Managing Users, Resources, and Applications

ZENworks® Mobile Management 3.0.x

January 2015

Legal Notices

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

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

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

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

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

Novell Trademarks

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

Third-Party Materials

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

Table of Contents

Accessing the Dashboard

Access the Dashboard

ZENworks Mobile Management dashboard requirements:

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

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

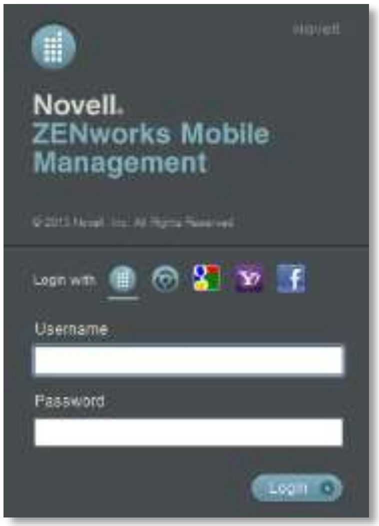
Example: https://my.ZENworks.server/dashboard

Standard Login

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

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

A system administrator can create additional logins to the dashboard with system administrator, organization administrator, or support administrator privileges. See the *System Administration Guide* for details.



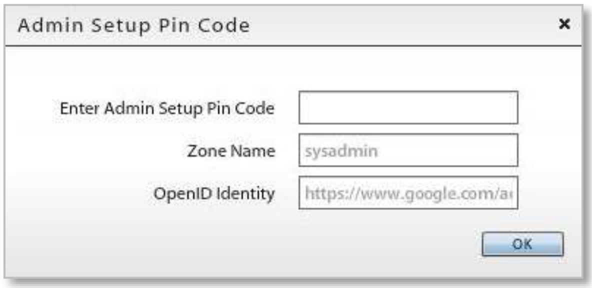
OpenID Login

Use your OpenID credentials to log in.

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

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

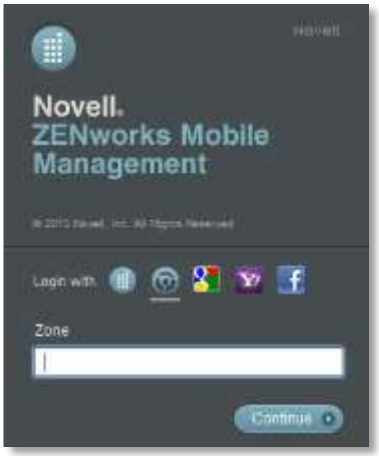
   Zone Name and new PIN codes are emailed to you from the *ZENworks Mobile Management* server.

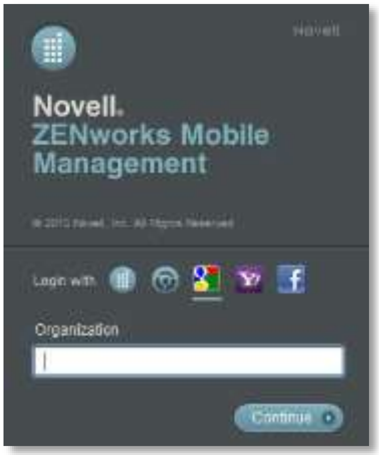

Admin Setup Pin Code

Enter Admin Setup Pin Code

Zone Name: sysadmin

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





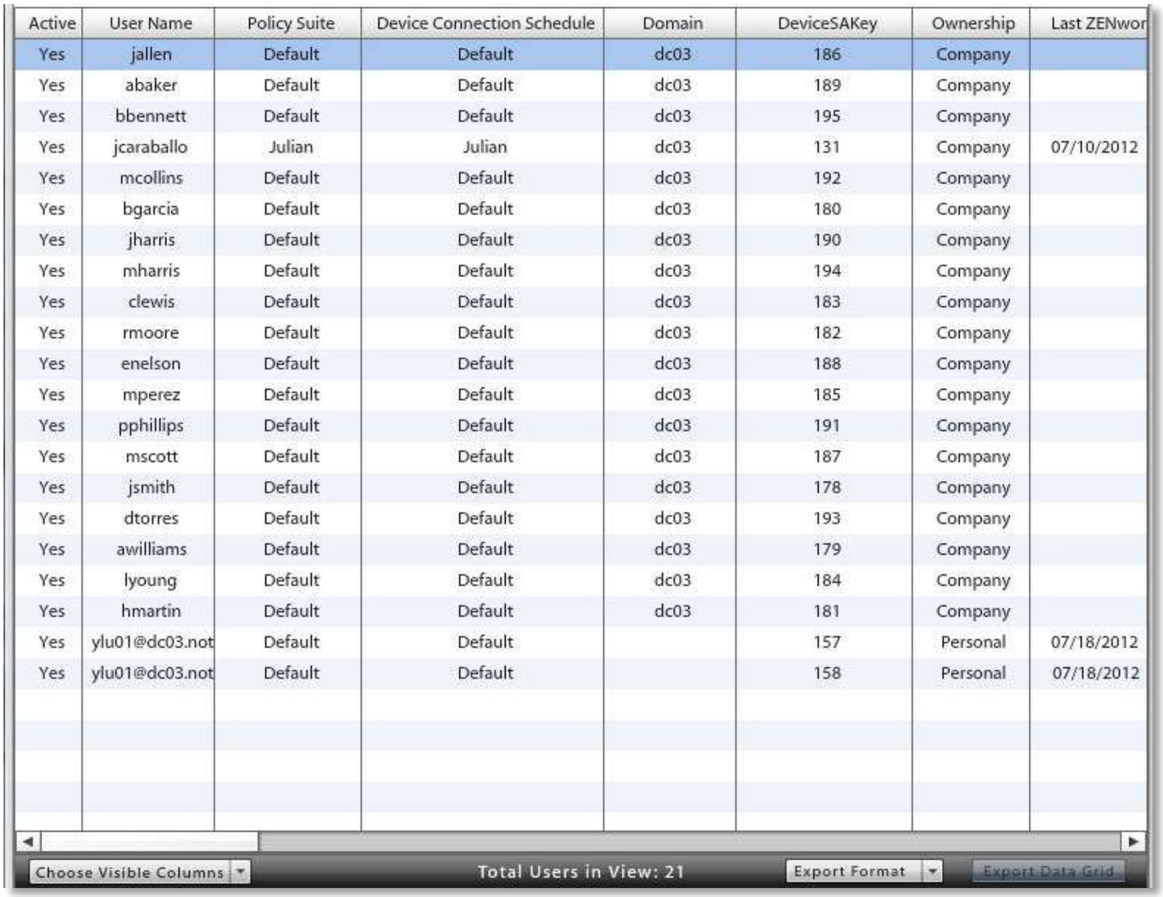
Managing Users

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

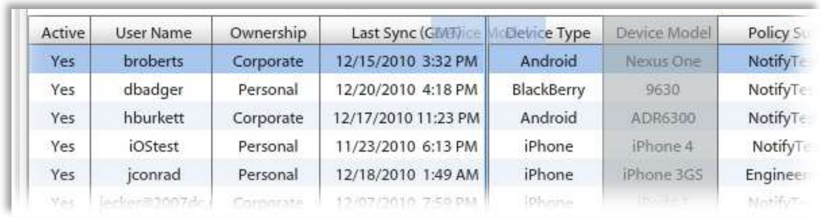
Total Users in View: 21

Customizing and Searching the User Grid

Customize the user list view by:

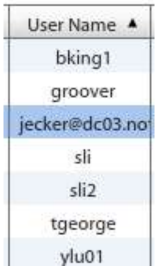
- Rearranging columns
- Sorting columns
- Choosing the visible columns
- Searching for and displaying a distinct category of users
- Limiting the list to members of an LDAP folder or group

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

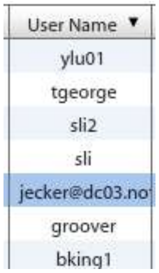


Active	User Name	Ownership	Last Sync (GMT)	Device Type	Device Model	Policy S
Yes	broberts	Corporate	12/15/2010 3:32 PM	Android	Nexus One	NotifyTe
Yes	dbadger	Personal	12/20/2010 4:18 PM	BlackBerry	9630	NotifyTe
Yes	hburkett	Corporate	12/17/2010 11:23 PM	Android	ADR6300	NotifyTe
Yes	iOStest	Personal	11/23/2010 6:13 PM	iPhone	iPhone 4	NotifyTe
Yes	jconrad	Personal	12/18/2010 1:49 AM	iPhone	iPhone 3GS	Enginee
Yes	jecker@2007dc	Corporate	12/07/2010 7:59 PM	iPhone	[illegible]	NotifyT

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

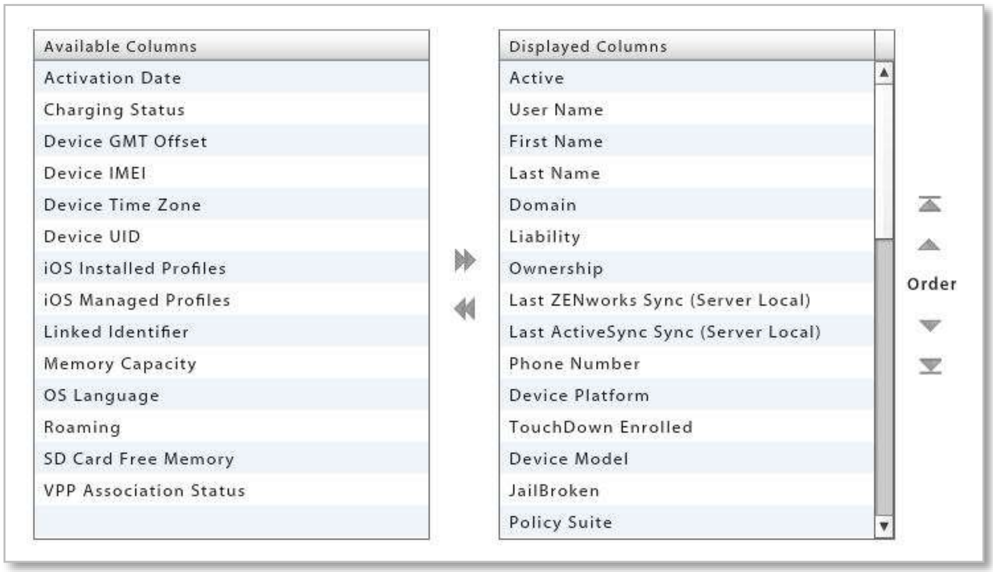


User Name ▲
bking1
groover
jecker@dc03.no
sli
sli2
tgeorge
ylu01



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

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



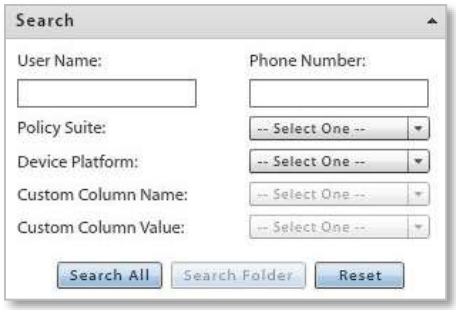
Available Columns
Activation Date
Charging Status
Device GMT Offset
Device IMEI
Device Time Zone
Device UID
iOS Installed Profiles
iOS Managed Profiles
Linked Identifier
Memory Capacity
OS Language
Roaming
SD Card Free Memory
VPP Association Status

Displayed Columns
Active
User Name
First Name
Last Name
Domain
Liability
Ownership
Last ZENworks Sync (Server Local)
Last ActiveSync Sync (Server Local)
Phone Number
Device Platform
TouchDown Enrolled
Device Model
JailBroken
Policy Suite

Available Columns

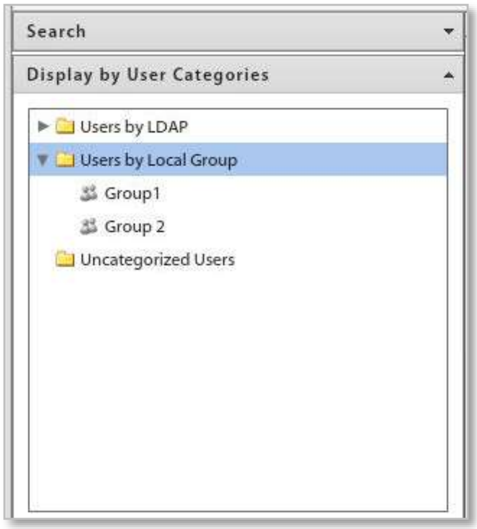
Activation Date
Active
ActiveSync Authorization Failures (User)
ActiveSync User Agent
ActiveSync Version
Apple DEP Device
Battery Level
Charging Status
Device Connection Schedule
Device GMT Offset
Device IMEI
Device Model
Device Name
Device Platform
Device Time Zone
Device UID
DeviceSAKey
Domain
Email Address
Expiration Date
First Name
Free Memory
IMSI Number
iOS Installed Profiles
iOS Managed Profiles
Jailbroken
KNOX EMM Status
KNOX Workspace Status
Last ActiveSync Sync (Server Local)
Last APN Check-In (Server Local)
Last APN Sent (Server Local)
Last Name
Last ZENworks Sync (Server Local)
Liability
Linked Identifier
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
User Name
UserSAKey
Violation Status
VPP Association Status
ZENworks App Language
ZENworks App Version
ZENworks Authorization Failures (user)

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



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

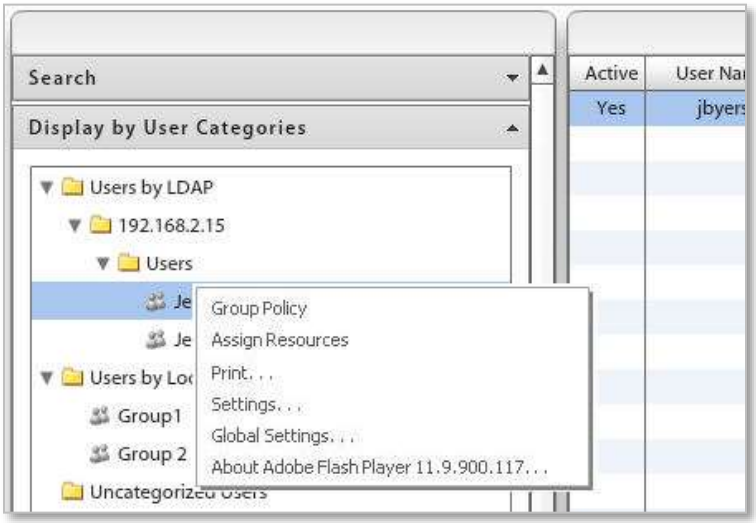
To refresh the grid so that it displays the entire list of users, click the group again, click the refresh button ↻, or click the *Reset* button in the *Search* option.



