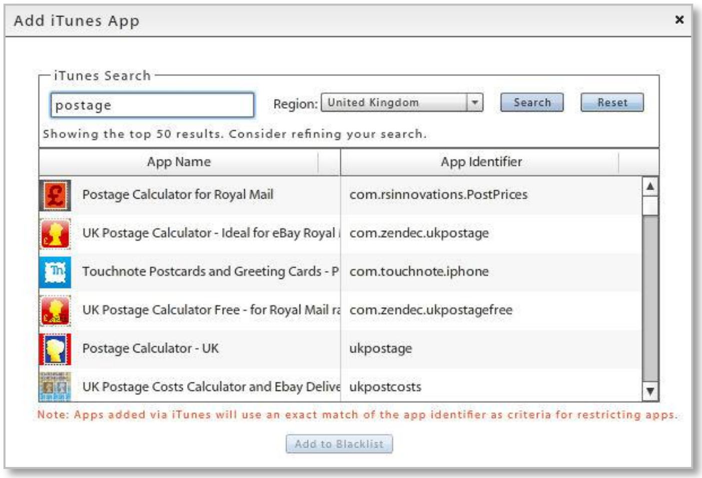
App Name	App Identifier	Method	Type
Angry Birds		Containing	Manual
poker		Containing	Manual
iBooks		Exactly Matching	Manual
Pandora Radio	com.pandora	Exactly Matching	iTunes
SoundHound	com.melodis.soundhound.free	Exactly Matching	iTunes

Edit

Remove

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, then click ***Search***. Apps added in this way are matched against their *App Identifier*.



Add iTunes App ×

iTunes Search

postage

Region: United Kingdom

Search Reset

Showing the top 50 results. Consider refining your search.

App Name	App Identifier
Postage Calculator for Royal Mail	com.rsinnovations.PostPrices
UK Postage Calculator - Ideal for eBay Royal	com.zendec.ukpostage
Touchnote Postcards and Greeting Cards - P	com.touchnote.iphone
UK Postage Calculator Free - for Royal Mail ra	com.zendec.ukpostagefree
Postage Calculator - UK	ukpostage
UK Postage Costs Calculator and Ebay Delive	ukpostcosts

Note: Apps added via iTunes will use an exact match of the app identifier as criteria for restricting apps.

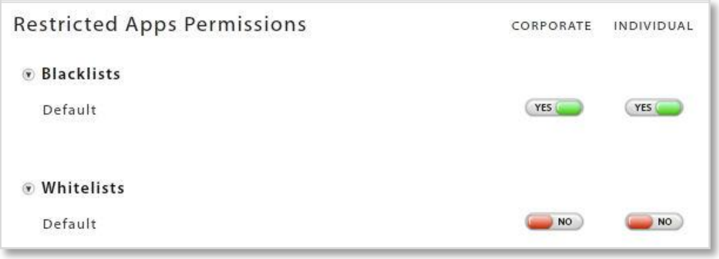
Add to Blacklist

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. In addition, the *Record application data usage* option is enabled automatically and must be remain enabled in order to monitor application usage.

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

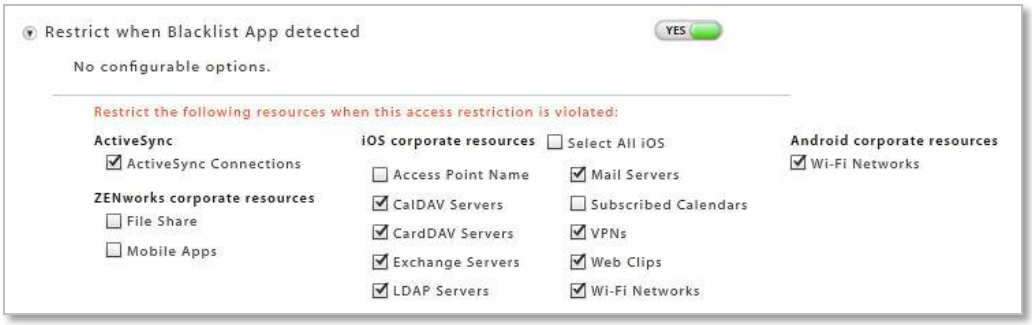
> *Note:* When you enable either the blacklist or the whitelist restricted app permission, the ***Record application data usage*** option (under the policy suite category *Audit Tracking*) is automatically enabled. This option must be remain enabled in order to monitor application usage.



Restricted Apps Permissions

	CORPORATE	INDIVIDUAL
Blacklists		
Default	YES	YES
Whitelists		
Default	NO	NO

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:

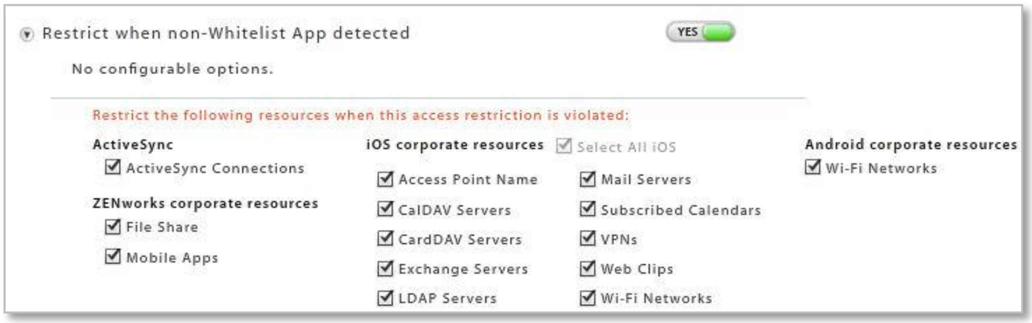
ActiveSync
☑ ActiveSync Connections

ZENworks corporate resources
□ File Share
□ Mobile Apps

iOS corporate resources □ Select All iOS
□ Access Point Name
☑ CalDAV Servers
☑ CardDAV Servers
☑ Exchange Servers
☑ LDAP Servers
☑ Mail Servers
□ Subscribed Calendars
☑ VPNs
☑ Web Clips
☑ Wi-Fi Networks

Android corporate resources
☑ Wi-Fi Networks

or



Restrict when non-Whitelist App detected YES

No configurable options.

Restrict the following resources when this access restriction is violated:

ActiveSync
☑ ActiveSync Connections

ZENworks corporate resources
☑ File Share
☑ Mobile Apps

iOS corporate resources ☑ Select All iOS
☑ Access Point Name
☑ CalDAV Servers
☑ CardDAV Servers
☑ Exchange Servers
☑ LDAP Servers
☑ Mail Servers
☑ Subscribed Calendars
☑ VPNs
☑ Web Clips
☑ Wi-Fi Networks

Android corporate resources
☑ Wi-Fi Networks

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 *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 *NotifySync*) users select ***Files*** from the *NotifySync* pop-up menu.
- iOS device users select the ***Files*** icon from the *ZENworks* main screen.
- Symbian S60 3 users select the ***Files*** tab from the *ZENworks* main screen.
- Windows Mobile 6 users select ***Files*** from the *ZENworks* pop-up menu.

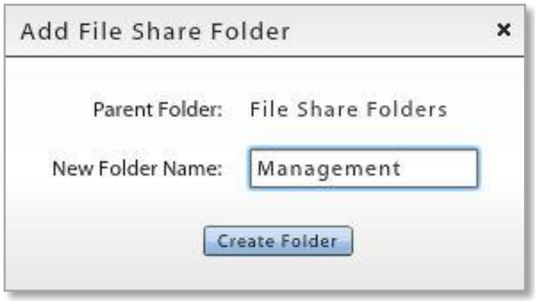
Adding Folders and Files to the Directory

To manage the file directory, select ***Organization*** > ***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***.



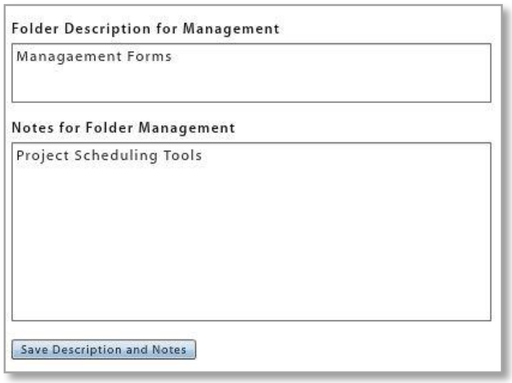
Parent Folder: File Share Folders

New Folder Name: Management

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

Management

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


Folder Description for Management

Managaement Forms

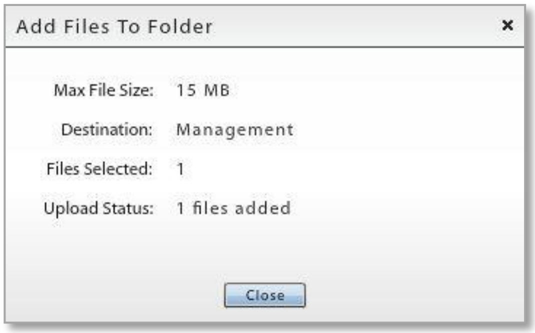
Notes for Folder Management

Project Scheduling Tools

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.