Assigning Settings and Resources to Groups/Folders from the Grid

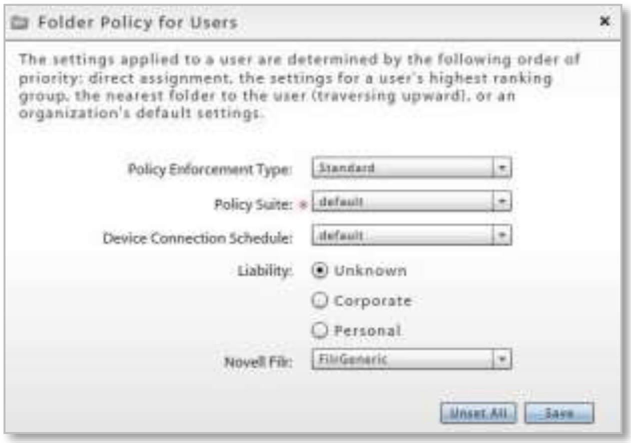
Settings such as Policy Suite, Connection Schedule, and Liability can be assigned to a local group or LDAP group/folder directly from the user grid. In addition, Android and iOS resources can be assigned to LDAP group/folder directly from the grid.

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



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

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

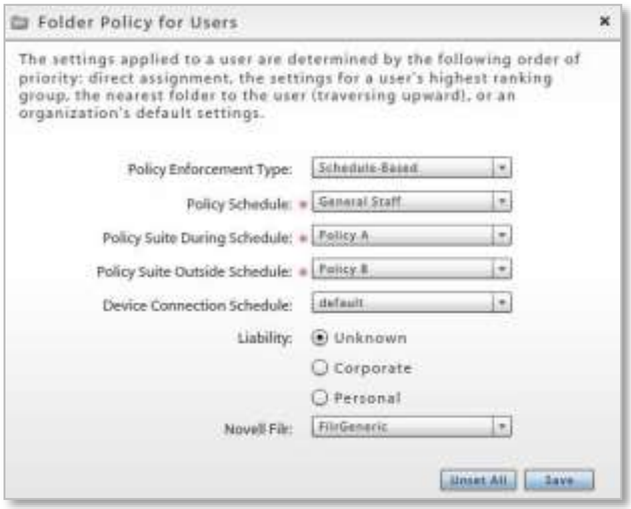


Folder Policy for Users

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: default
Liability: ● Unknown ○ Corporate ○ Personal
Novell Filr: FilrGeneric

Standard Policy Enforcement



Folder Policy for Users

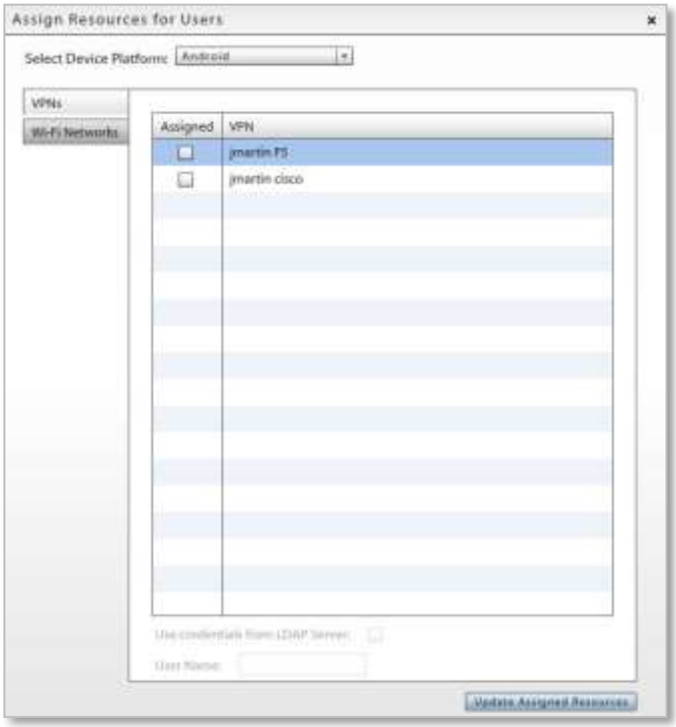
The settings applied to a user are determined by the following order of priority: direct assignment, the settings for a user's highest ranking group, the nearest folder to the user (traversing upward), or an organization's default settings.

Policy Enforcement Type: Schedule-Based
Policy Schedule: * General Staff
Policy Suite During Schedule: * Policy A
Policy Suite Outside Schedule: * Policy B
Device Connection Schedule: default
Liability: ● Unknown ○ Corporate ○ Personal
Novell Filr: FilrGeneric

Schedule-Based Policy Enforcement

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

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



Assign Resources for Users

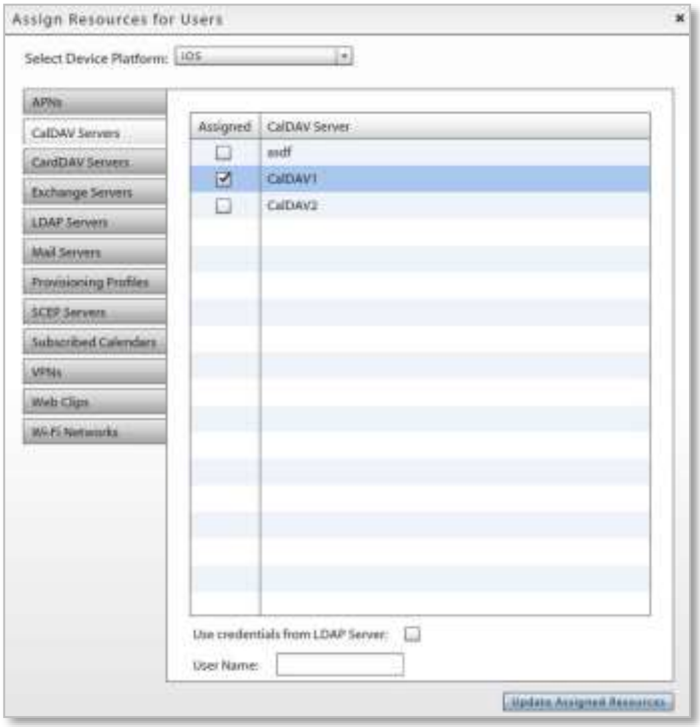
Select Device Platform: Android

Assigned	VPN
□	jmartin FS
□	jmartin cisco

Use credentials from LDAP Server: □

User Name:

Android Resource Assignments



Assign Resources for Users

Select Device Platform: iOS

Assigned	CalDAV Server
□	asdf
☑	CalDAV1
□	CalDAV2

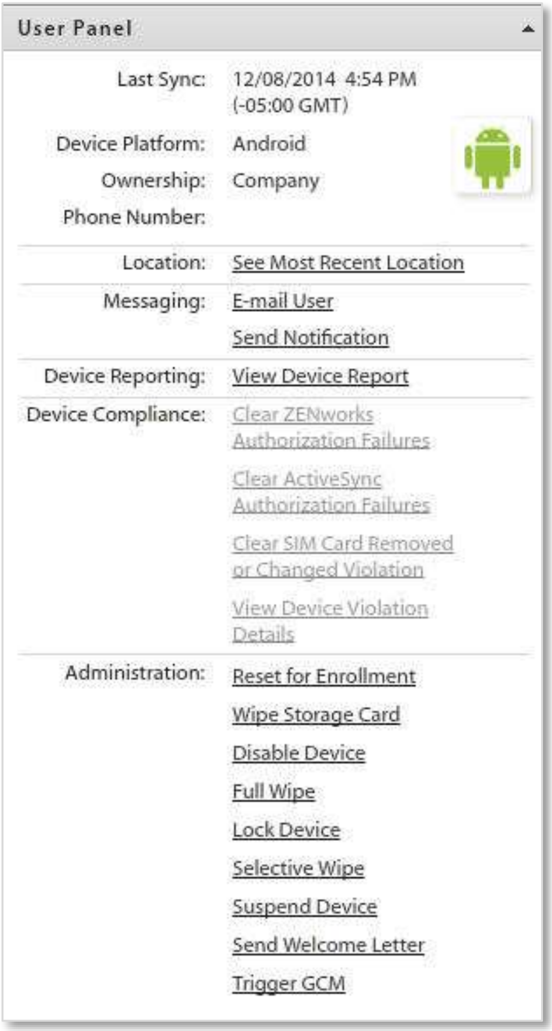
Use credentials from LDAP Server: □

User Name:

iOS Resource Assignments

The User Panel

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



User Panel

Last Sync:	12/08/2014 4:54 PM (-05:00 GMT)
Device Platform:	Android
Ownership:	Company
Phone Number:	
Location:	See Most Recent Location
Messaging:	E-mail User Send Notification
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:	Reset for Enrollment Wipe Storage Card Disable Device Full Wipe Lock Device Selective Wipe Suspend Device Send Welcome Letter Trigger GCM

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
- Send Notification – Compose and send a notification to an Android or iOS device (160 character limit).
- View Device Report - Device statistics

Device Compliance – allows the administrator to clear a violation restriction or view device violation details and create a User Exception for a violation. *See Monitoring Device Compliance for details.*

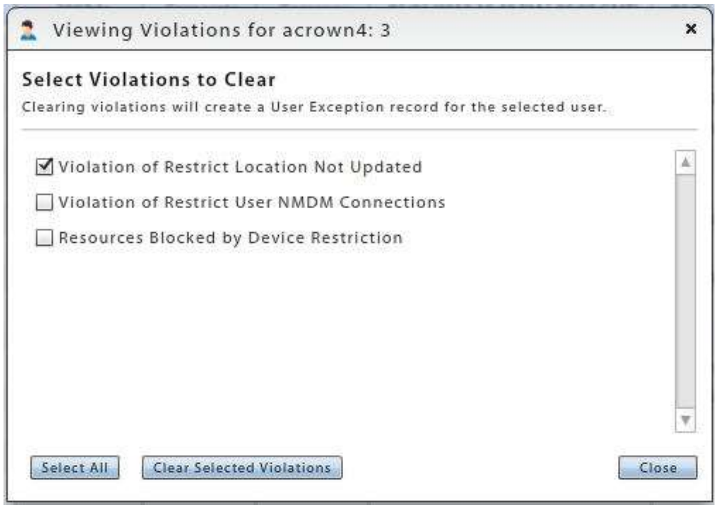
Administration – Security commands and administrative actions can be performed quickly. Only options that apply to the device platform will appear. Administrative actions can also be issued through the User Self Administration Portal.

- **Security Commands** - Gives quick access to reactive security commands, such as *Full Wipe*. *See Remote Security Commands.* Security commands can also be issued through the User Self Administration Portal.
- **Send VPP Invitation** - Send an invitation to an iOS 7.0.3+ user to join the Apple Volume Purchase Program if they have not yet been invited or have not yet accepted an invitation. Check user's status in the *VPP Association Status* column of the *User Grid.*
- **Send Welcome Letter** - Send the Welcome Letter email to the user.
- **Reset for Enrollment** – Used for troubleshooting enrollment issues. Clears server data that prevents a user from re-enrolling a device ot reloading iOS profiles when a device experiences enrollment issues.
  - **Reboot** – Reboots the device. Applicable for Samsung KNOX devices only.
  - **Power Off** – Turns the device off. Applicable for Samsung KNOX devices only.
- **Unblock Password Entry** – unblocks the password entry on a device blocked due to a password policy violation. Applicable for Samsung KNOX devices only.

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

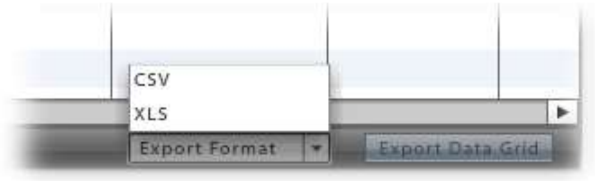
☐ Violation of Restrict User NMDM Connections

☐ Resources Blocked by Device Restriction

Violation Details Pop-up

Exporting Data from the User Grid

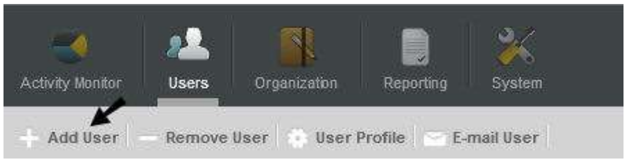
Exporting data from the list to a comma separated values (CSV) or Excel (XLS) file. Choose the *Export Format*, then click the *Export Data Grid* button to save the current grid to a file.



Adding / Removing / Disabling Users

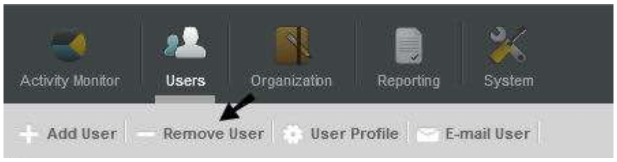
The ***Add User*** button launches a window that allows the manual addition of individual users or addition of users via batch import methods (.CSV file or an LDAP server).

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

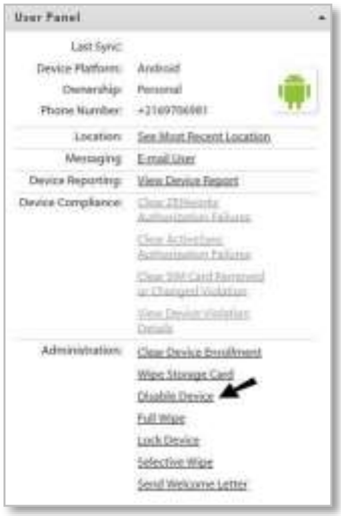


Add User button

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

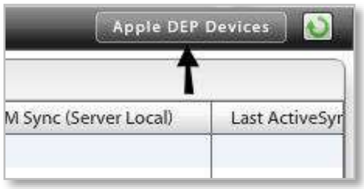
Last Sync:
Device Platform: Android
Ownership: Personal
Phone Number: +2169706981
Location: See Most Recent Location
Messaging: E-mail User
Device Reporting: View Device Report
Device Compliance: Clear ZENworks Authentication Failures
Clear ActiveSync Authentication Failures
Clear SIM Card Removed or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

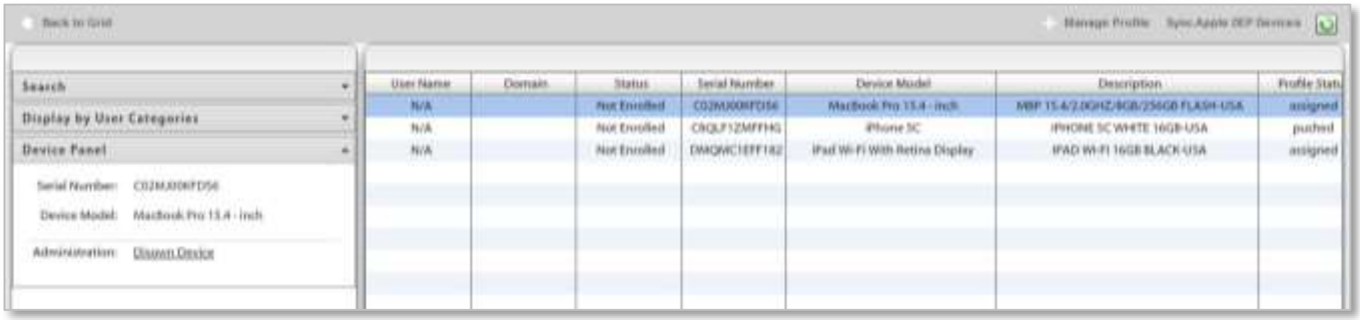
The Apple DEP User Grid

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

> ***Note:*** For information on configuring your system for DEP devices, see the Supervised iOS Devices guide.

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





Serial Number: C02MJ00RFD56
Device Model: MacBook Pro 15.4 - inch
Administration: Disown Device

User Name	Domain	Status	Serial Number	Device Model	Description	Profile Statu
N/A		Not Enrolled	C02MJ00RFD56	MacBook Pro 15.4 - inch	MBP 15.4/2.0GHZ/8GB/256GB FLASH-USA	assigned
N/A		Not Enrolled	C8QLF1ZMFFHG	iPhone 5C	IPHONE 5C WHITE 16GB-USA	pushed
N/A		Not Enrolled	DMQMC1EFF182	iPad Wi-Fi With Retina Display	IPAD WI-FI 16GB BLACK-USA	assigned

Apple DEP User Grid

The User Profile

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

User Information

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

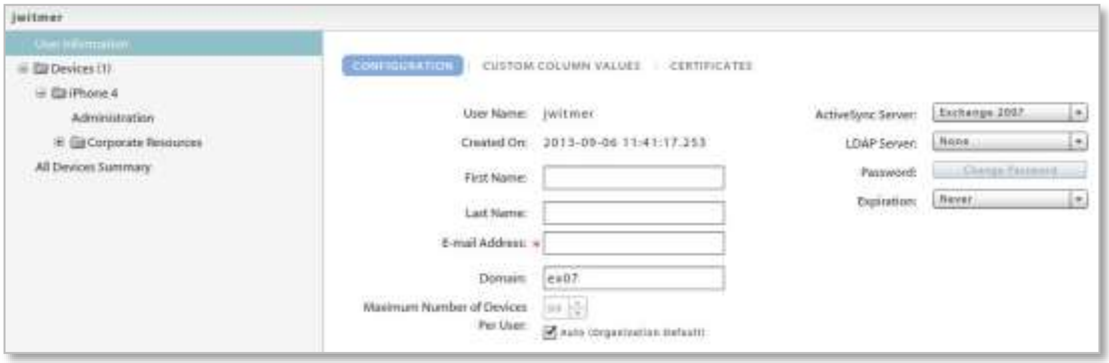
- Configuration
- Custom Column Values
- Certificates
- Local Groups

User Information: Configuration

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

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

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



User Name: jwitmer

Created On: 2013-09-06 11:41:17.253

First Name:

Last Name:

E-mail Address: *

Domain: ex07

Maximum Number of Devices Per User:

☑ Auto (Organization Default)

ActiveSync Server: Exchange 2007

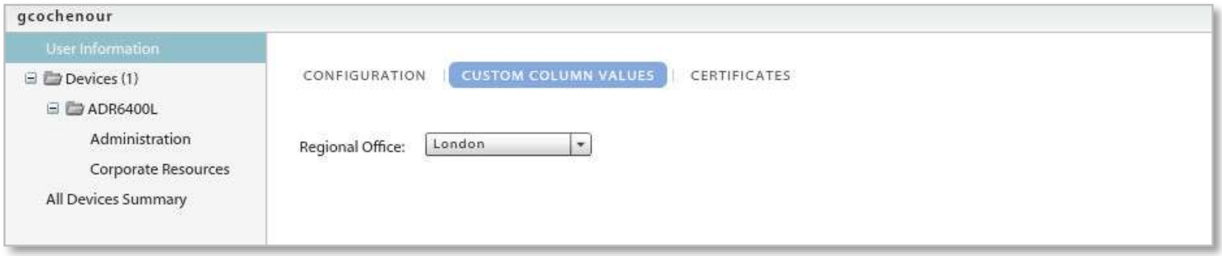
LDAP Server: None

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:

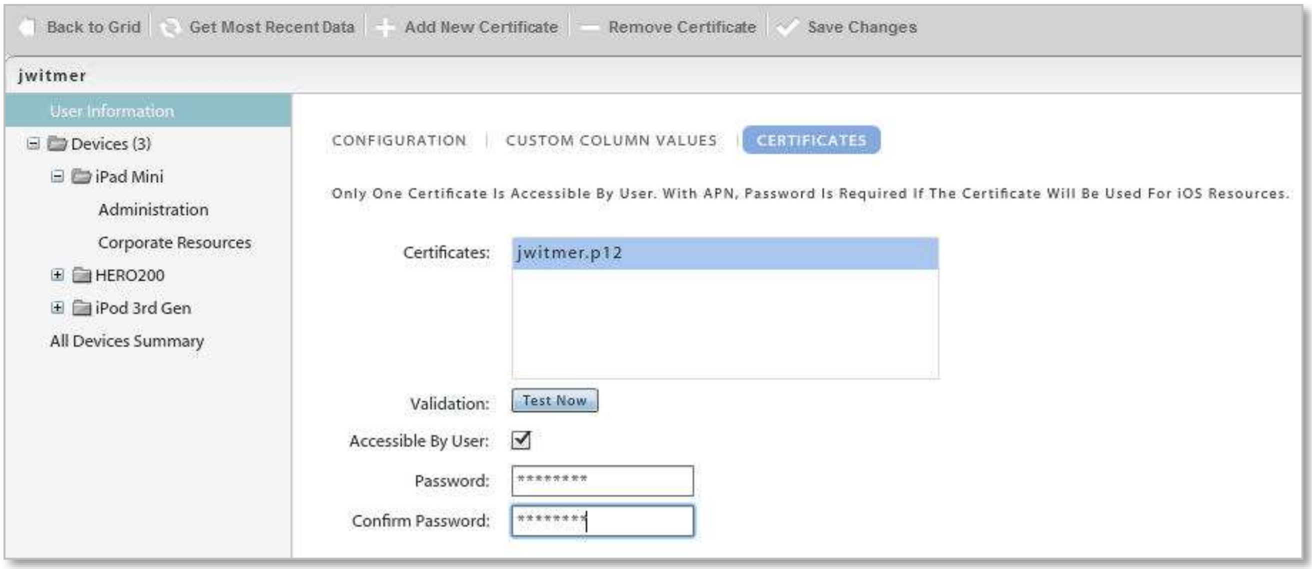
- Instruct users to install the certificate, while in the corporate setting, using Wi-Fi.
- Locate the *ZENworks Mobile Management* Desktop and Mobile User Self-Administration portals outside the corporate firewall.
    - Assign a second address to the *ZENworks Mobile Management* server for the User 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.

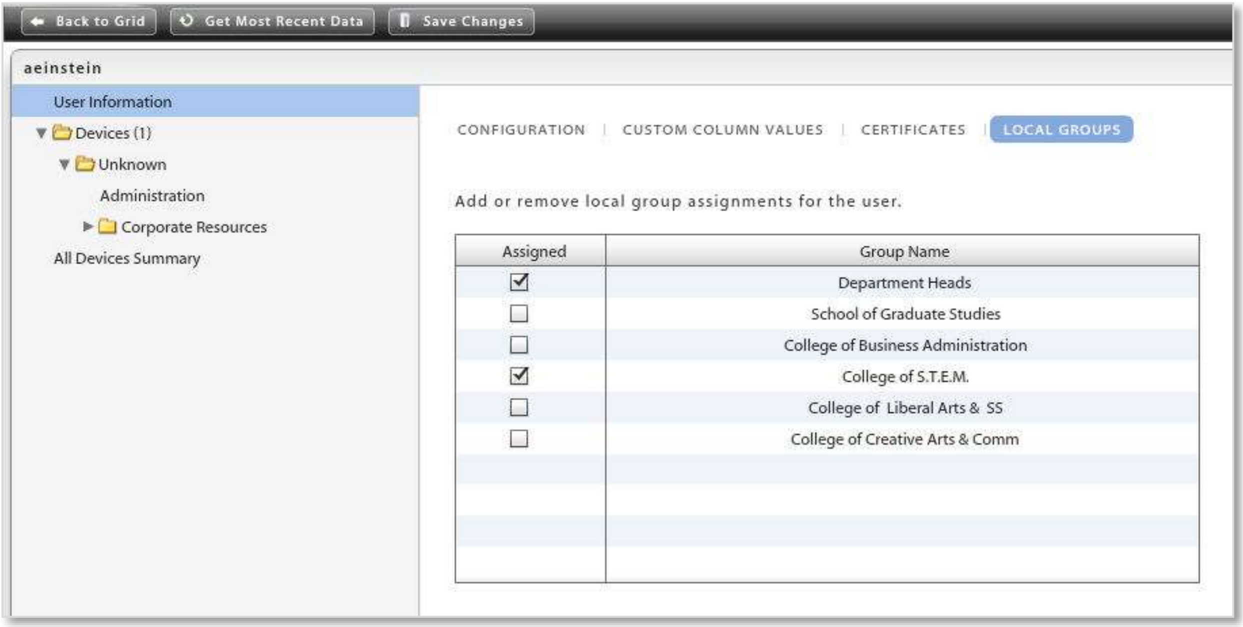
Certificate Formats Supported on Various Device Platforms		
	.cer	**.pfx / .p12**
Android	OS 2.1 update 1	
	OS 2.2	OS 2.2
	OS 2.3	OS 2.3
	OS 2.3.4	OS 2.3.4
BlackBerry (with *GO!NotifySync*)	OS 4.5	
	OS 4.6	
	OS 5.0	
	OS 6.0	OS 6.0
	OS 7.0	OS 7.0
iOS	iOS 6+	iOS 6+

User Information: Local Groups

(*return to User Information menu*)

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

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



Add or remove local group assignments for the user.