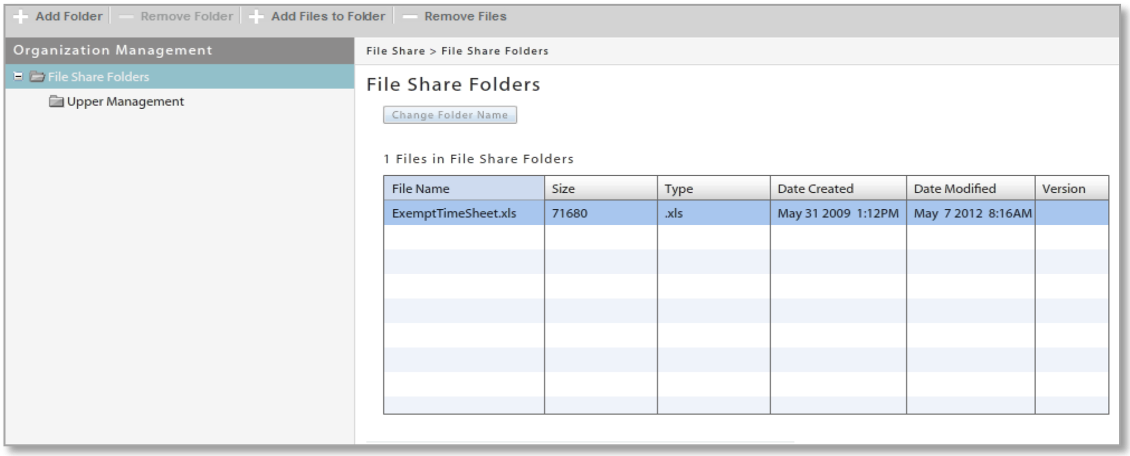


Max File Size: 15 MB

Destination: Management

Files Selected: 1

Upload Status: 1 files added



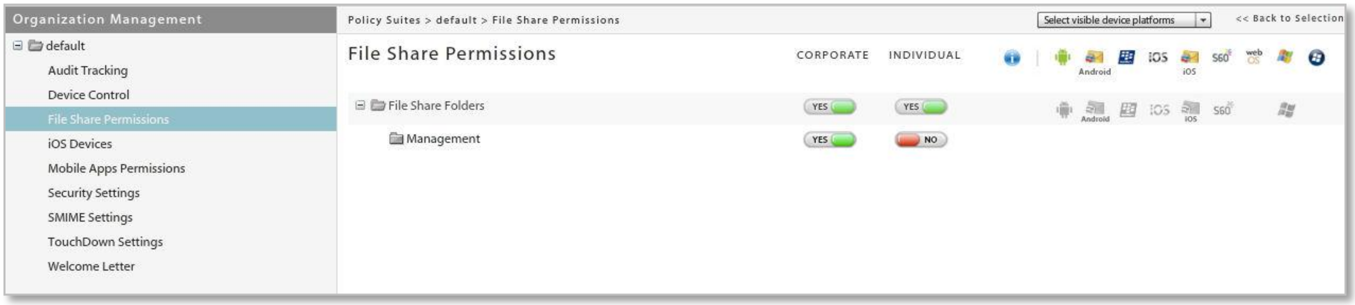
1 Files in File Share Folders

File Name	Size	Type	Date Created	Date Modified	Version
ExemptTimeSheet.xls	71680	.xls	May 31 2009 1:12PM	May 7 2012 8:16AM	

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 Suites*** > (*select policy suites*) > ***File Share Permissions***.



	CORPORATE	INDIVIDUAL
File Share Folders	YES	YES
Management	YES	NO

Mobile Apps

Mobile 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 *NotifySync* application.

When an administrator creates an app list for each supported device platform and enables the *Mobile App Permissions* in the policy suite, users can access the recommended applications from the *ZENworks Mobile Management* application on the device.

In this section you will find information on:

Adding Mobile Apps: An Overview

Adding Mobile Apps for BlackBerry, Symbian, and Windows Mobile

Enabling Mobile App Permissions

Adding and Managing Mobile Apps for iOS 5+ Devices

Adding and Managing Mobile Apps for Android Devices

Accessing Mobile Apps on a Device

Users can access the recommended applications from the *ZENworks Mobile Management* application on the device:

- Android users select ***Mobile Apps*** from the *ZENworks* main screen.
- BlackBerry (with *NotifySync*) users select ***Mobile Apps*** from the *NotifySync* pop-up menu.
- iOS device users select the ***Apps*** icon from the *ZENworks* main screen.
- Symbian S60 3 users select the ***Apps*** tab from the *ZENworks* main screen.
- Windows Mobile 6 users select ***Applications*** from the *ZENworks* pop-up menu.

Adding Mobile Apps: An Overview

If the Mobile App list is accessed by users in different countries or regions, read this Knowledge Base article.

User Installed Apps

Apps can be added to the list 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.

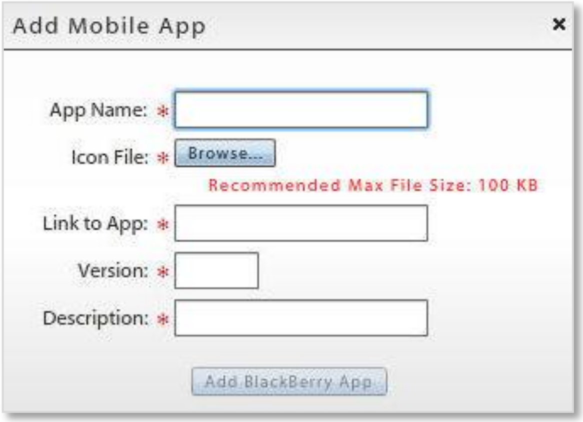
- For ***Android***, ***BlackBerry 4.5-7.1 iOS***, ***Symbian***, or ***Windows Mobile*** devices, provide application store URLs so that users can link to an application store or download page to obtain the app.
- For ***Android***, ***iOS***, ***Symbian***, and ***Windows Mobile*** devices, you can enter an actual app file. If you synchronize app files to the device, users can open and install them directly from the *ZENworks Mobile Management* app.

Administrator Managed Apps

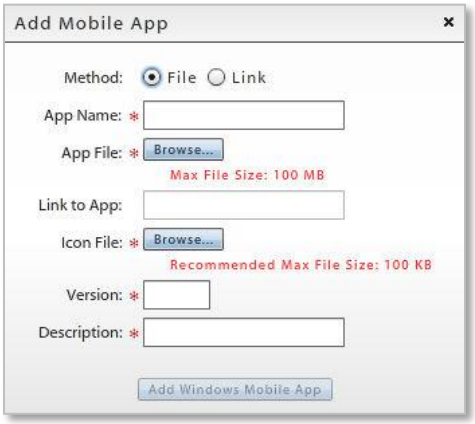
- For ***iOS 5+*** devices, MDM functionality makes it possible to add and manage free App Store apps, enterprise apps, and apps that have been pre-purchased through the Apple Volume Purchase Program (VPP).
- For ***Android*** devices, MDM functionality makes it possible to add and manage free Google Play Store apps and enterprise apps. (*ZENworks Mobile Management* version 2.7.1 or higher is required.)

Adding Mobile Apps for BlackBerry, Symbian, and Windows Mobile

1. Select ***Organization*** > ***Mobile Apps***.
2. Select the type of application you want to add from the left panel: ***BlackBerry***, ***Symbian***, or ***Windows Mobile***, then click ***Add Mobile App***.



Add Apps for BlackBerry



Method: ● File ○ Link

Add Apps in a File or Link format for Symbian or Windows Mobile

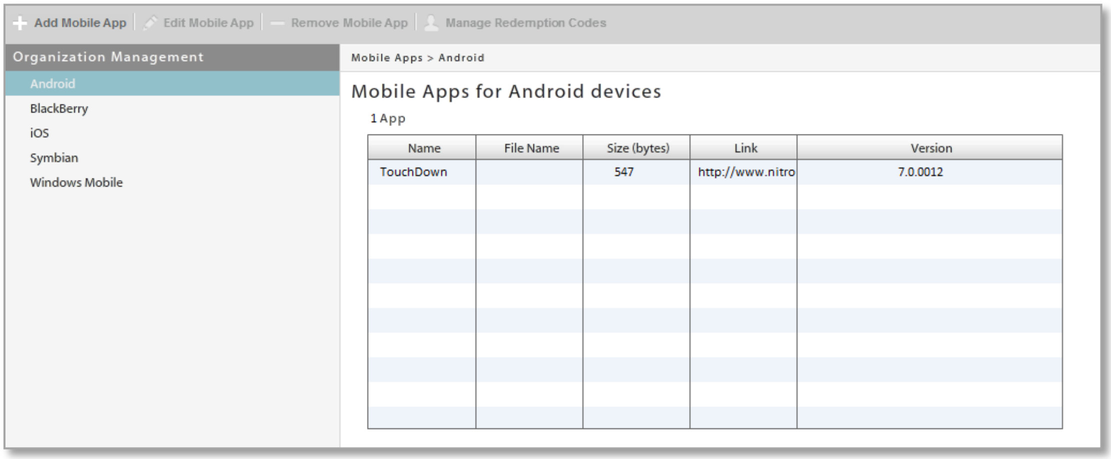
3. Select ***File*** or ***Link***. If you are adding a BlackBerry app, the default is the *Link* method.
4. Enter a ***Name***, ***Version***, and ***Description*** for the app. What you enter displays on the device.
5. For *Links*, provide the application store URL in the ***Link to App*** field.

   For *Files*, browse to select a file for the ***App File*** field.

   - For *Symbian*, select: **.sis** or **.sisx** files
   - For *Windows Mobile*, select: **.cab** files
6. For *Links*, browse your image files in the ***Icon File*** field to associate an icon with the application. This also displays on the device.
7. 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 Mobile App*** or ***Remove Mobile App*** button to edit or delete an app.



Mobile Apps for Android devices

1 App

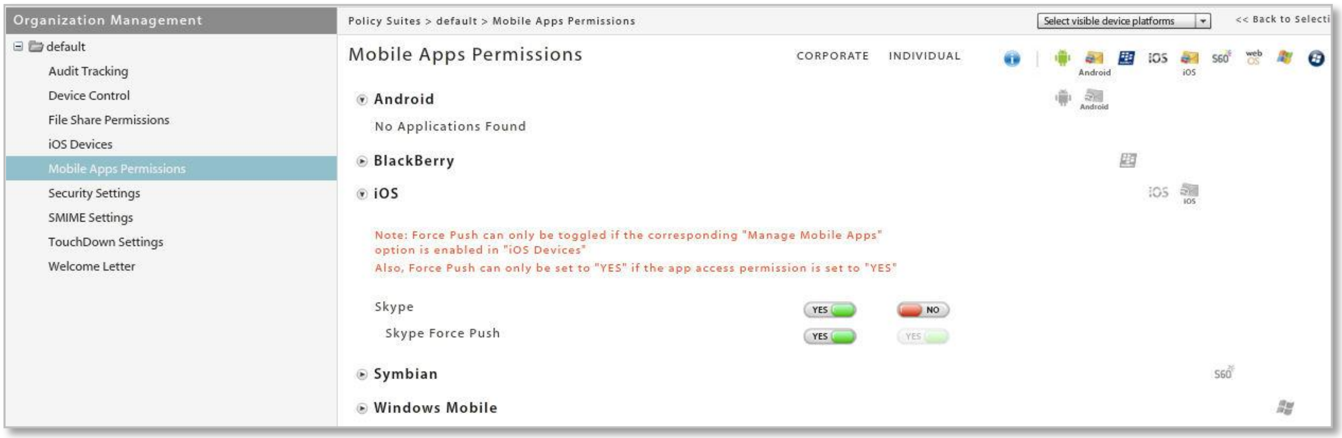
Name	File Name	Size (bytes)	Link	Version
TouchDown		547	http://www.nitro	7.0.0012

Enabling Mobile App Permissions

Mobile apps are not available to users until you enable the ***Mobile App Permissions*** in the policy suites for each app you add to the list.

1. From the *ZENworks Mobile Management* dashboard, select ***Organization*** > ***Policy Suites*** > (*select policy suite*) > ***Mobile App Permissions***.

   Select a device platform, locate the app, and enable it. YES



Android

No Applications Found

BlackBerry

iOS

Note: Force Push can only be toggled if the corresponding "Manage Mobile Apps" option is enabled in "iOS Devices"
Also, Force Push can only be set to "YES" if the app access permission is set to "YES"

Skype	YES	NO
Skype Force Push	YES	YES

Symbian

Windows Mobile

2. For iOS apps, verify that the following policies are enabled.
   Select ***Organization*** > ***Policy Suites*** > (*select policy suite*) > ***iOS Devices*** > ***Applications***.

   These policies should be enabled:

   - ***Allow application installation***
   - ***Allow iTunes***

Adding and Managing Mobile Apps for iOS 5+ Devices

Apple MDM functionality makes it possible for an administrator to manage the iOS 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 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:

Policy Rules Required for Managing iOS Apps

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

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

1. Choose policy suite category ***iOS Devices*** > ***iOS MDM*** and enable the following option:

   Manage Mobile Apps – Required for Force Push and administrator initiated app installations.