Assigned	Group Name
☑	Department Heads
□	School of Graduate Studies
□	College of Business Administration
☑	College of S.T.E.M.
□	College of Liberal Arts & SS
□	College of Creative Arts & Comm

Device Administration

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

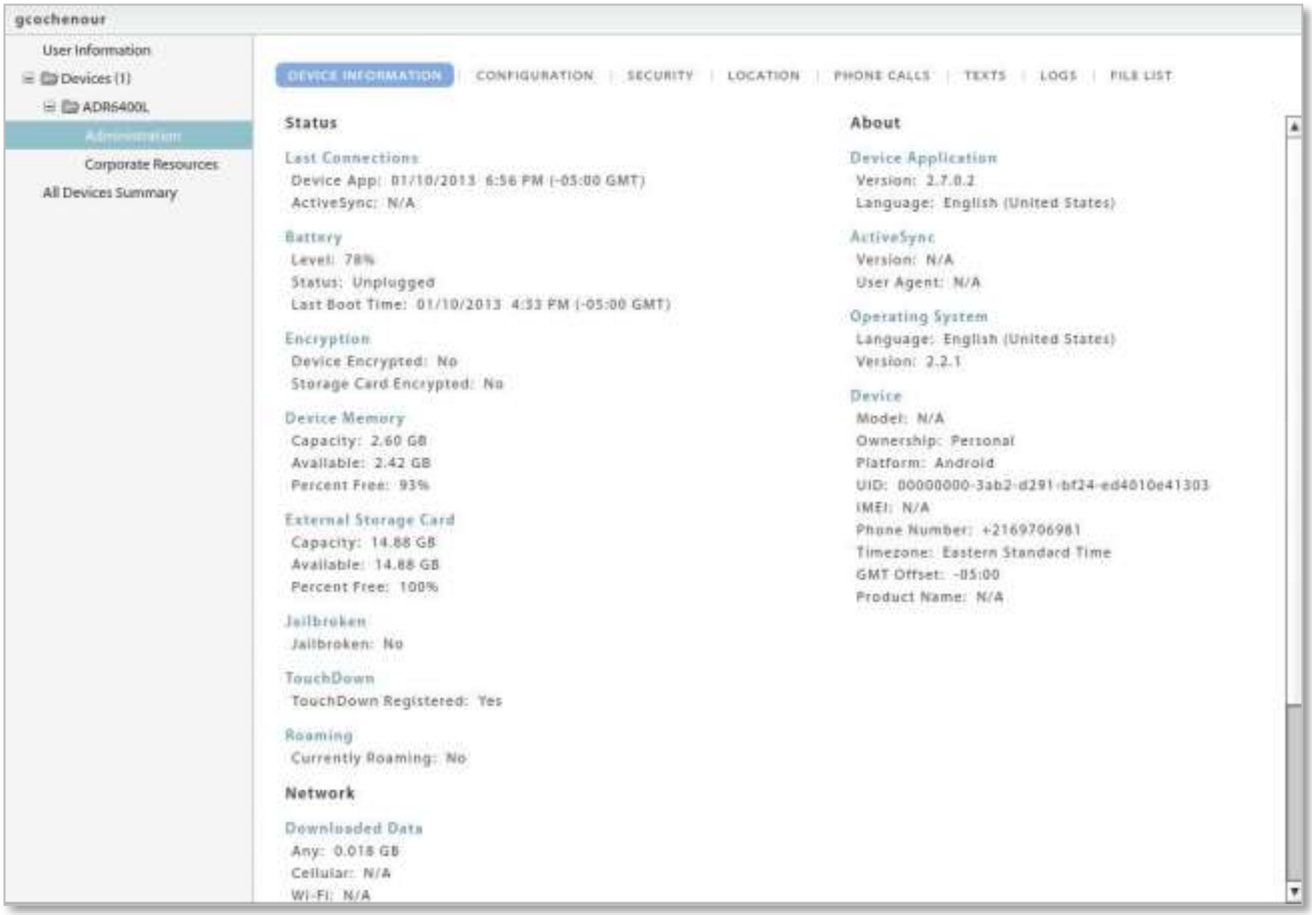
- Device Information
- Configuration
- Security
- Location
- Phone Calls and Texts
- Viewing Logs
- File List

Device Administration: Device Information

(return to Device Administration menu)

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

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



Status

Last Connections
Device App: 01/10/2013 6:56 PM (-05:00 GMT)
ActiveSync: N/A

Battery
Level: 78%
Status: Unplugged
Last Boot Time: 01/10/2013 4:33 PM (-05:00 GMT)

Encryption
Device Encrypted: No
Storage Card Encrypted: No

Device Memory
Capacity: 2.60 GB
Available: 2.42 GB
Percent Free: 93%

External Storage Card
Capacity: 14.88 GB
Available: 14.88 GB
Percent Free: 100%

Jailbroken
Jailbroken: No

TouchDown
TouchDown Registered: Yes

Roaming
Currently Roaming: No

Network

Downloaded Data
Any: 0.018 GB
Cellular: N/A
Wi-Fi: N/A

About

Device Application
Version: 2.7.0.2
Language: English (United States)

ActiveSync
Version: N/A
User Agent: N/A

Operating System
Language: English (United States)
Version: 2.2.1

Device
Model: N/A
Ownership: Personal
Platform: Android
UID: 00000000-3ab2-d291-bf24-ed4010e41303
IMEI: N/A
Phone Number: +2169706981
Timezone: Eastern Standard Time
GMT Offset: -05:00
Product Name: N/A

Device Administration: Configuration

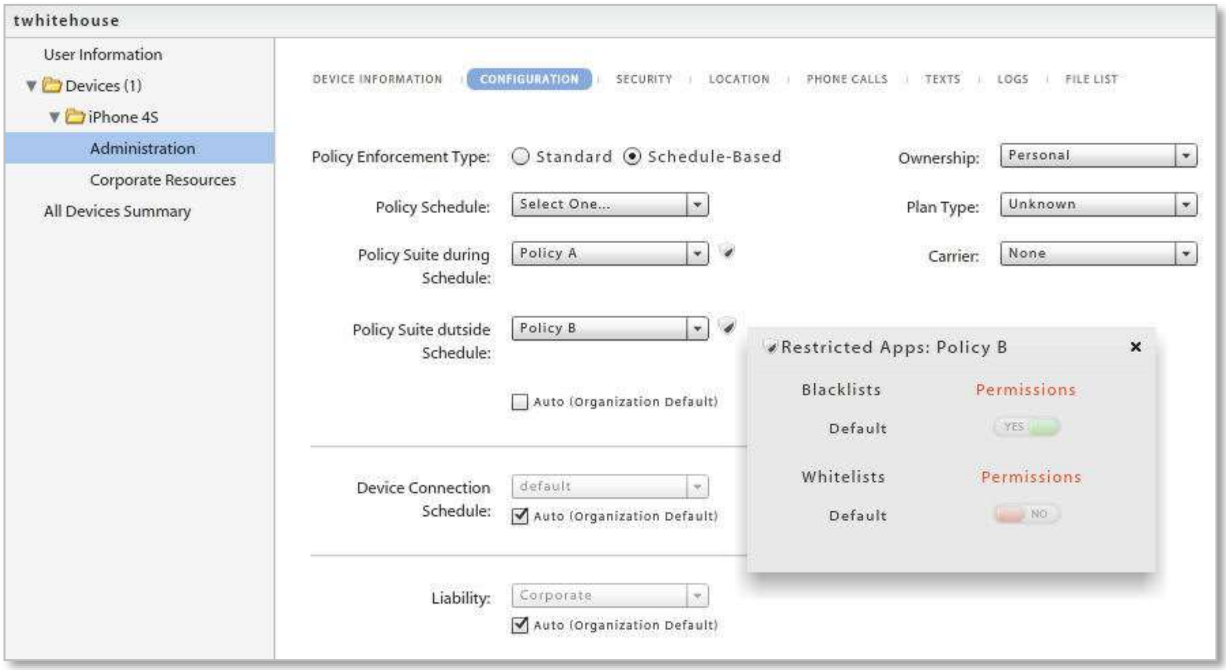
(return to Device Administration menu)

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

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

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

Ownership, Plan Type, Carrier, and 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: Select One...

Policy Suite during Schedule: Policy A

Policy Suite dutside Schedule: Policy B

□ Auto (Organization Default)

Device Connection Schedule: default

☑ Auto (Organization Default)

Liability: Corporate

☑ Auto (Organization Default)

Ownership: Personal

Plan Type: Unknown

Carrier: None

Restricted Apps: Policy B ×

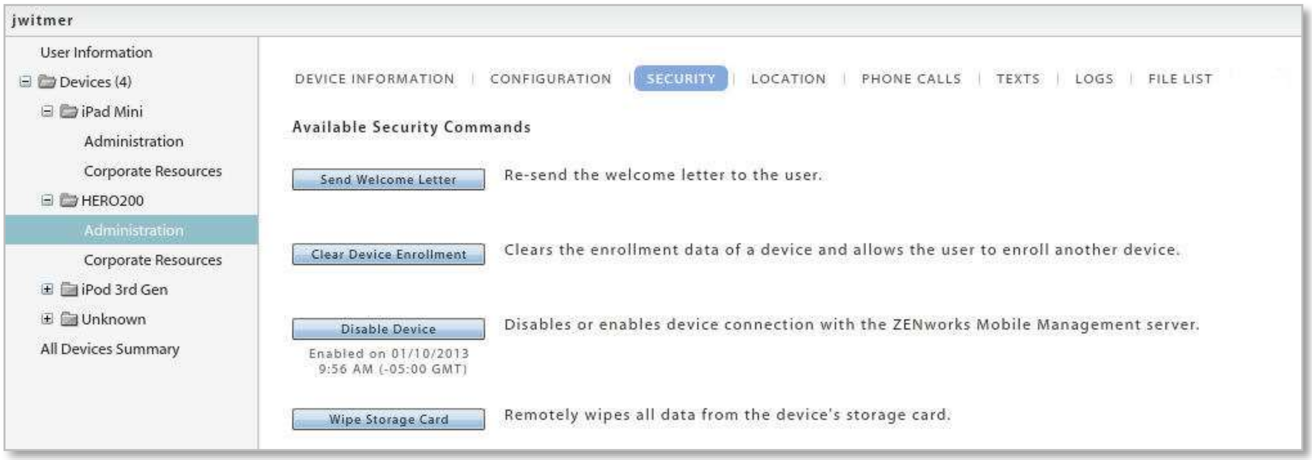
Blacklists	Permissions
Default	YES

Whitelists	Permissions
Default	NO

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.

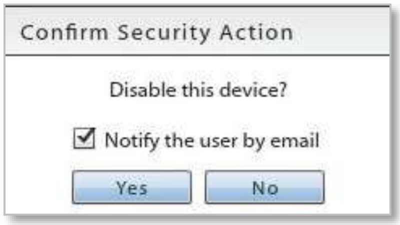
How Security Commands are Issued

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.

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

Security Action Confirmation Emails

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



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	**wOS**	webOS devices
TD/A	*Android devices with TouchDown*	**WP**	Windows Phone devices
NS/BB	*GO!NotifySync for BlackBerry*	**BB10**	BlackBerry 10 devices
iOS	iOS multitasking devices		
TD/iOS	iOS multitasking devices with TouchDown		

Action	Description	Devices that Support
Full Wipe	Administrators can issue a Full Wipe command. Once the wipe is completed, the device is removed from the dashboard User Grid. Functionality varies by device. *Note:* See Appendix A for information on recovering user information for devices removed from the grid. *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 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 *Selective Wipe* option to wipe the data associated with TouchDown. *BlackBerry*: Requires the *GO!NotifySync for BlackBerry* application. Removes all mail and PIM data associated with the *GO!NotifySync* application and removes the *GO!NotifySync* account. Locks the device if *Require Password* is enabled. Erases *GO!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. iOS 7.0.3+ devices enrolled in the Volume Purchase Program : VPP licenses are reclaimed and the user is retired from the program when it is the last iOS 7.0.3+ device associated with the user. *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.	**ZENworks Mobile Management app:** Anrd, NS/BB, iOS, TD/iOS, TD/A **ActiveSync only:** BB10, wOS, WP
Selective Wipe	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.) iOS 7.0.3+ devices enrolled in the Volume Purchase Program : VPP licenses are reclaimed and the user is retired from the program when it is the last iOS 7.0.3+ device associated with the user.	**ZENworks Mobile Management app:** Anrd, NS/BB, iOS, TD/iOS, TD/A

Remove User	Stops managing all devices associated with the user and subsequently removes the user from the *ZENworks Mobile Management* server and dashboard grid. iOS 7.0.3+ devices enrolled in the Volume Purchase Program : VPP licenses are reclaimed and the user is retired from the program.	**ZENworks Mobile Management app:** Anrd, NS/BB, iOS, TD/iOS, TD/A **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
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
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 **ActiveSync only:** BB10, wOS, WP
Disown Device	Disown Device should only be used if you want to permanently remove an Apple DEP device from the grid and notify the Apple servers that your organization no longer owns the device. Once a device is disowned, it cannot be reassigned to the server as an Apple DEP device. Disowning removes the DEP profile from the device. **Note**: Issue a Selective Wipe prior to disowning a device. *(In a future release, disowning a device will initiate a Selective Wipe automatically, as well as remove the DEP profile from the device.)*	**iOS DEP devices**
Suspend/Resume Device	Device is managed (it can be wiped and continues to send statistics) while suspended, but blocked from corporate resources. User cannot access the application's Config, Managed Apps, and File Share options and must enter a password to gain full functionality when suspension is lifted.	**ZENworks Mobile Management app:** Anrd, NS/BB, iOS, TD/iOS, TD/A **ActiveSync only:** BB10, wOS, WP7
Show Recovery Password	If a device has the capability to issue a request for a temporary recovery password, this is where you can retrieve the temporary unlock password that has been generated. A user can also view it from the *ZENworks Mobile Management* User Self-Administration portal. See *Enabling Password Recovery*.	**ZENworks Mobile Management app:** NS/BB, TD/A, TD/iOS
Clear Passcode	iOS device passcode is cleared. If a passcode is required by the user's policy, the user is prompted to enter a new passcode.	**ZENworks Mobile Management app:** iOS, TD/iOS
Trigger APN	Immediately sends an APN to an iOS device causing it to check the server and retrieve any pending commands. This can be used to remedy a situation in which Apple Push Notifications are not synchronizing. A list of pending iOS MDM device commands accompanies this option. Verify that the device is unlocked before issuing this command.	**ZENworks Mobile Management app:** iOS, TD/iOS
Trigger GCM	Immediately sends a notification to an Android device causing it to check the server and retrieve any pending commands. This can be used to remedy a situation in which GCM notifications are not synchronizing, allowing the administrator to get the latest stats and location for the device.	**ZENworks Mobile Management app:** Anrd, TD/A

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.