2. Choose policy suite category ***iOS Devices*** > ***Applications*** and enable the following options:

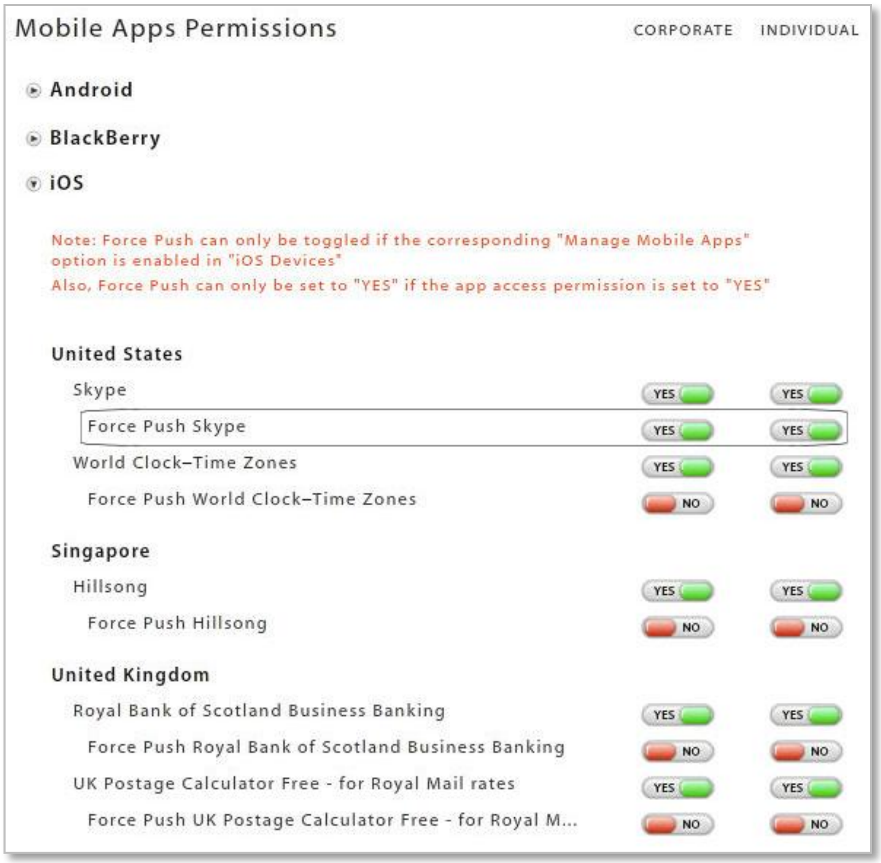
   Allow application installation – Required for Force Push and administrator initiated app installations.

   Allow iTunes – Required for Force Push and administrator initiated App Store app installations.

3. Choose policy suite category ***Mobile App Permissions*** > ***iOS***. For each mobile app listed under the iOS platform:

   a. Enable the app to make it available to users associated with the policy suite.

   b. Enable the *Force Push* option to set the app to be automatically installed on the devices of all users associated with the policy suite. This makes it a required app.



Mobile Apps Permissions

▸ Android

▸ BlackBerry

▾ iOS

Note: Force Push can only be toggled if the corresponding "Manage Mobile Apps" option is enabled in "iOS Devices"
Also, Force Push can only be set to "YES" if the app access permission is set to "YES"

	CORPORATE	INDIVIDUAL
United States		
Skype	YES	YES
Force Push Skype	YES	YES
World Clock–Time Zones	YES	YES
Force Push World Clock–Time Zones	NO	NO
Singapore		
Hillsong	YES	YES
Force Push Hillsong	NO	NO
United Kingdom		
Royal Bank of Scotland Business Banking	YES	YES
Force Push Royal Bank of Scotland Business Banking	NO	NO
UK Postage Calculator Free - for Royal Mail rates	YES	YES
Force Push UK Postage Calculator Free - for Royal M...	NO	NO

Enabling Force Push for Required Apps

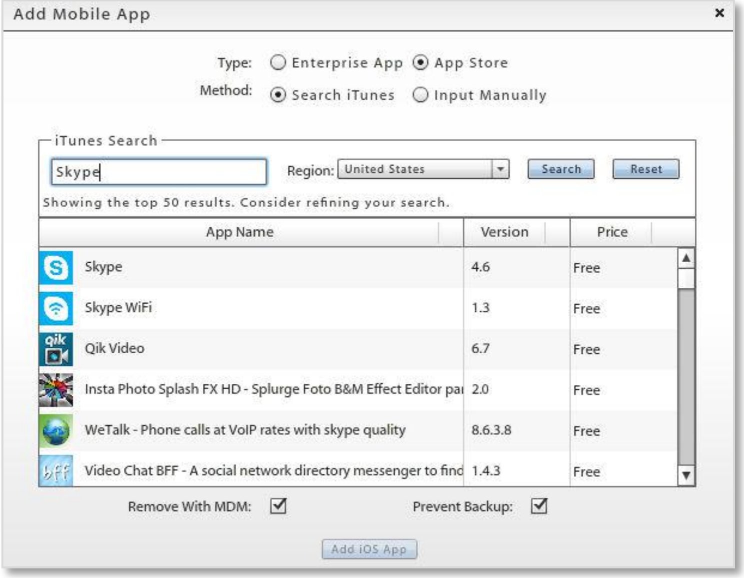
Adding iOS App Store Apps

If the Mobile App list is accessed by users in different countries or regions, read this Knowledge Base article.

1. Select ***Organization*** > ***Mobile Apps***.
2. Select ***iOS*** from the left panel, then click ***Add Mobile 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.
   a. If searching iTunes, enter a string to search on and the region in which the app is available, then click ***Search***.
   b. If inputting manually, enter an ***App Name***, ***Version***, and ***Description*** for the app. What you enter is displayed on the device in the mobile 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 mobile app list.
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. Click ***Add iOS App*** to add the App to the iOS Mobile App list.