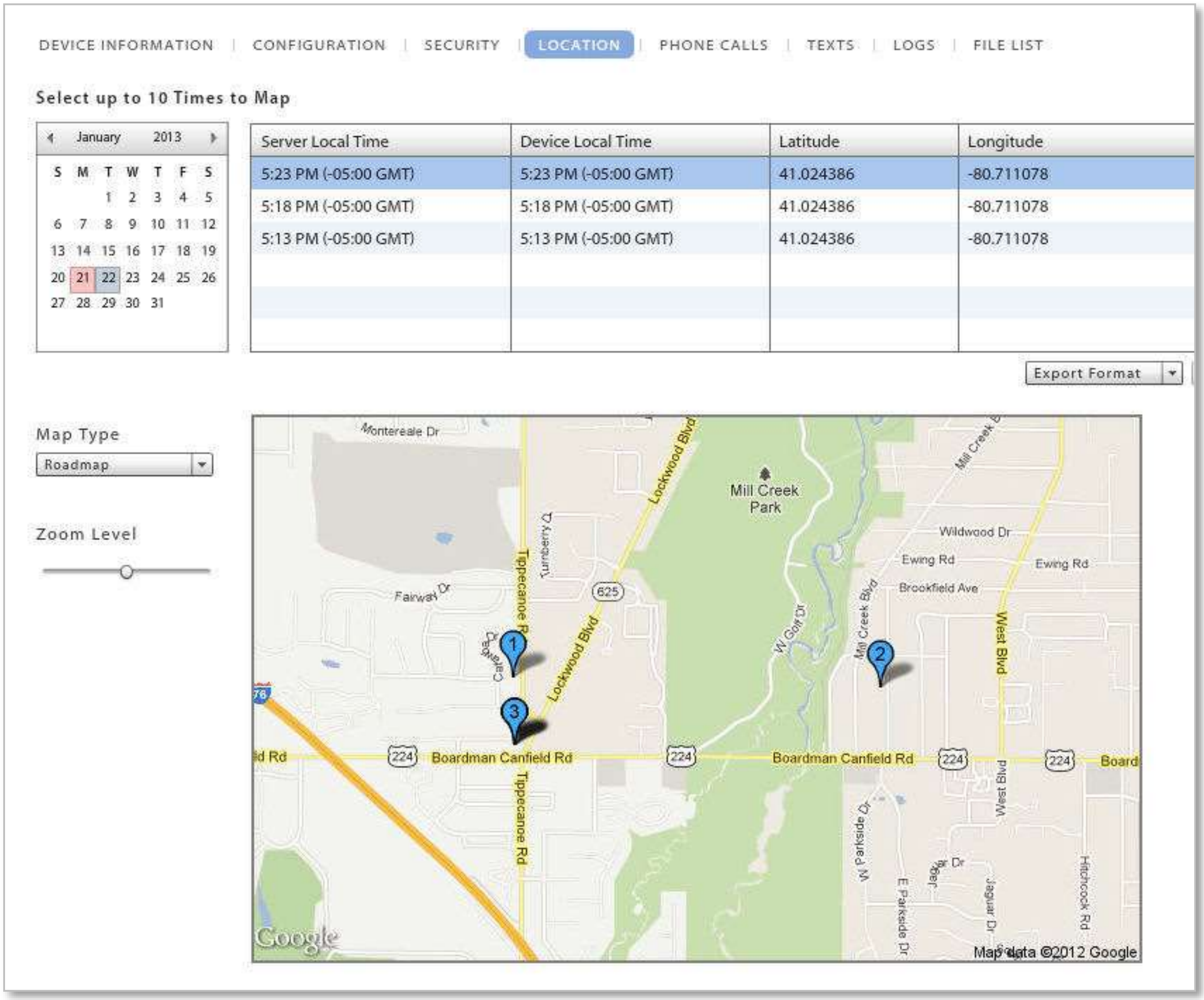
Device Administration: Location

(*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

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

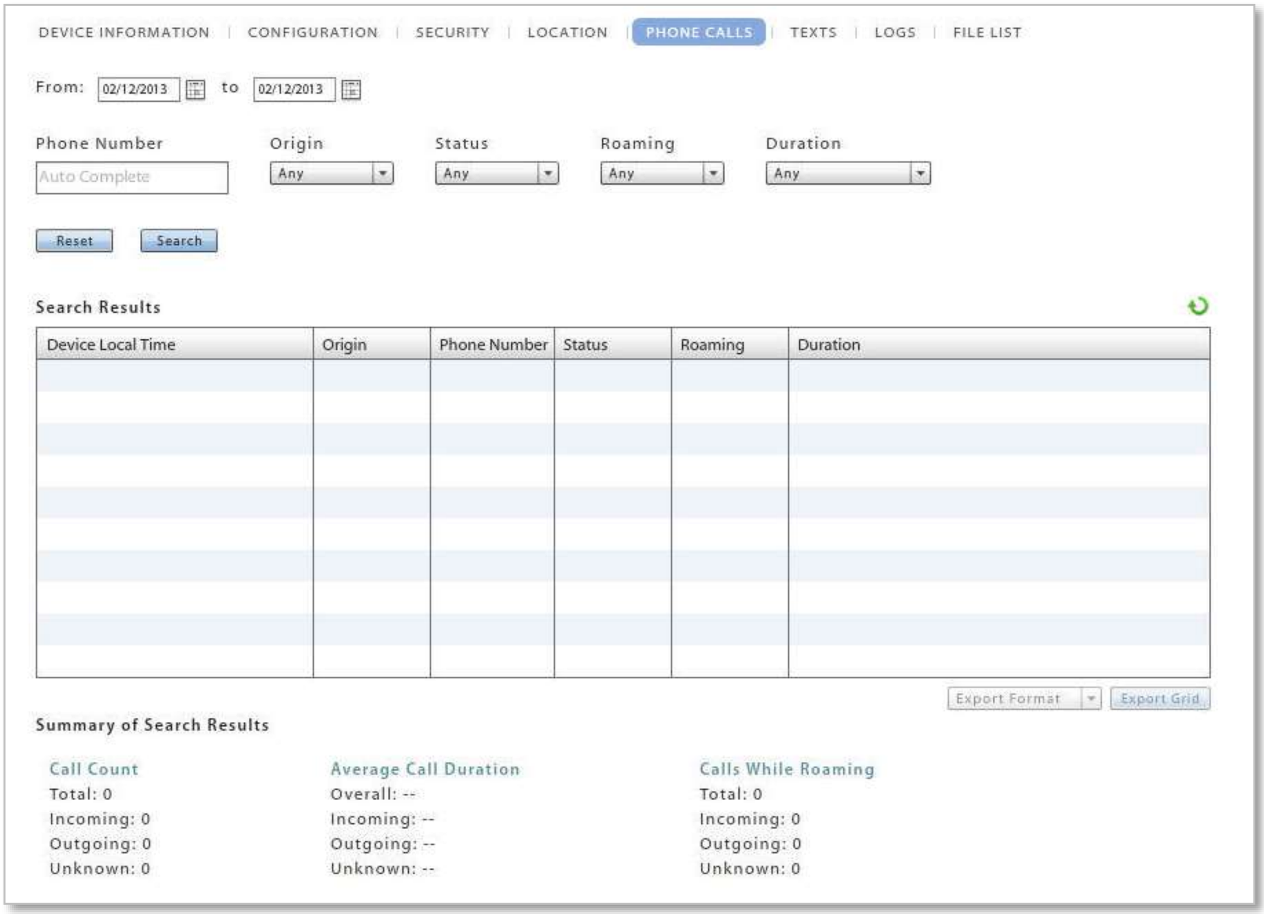
On the action bar, click the ***Get Most Recent Data*** button to refresh the location data.
Click the ***Locate on Google Maps*** button to view a Google Map and the location address.

Device Administration: Phone Calls and Texts

(return to Device Administration menu)

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

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



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

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

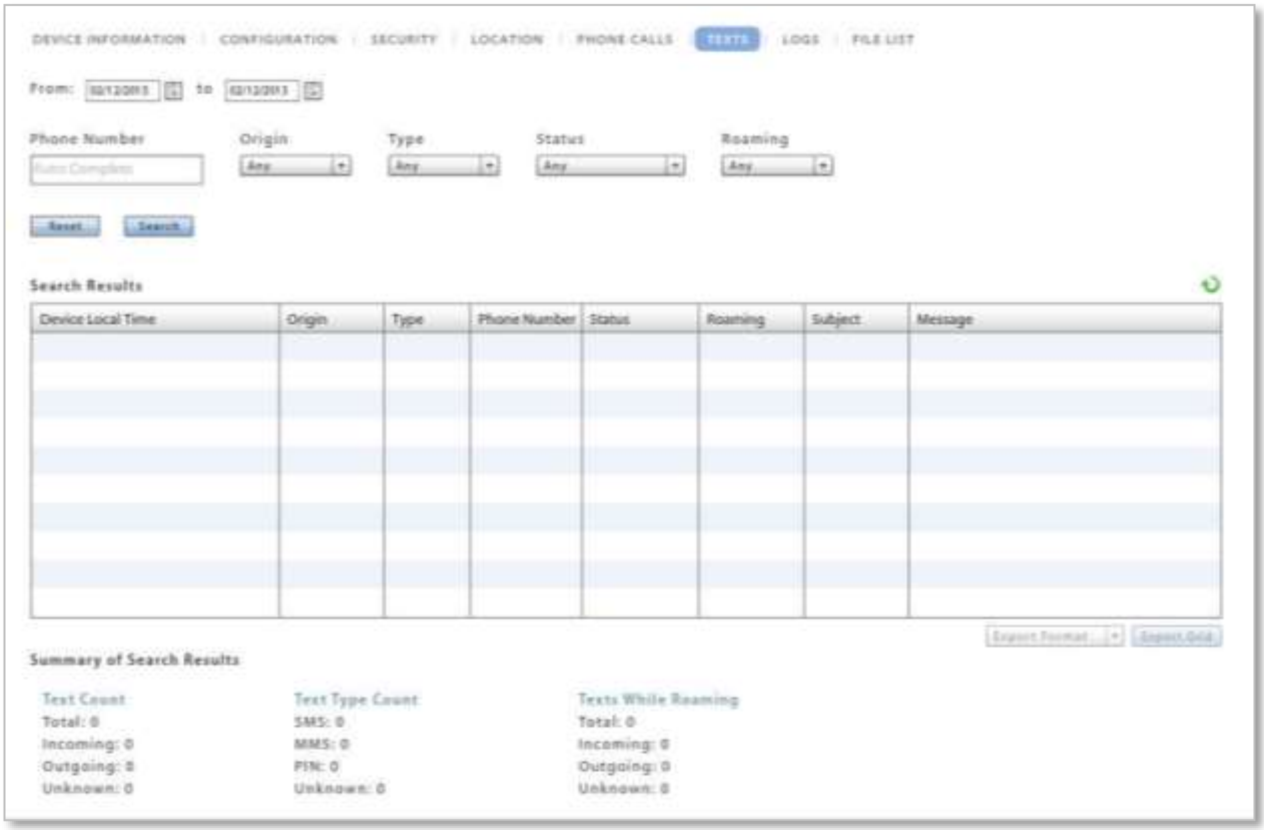
Call Count
Total: 0
Incoming: 0
Outgoing: 0
Unknown: 0

Average Call Duration
Overall: --
Incoming: --
Outgoing: --
Unknown: --

Calls While Roaming
Total: 0
Incoming: 0
Outgoing: 0
Unknown: 0

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

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



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

Phone Number: Auto Complete

Origin: Any

Type: Any

Status: Any

Roaming: Any

Search Results

Device Local Time	Origin	Type	Phone Number	Status	Roaming	Subject	Message

Summary of Search Results

Text Count
Total: 0
Incoming: 0
Outgoing: 0
Unknown: 0

Text Type Count
SMS: 0
MMS: 0
PIN: 0
Unknown: 0

Texts While Roaming
Total: 0
Incoming: 0
Outgoing: 0
Unknown: 0

Device Administration: Viewing Logs

(return to Device Administration menu)

User level logs assist administrators with diagnosing problems and in understanding the communications between devices and the server. Both server and device logging options are available.