Type: ○ Enterprise App ● App Store

Method: ● Search iTunes ○ Input Manually

iTunes Search

Skype

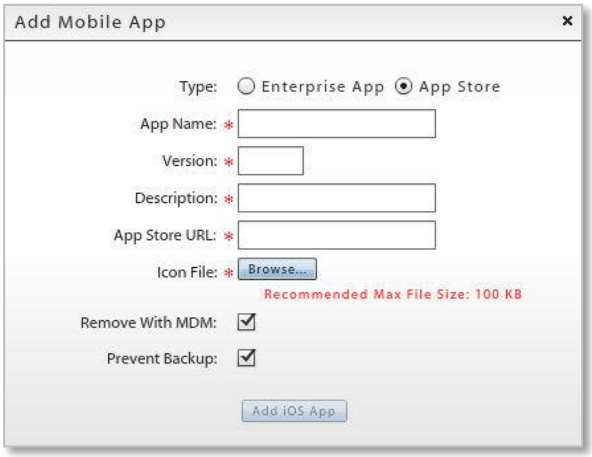
Region: United States

Showing the top 50 results. Consider refining your search.

App Name	Version	Price
Skype	4.6	Free
Skype WiFi	1.3	Free
Qik Video	6.7	Free
Insta Photo Splash FX HD - Splurge Foto B&M Effect Editor pai	2.0	Free
WeTalk - Phone calls at VoIP rates with skype quality	8.6.3.8	Free
Video Chat BFF - A social network directory messenger to find	1.4.3	Free

Remove With MDM: ☑ Prevent Backup: ☑

Search iTunes to add an app



Type: ○ Enterprise App ● App Store

App Name: *

Version: *

Description: *

App Store URL: *

Icon File: *

Recommended Max File Size: 100 KB

Remove With MDM: ☑

Prevent Backup: ☑

Manually add an app

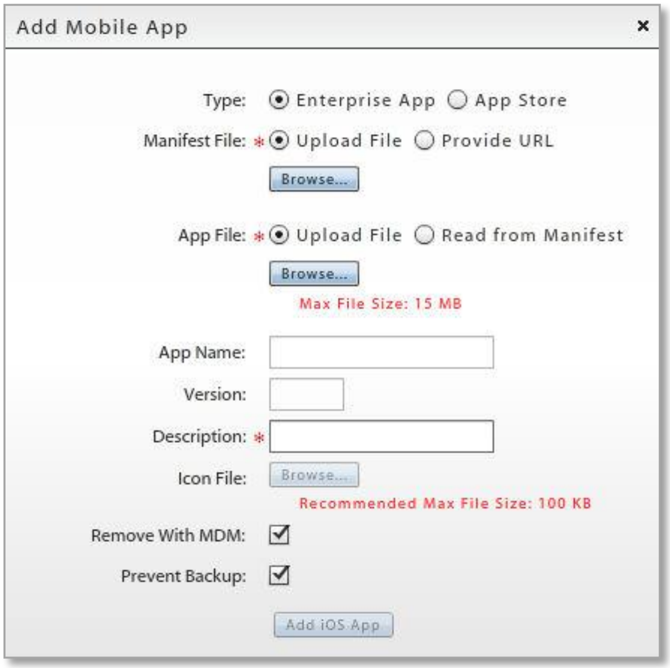
Adding an iOS Enterprise App

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*** > ***Mobile Apps***.
2. Select ***iOS*** from the left panel, then click ***Add Mobile 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 *ZENworks Mobile Management* server	Select **Upload File** Upload the appropriate .plist file	Select **Upload File** Upload the appropriate .ipa file	Description
The manifest file is on the *ZENworks Mobile Management* 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**	*Not Applicable*	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.



Add Mobile App ×

Type: ● Enterprise App ○ App Store

Manifest File: * ● Upload File ○ Provide URL

Browse...

App File: * ● Upload File ○ Read from Manifest

Browse...

Max File Size: 15 MB

App Name:

Version:

Description: *

Icon File: Browse...

Recommended Max File Size: 100 KB

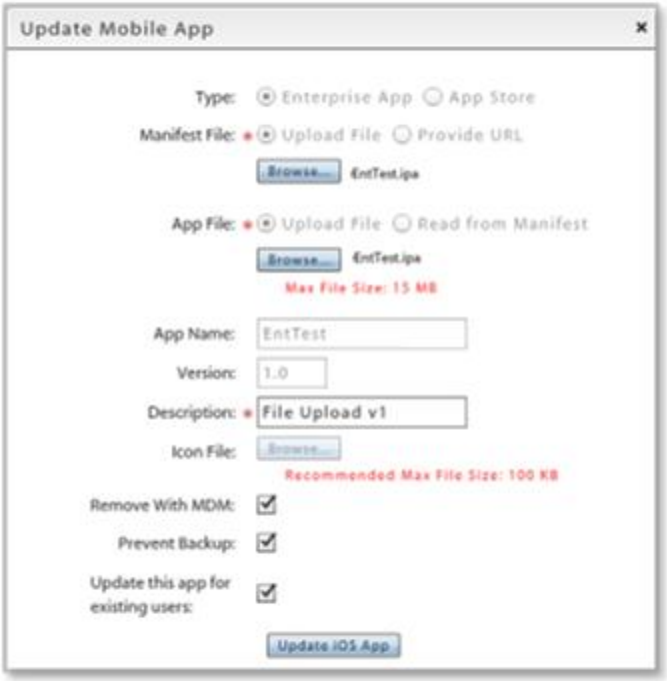
Remove With MDM: ☑

Prevent Backup: ☑

Add iOS App

Updating iOS App Versions

Edit the original app and update the application information. If the app is set to *Force Push*, users are prompted to update the app on the device. If the app is not set to *Force Push* you can check the ***Update this app for existing users*** box to push the upgrade down. Users will be prompted to update the app.



Type: ● Enterprise App ○ App Store

Manifest File: * ● Upload File ○ Provide URL — EntTest.ipa

App File: * ● Upload File ○ Read from Manifest — EntTest.ipa

App Name: EntTest

Version: 1.0

Description: * File Upload v1

Icon File:

Remove With MDM: ☑

Prevent Backup: ☑

Update this app for existing users: ☑

Managing Application Redemption Codes

For apps on your list that have been purchased through the Apple Volume Purchase Program (VPP), 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 the United States and in nine countries outside the US. 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.

The Volume Purchase Program is available in Australia, Canada, France, Germany, Italy, Japan, New Zealand, Spain, the United Kingdom, and the United States.

To Add Redemption Codes:

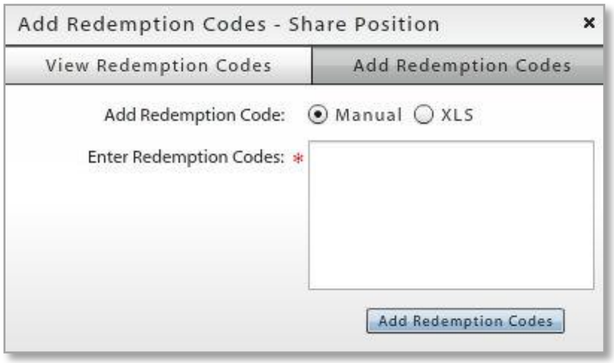
1. Add the app to the iOS Mobile App list.
2. Select the app, then click ***Manage Redemption Codes***.
3. Select the ***Add Redemption Codes*** tab.

4. Select ***Manual*** or XLS (for XLS, proceed to step 6).if you will enter each code individually.

   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 Code: ● Manual ○ XLS

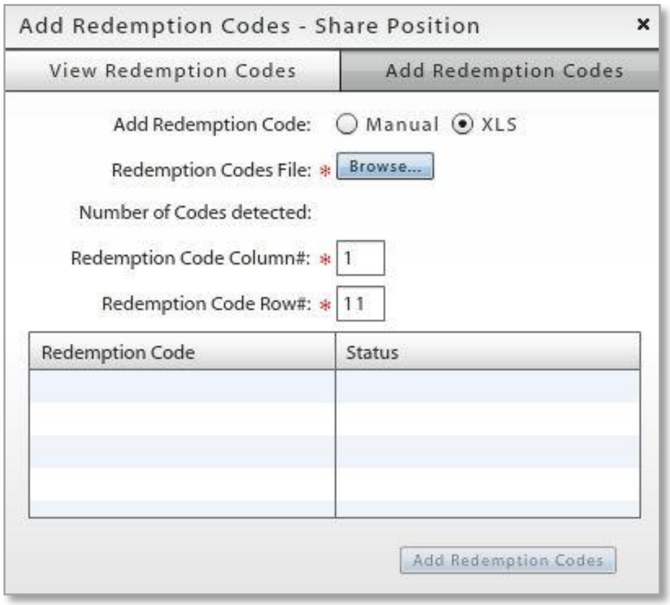
Enter Redemption Codes: *

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 Code: ○ Manual ● XLS

Redemption Codes File: *

Number of Codes detected:

Redemption Code Column#: * 1

Redemption Code Row#: * 11

Redemption Code	Status

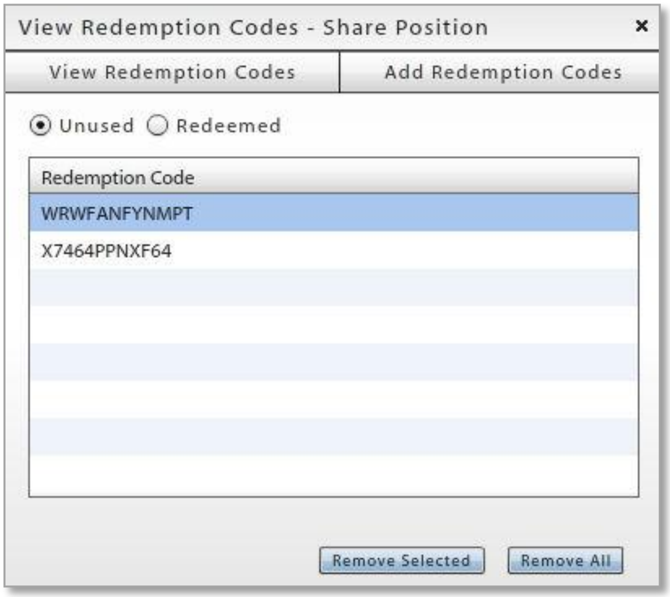
To View or Remove Redemption Codes:

1. Select an app from the iOS Mobile App list, then click ***Manage Redemption Codes***.

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.



● Unused ○ Redeemed

Redemption Code
WRWFANFYNMPT
X7464PPNXF64

Adding and Managing Mobile 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 a policy are automatically prompted to install
- Adding Enterprise (in-house) apps to the list

In this section:

Mobile App Permissions for Managing Android Apps

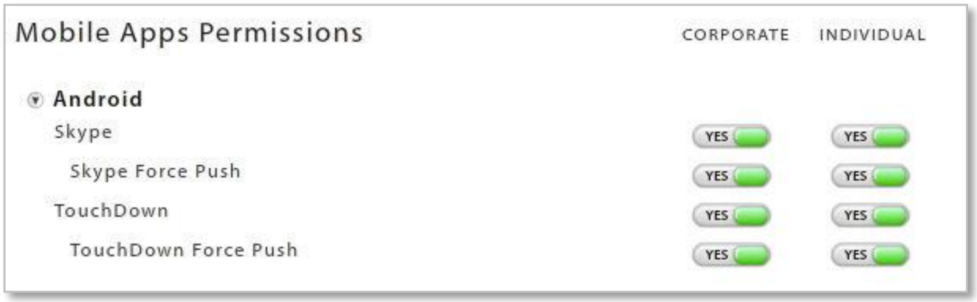
Enable the *Force Push* policy suite options for apps that you want to automatically push to devices. Users will be prompted to install these apps.