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

- **ActiveSync Log** – View events logged during connections between the *ZENworks Mobile Management* server and the ActiveSync server and between the device's ActiveSync client and the *ZENworks Mobile Management* server.
- **GCM Log** –View successful events logged during connections between the *ZENworks Mobile Management* server and the Google Cloud Messaging (GCM) server and between the *ZENworks Mobile Management* server and Android devices using GCM service.
- **iOS MDM Sync Log –** View successful events logged during connections between the *ZENworks Mobile Management* server and the Apple iOS MDM server and between the *ZENworks Mobile Management* server and the device's iOS MDM functions. Unsuccessful events (errors) are logged in the Error Chain Log. (iOS device specific)
- **ZENworks Sync Log** - View events logged during connections between the device's *ZENworks Mobile Management* app and the *ZENworks Mobile Management* server.
- **Configuration/Feedback Log** – View results of a request to see managed iOS application configuration and feedback information.
- **Data Usage Log** – Track the amount of data being exchanged:
    - Between the device's *ZENworks Mobile Management* app and the *ZENworks Mobile Management server*
    - Between the device's ActiveSync client and the *ZENworks Mobile Management* server
    - As iOS MDM traffic between the device and the *ZENworks Mobile Management* servers
    - Between the *ZENworks Mobile Management* and ActiveSync servers
- **Device Log** – to request and view a log from a device running the *ZENworks Mobile Management* application.
- **Error Chain Log** – to view detailed messages for errors logged in the *iOS MDM Sync Log*. (iOS device specific)

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

Configuration/Feedback Log

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

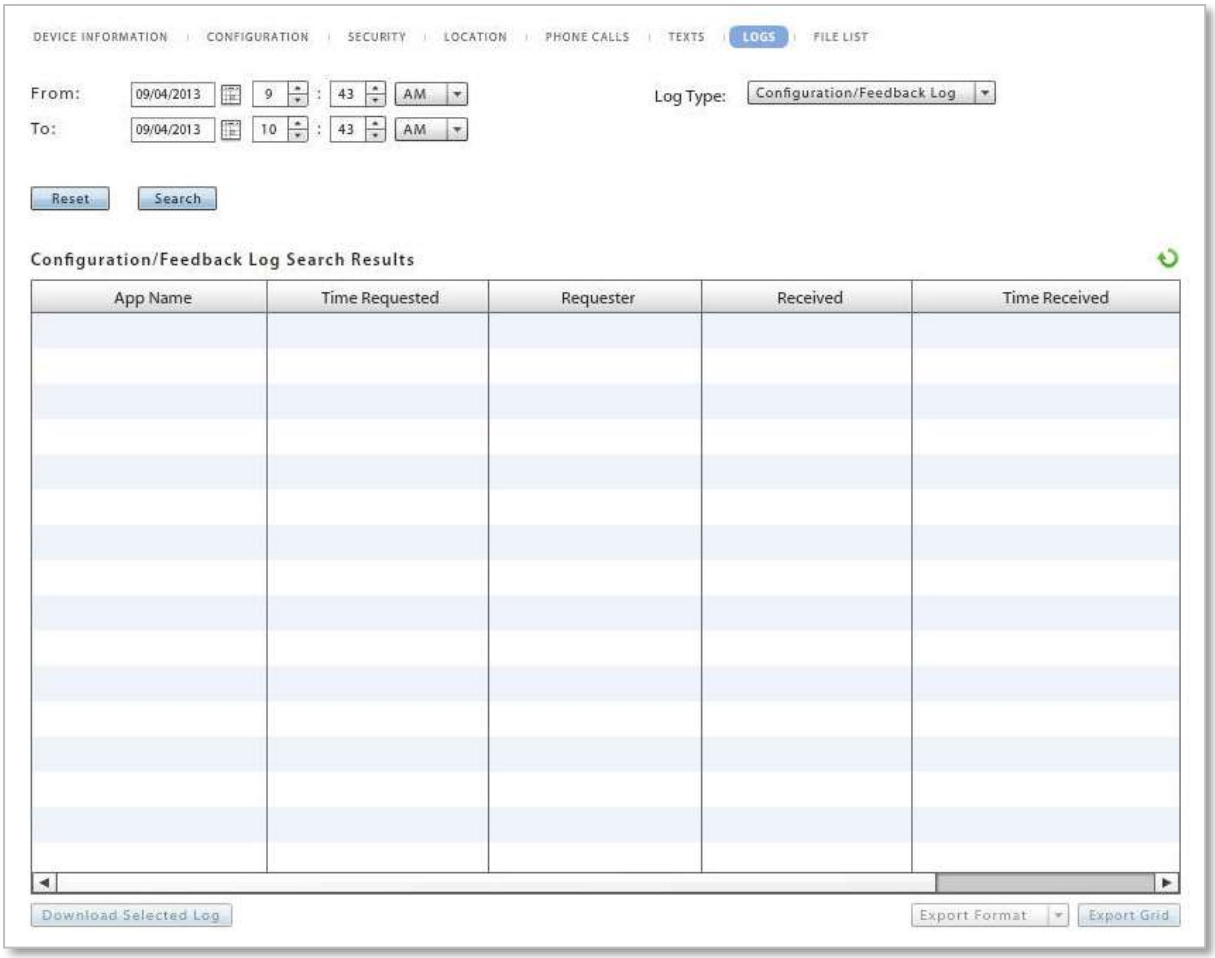
The log displays:

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

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

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

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



From: 09/04/2013 9 : 43 AM

To: 09/04/2013 10 : 43 AM

Log Type: Configuration/Feedback Log

Configuration/Feedback Log Search Results

App Name	Time Requested	Requester	Received	Time Received

Sample Configuration/Feedback Log Grid

Synchronization Logs

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

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

The GCM Log logs successful events that occur during connections between the *ZENworks Mobile Management* server and the Google Cloud Messaging server and between the *ZENworks Mobile Management* server and Android devices using GCM service.

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

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

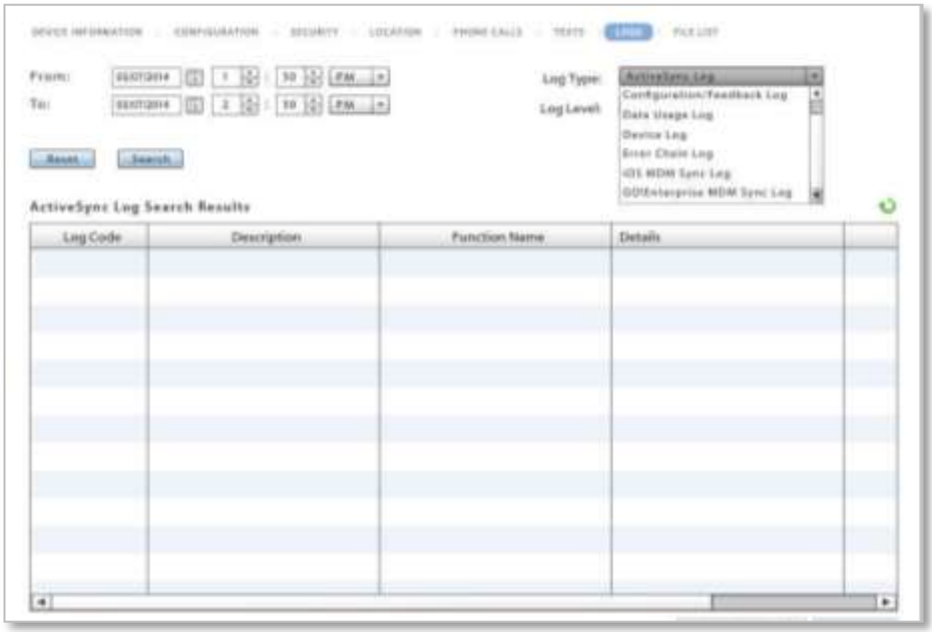
The logs display:

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

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

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

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



From: [illegible] 1 : 50 PM

To: [illegible] 2 : 10 PM

Log Type: ActiveSync Log

Log Level:

ActiveSync Log Search Results

Log Code	Description	Function Name	Details	

Sample Synchronization Log Grid

Data Usage Log

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

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

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

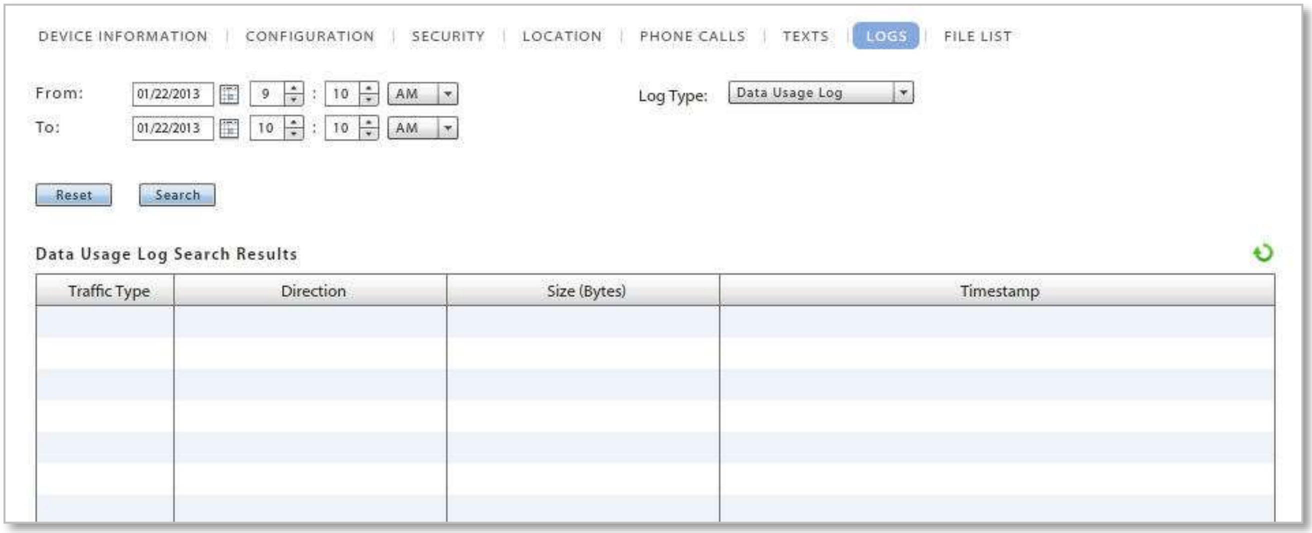
The log displays:

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

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

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

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



From: 01/22/2013 9 : 10 AM

To: 01/22/2013 10 : 10 AM

Log Type: Data Usage Log

Traffic Type	Direction	Size (Bytes)	Timestamp

Device Logs

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

Device Type	**Device Requirements / Behavior**
Android	The device sends only the logcat log to the dashboard. *ZENworks* logging must be enabled on the device (*Log Settings*). The *ZENworks* log is written to the SD card.
BlackBerry (with *GO!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.

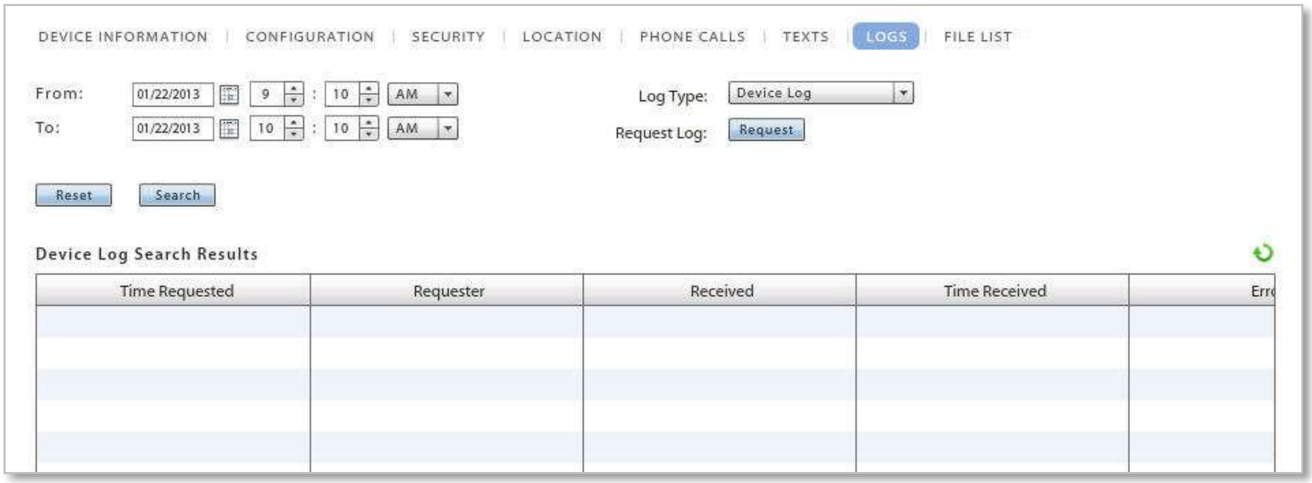
Select ***Device Log*** from the drop-down list.

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

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*.

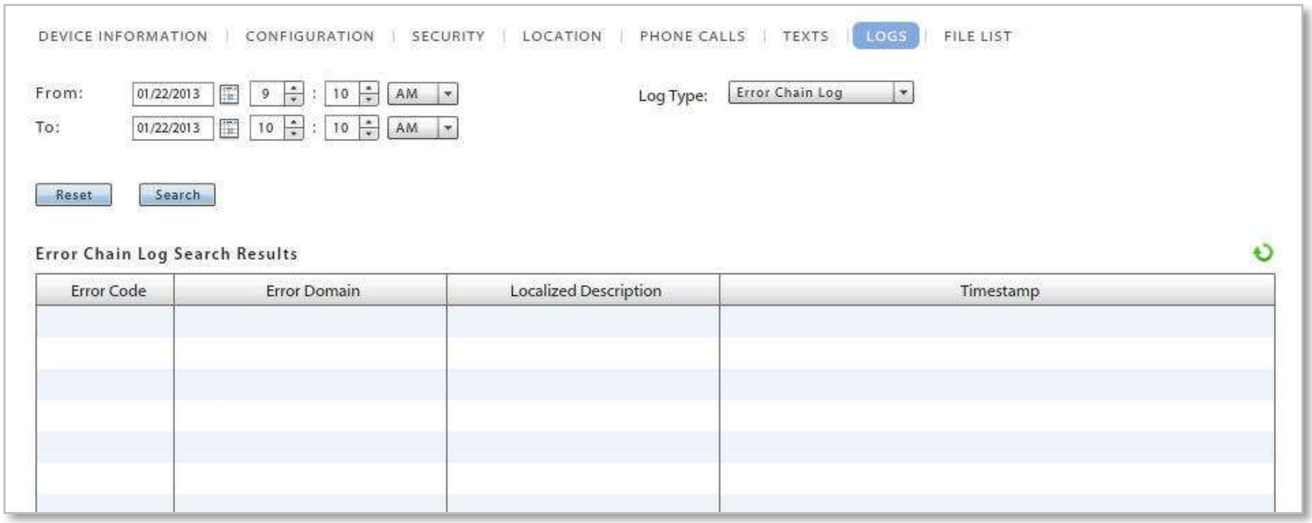
The log displays:

- 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

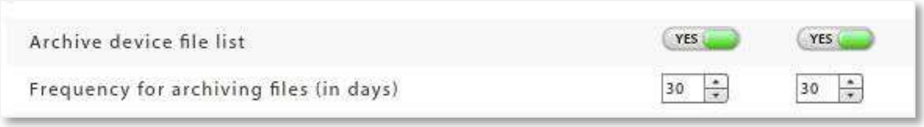
Error Chain Log Grid

Device Administration: File List

(return to Device Administration menu)

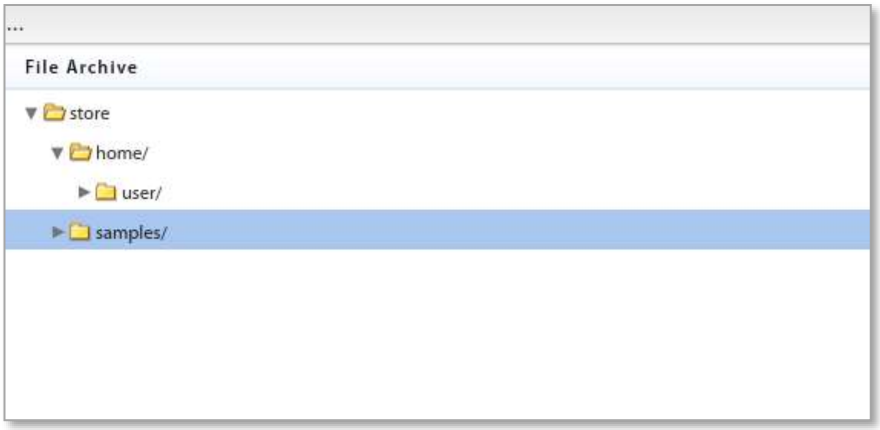
Select the ***Archive device file list*** tab to view the file list sent up from the device. The *Archive files on device* policy rule must be enabled in the policy suite to which the user belongs. When the rule is enabled, the device periodically sends a list of all folders and files stored on the device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

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



Archive device file list	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/

Corporate Resource Assignments

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

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

> **Note:** Configuration of these resources is done from the *Organization* view. See the Organization Administration Guide. Reference the sections, *Corporate Resource Management* and *Application Management.*
>
> Removal of a resource that has been assigned via LDAP group or folder is temporary, since LDAP periodic updates will keep reassigning the resource.

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

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

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

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

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

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

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

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

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

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

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

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

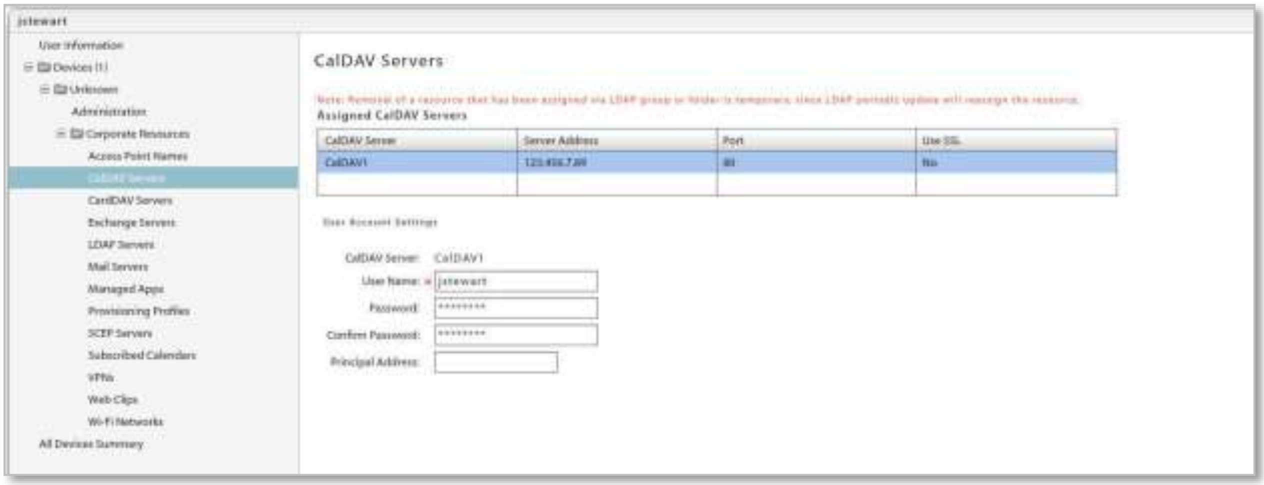
Mail Servers and ***Assign Exchange Servers*** have two options that can be enabled/disabled to govern how the mail account can be used by an iOS user. If they are set when the resource is created, however, they cannot be changed at the user level.

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

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

Corporate Resources: Servers, Networks, etc.

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



CalDAV Servers

Note: Removal of a resource that has been assigned via LDAP group or folder is temporary, since LDAP periodic update will reassign the resource.

Assigned CalDAV Servers

CalDAV Server	Server Address	Port	Use SSL
CalDAV1	123.456.7.89	80	No

User Account Settings

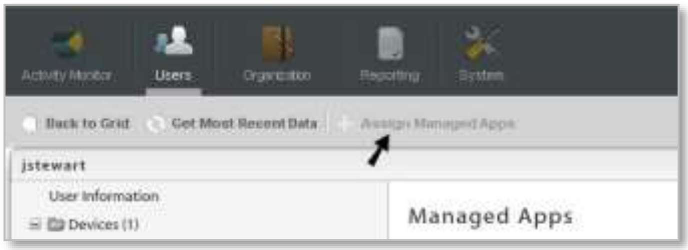
CalDAV Server: CalDAV1
User Name: * jstewart
Password: ********
Confirm Password: ********
Principal Address:

Sample iOS Resource Assignment

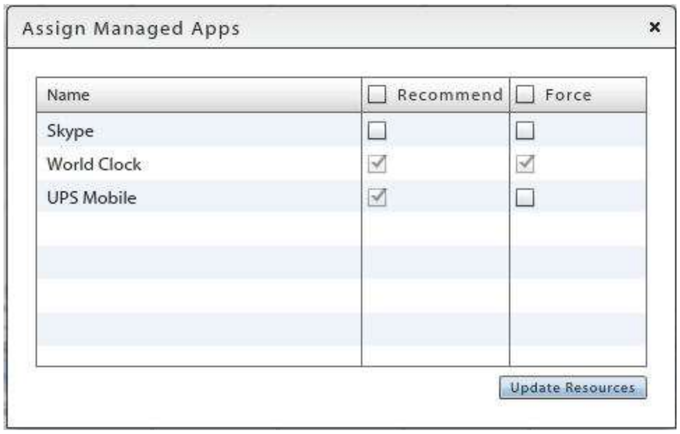
Corporate Resources: Managed Apps

Assigning Managed Apps

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

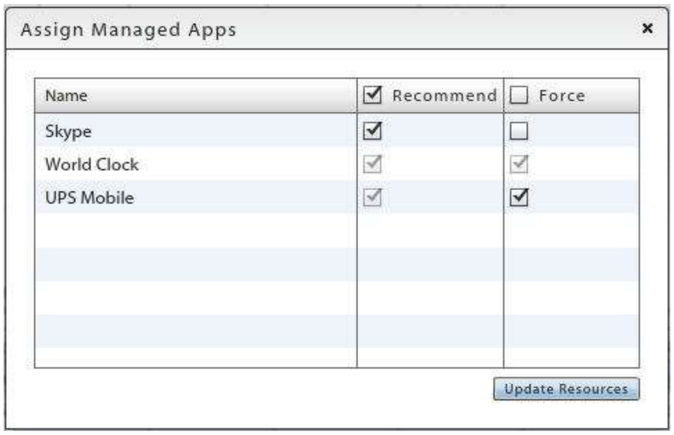


3. A pop-up grid appears listing all apps available for the user's device type. Check boxes for apps that have already been assigned to the user via a Policy Suite, LDAP Group/Folder, or Local Group will be grayed out and cannot be edited. An administrator can check any box that is not grayed out to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



Name	□ Recommend	□ Force
Skype	□	□
World Clock	☑	☑
UPS Mobile	☑	□

Assign apps that have not already been assigned



Name	☑ Recommend	□ Force
Skype	☑	□
World Clock	☑	☑
UPS Mobile	☑	☑

Remove only the apps assigned at the user level

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

The App Grids: Policies that Control Application Reporting and Management

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

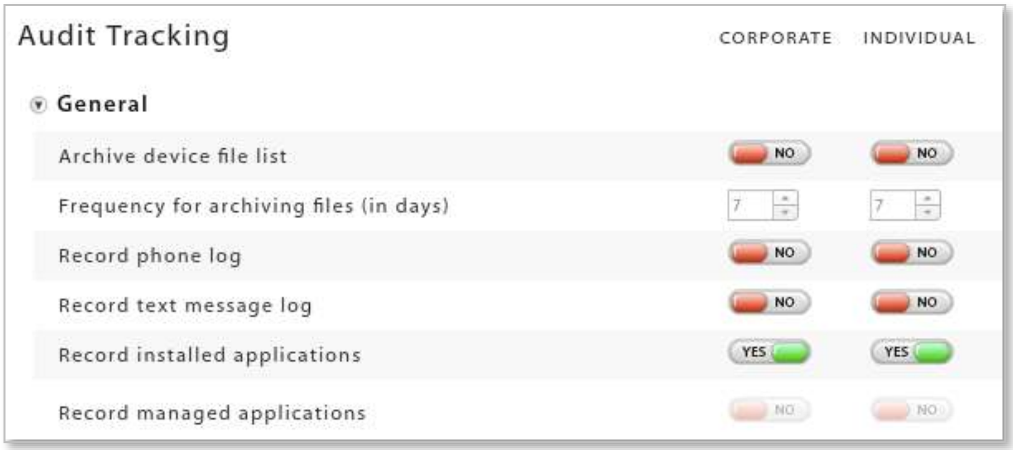
Certain policies must be enabled in order for app information to be reported in the grids.

ANDROID POLICIES

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

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

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



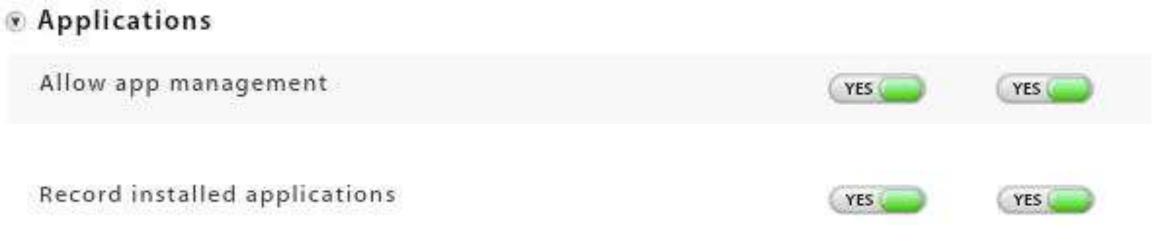
Audit Tracking

General	CORPORATE	INDIVIDUAL
Archive device file list	NO	NO
Frequency for archiving files (in days)	7	7
Record phone log	NO	NO
Record text message log	NO	NO
Record installed applications	YES	YES
Record managed applications	NO	NO

IOS POLICIES

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

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



Applications		
Allow app management	YES	YES
Record installed applications	YES	YES

The App Grids: Managed Apps

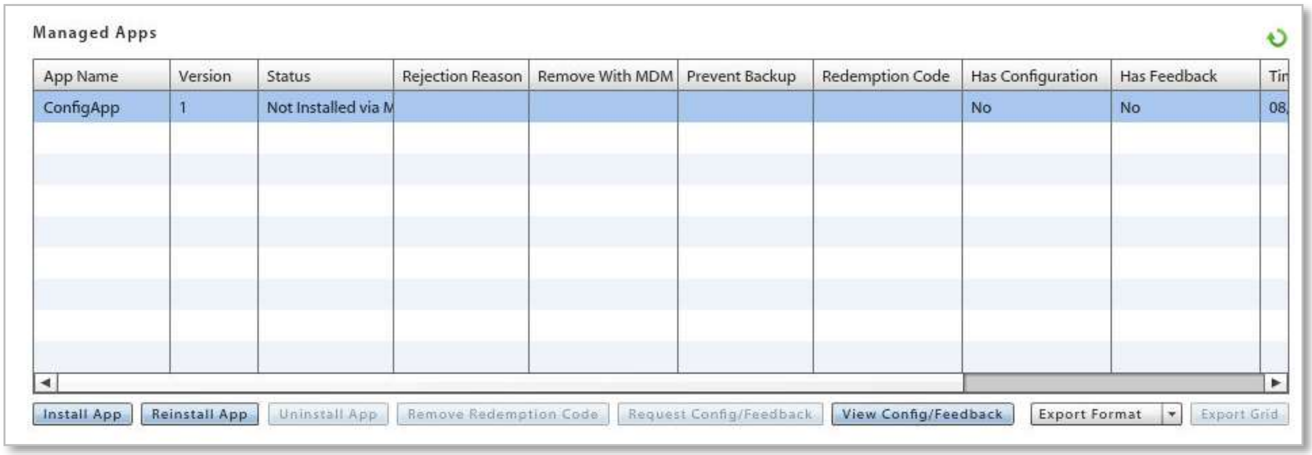
The ***Managed Apps*** grid lists all applications available to an Android or iOS user as determined by the *Managed App Permissions* on the policy suite with which the user is associated.