Choose the policy suite category ***Mobile App Permissions*** > ***Android****.* For each mobile app listed under the *Android* platform:

a. Enable the app to make it available to users associated with the policy suite.

b. Enable the *Force Push* option to set the app to automatically prompt users associated with the policy suite to install the app. This makes it a required app.

> **Note:** Administrators can issue an uninstall command using the *Uninstall App* button in the *Apps* section of the *User Profile*. The *Force Push* option should be disabled first, however, so that the app does not get pushed back to the device after the user uninstalls.



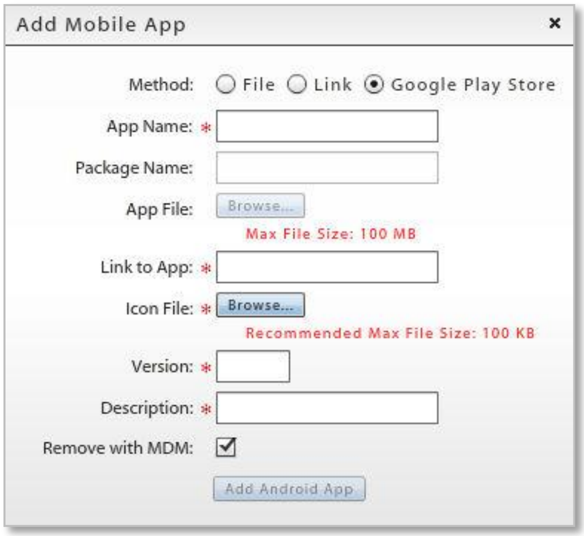
Mobile Apps Permissions

	CORPORATE	INDIVIDUAL
▾ Android		
Skype	YES	YES
Skype Force Push	YES	YES
TouchDown	YES	YES
TouchDown Force Push	YES	YES

Enabling Force Push for required apps

Adding Google Play Store Apps

1. Select ***Organization*** > ***Mobile Apps***.
2. Select ***Android*** from the left panel, then click ***Add Mobile 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. Click ***Add Android App*** to add the App to the Android Mobile App list.



Add Mobile App ×

Method: ○ File ○ Link ● Google Play Store

App Name: *

Package Name:

App File: Browse...

Max File Size: 100 MB

Link to App: *

Icon File: * Browse...

Recommended Max File Size: 100 KB

Version: *

Description: *

Remove with MDM: ☑

Add Android App

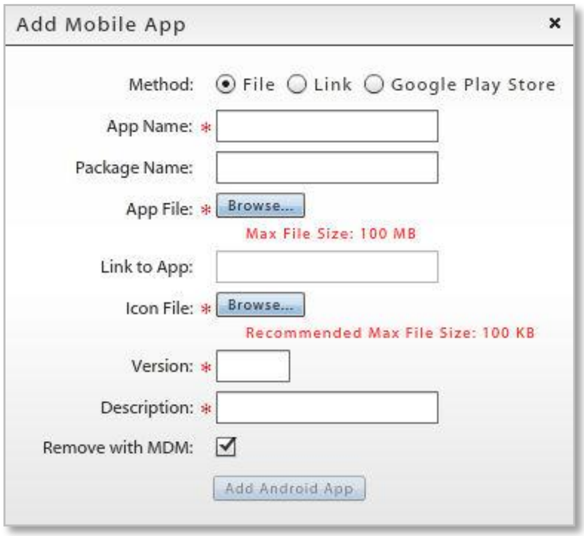
Adding an Android Enterprise App

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

1. Select ***Organization*** > ***Mobile Apps***.
2. Select ***Android*** from the left panel, then click ***Add Mobile App***..
3. Choose *File* or *Link* 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. 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.

   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.



Add Mobile App ×

Method: ● File ○ Link ○ Google Play Store

App Name: *

Package Name:

App File: * Browse...

Max File Size: 100 MB

Link to App:

Icon File: * Browse...

Recommended Max File Size: 100 KB

Version: *

Description: *

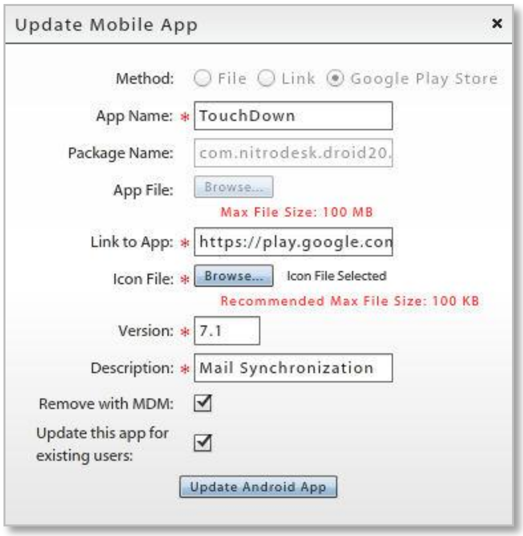
Remove with MDM: ☑

Add Android App

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. Click ***Add Android App*** to add the App to the Android Mobile App list.

Updating Android App Versions

Edit the original app and update the application information. If the app is already on the device, you can check the ***Update this app for existing users*** box to push the upgrade down. Users will be prompted to update the app.



Method: ○ File ○ Link ● Google Play Store
App Name: * TouchDown
Package Name: com.nitrodesk.droid20.
App File: Max File Size: 100 MB
Link to App: * https://play.google.con
Icon File: * Icon File Selected Recommended Max File Size: 100 KB
Version: * 7.1
Description: * Mail Synchronization
Remove with MDM: ☑
Update this app for existing users: ☑