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

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

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

iOS Managed Apps Grid



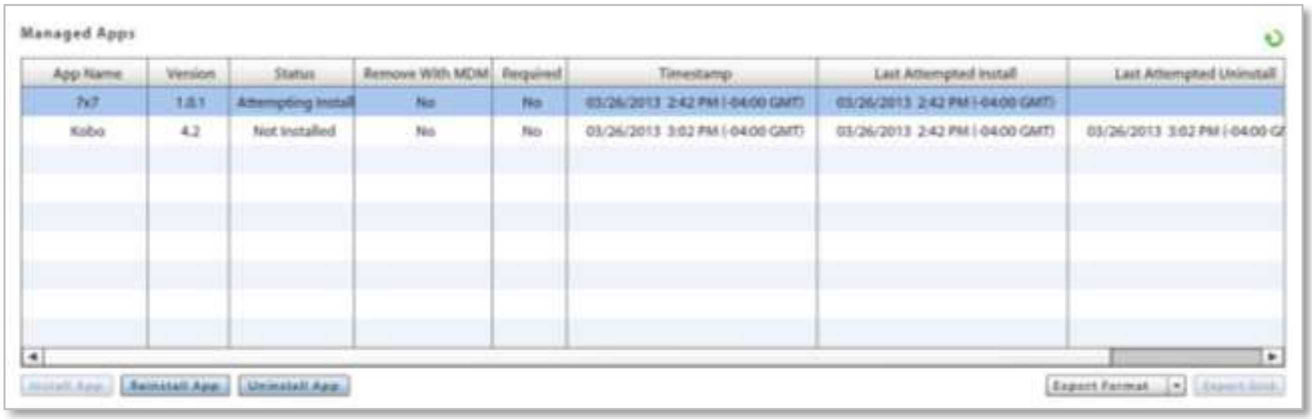
Managed Apps

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

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*. OR ○ Indicates the app was installed prior to the device being enrolled with MDM or prior to the app being designated as a managed app. MDM is not able to manage it unless the user removes the app and then re-installs it through MDM. • *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.
Has Configuration	Whether the app has a server-provided configuration.
Has Feedback	Whether the configured app has feedback for the server.
Timestamp	Last update of the app's status.
Install App button	Issues a command that prompts the user to install the app.
Reinstall App button	Issues a command that prompts the user to reinstall the app.
Uninstall App button	Issues a command that prompts the user to uninstall the app. The *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.
Request Config/Feedback button	If an app in the Managed Apps list has a server-provided configuration or feedback, click this button to request information about whether the app received the configuration file.
View Config/Feedback button	Links to the ***Logs*** tab so that you can view the information the app received via the configuration file and any available feedback information.

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.

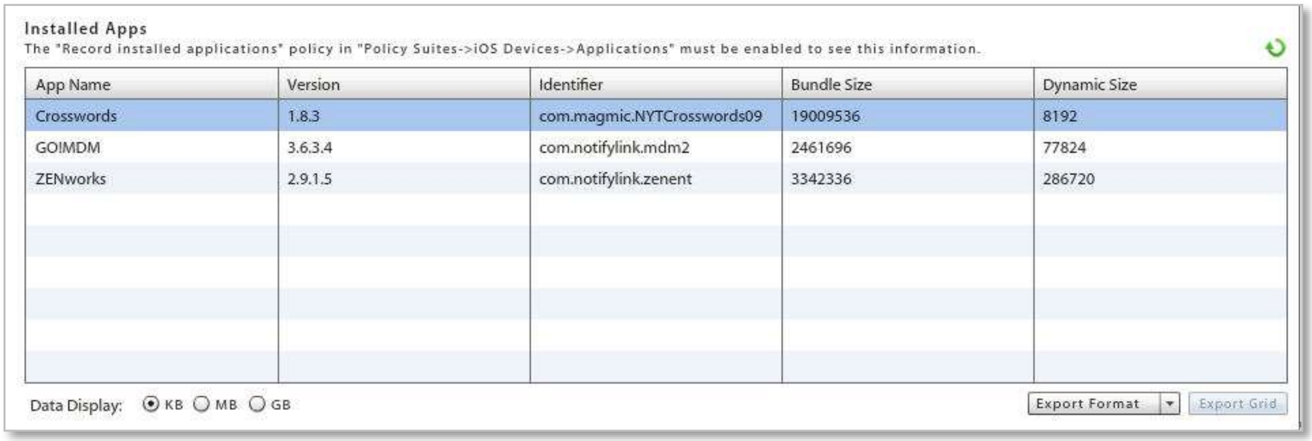
The App Grids: Installed Apps

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

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

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

IOS INSTALLED APPS GRID



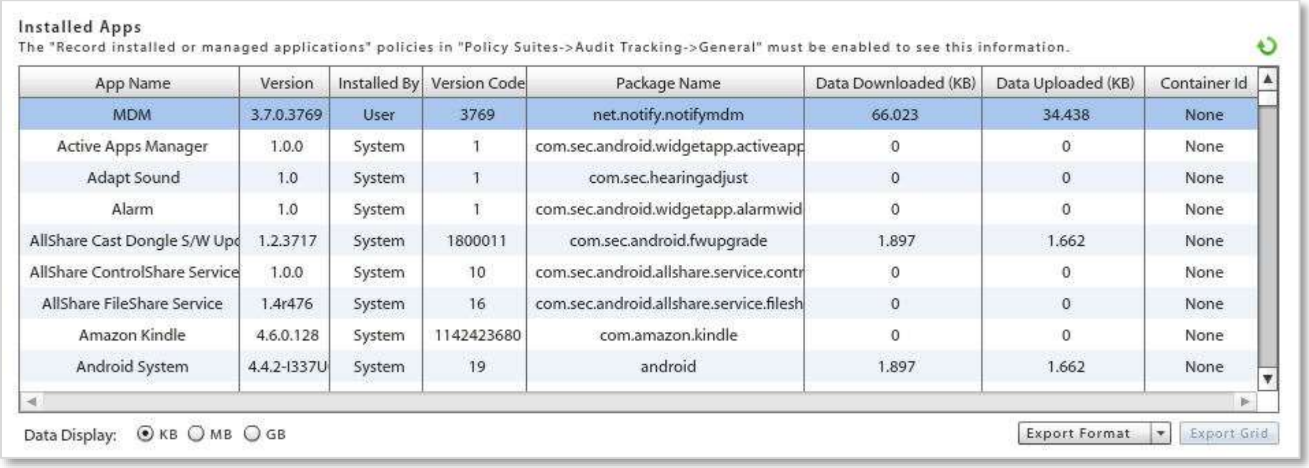
Installed Apps

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

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

Data Display: ● KB ○ MB ○ GB

ANDROID INSTALLED APPS GRID



Installed Apps

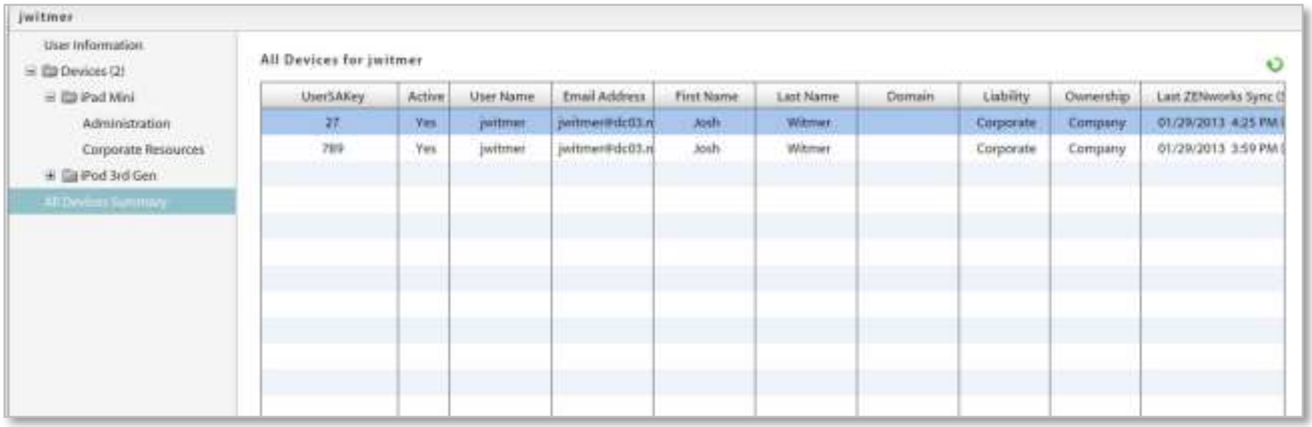
The "Record installed or managed applications" policies in "Policy Suites->Audit Tracking->General" must be enabled to see this information.

App Name	Version	Installed By	Version Code	Package Name	Data Downloaded (KB)	Data Uploaded (KB)	Container Id
MDM	3.7.0.3769	User	3769	net.notify.notifymdm	66.023	34.438	None
Active Apps Manager	1.0.0	System	1	com.sec.android.widgetapp.activeapp	0	0	None
Adapt Sound	1.0	System	1	com.sec.hearingadjust	0	0	None
Alarm	1.0	System	1	com.sec.android.widgetapp.alarmwid	0	0	None
AllShare Cast Dongle S/W Upc	1.2.3717	System	1800011	com.sec.android.fwupgrade	1.897	1.662	None
AllShare ControlShare Service	1.0.0	System	10	com.sec.android.allshare.service.contr	0	0	None
AllShare FileShare Service	1.4r476	System	16	com.sec.android.allshare.service.filesh	0	0	None
Amazon Kindle	4.6.0.128	System	1142423680	com.amazon.kindle	0	0	None
Android System	4.4.2-I337U	System	19	android	1.897	1.662	None

Data Display: ● KB ○ MB ○ GB

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.



All Devices for jwitmer

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

Local Groups

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

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

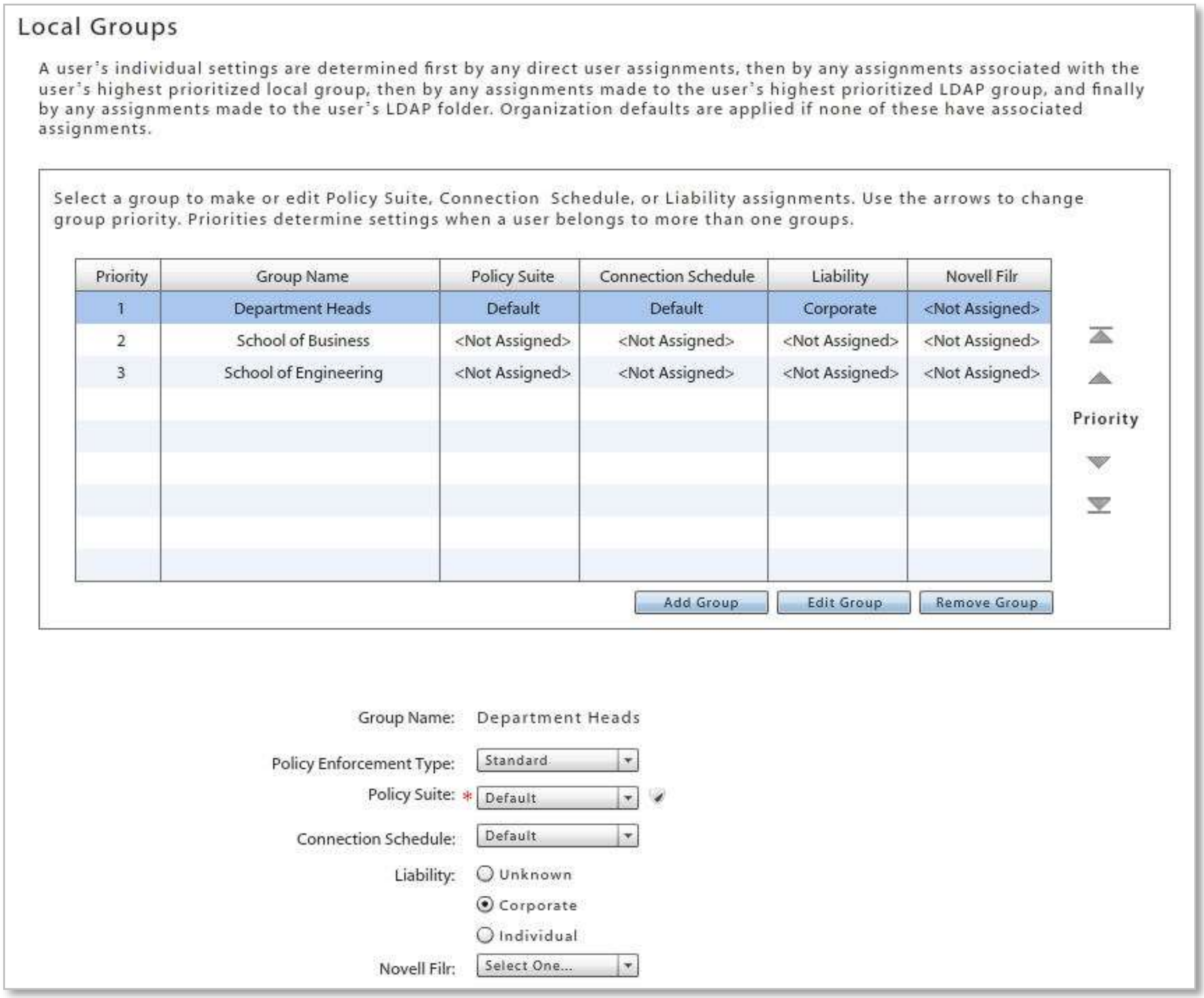
A user may belong to multiple groups. The groups can be prioritized to determine the order in which the settings are inherited. See *Prioritizing Groups* below,

Managing Local Groups

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

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

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



Local Groups

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

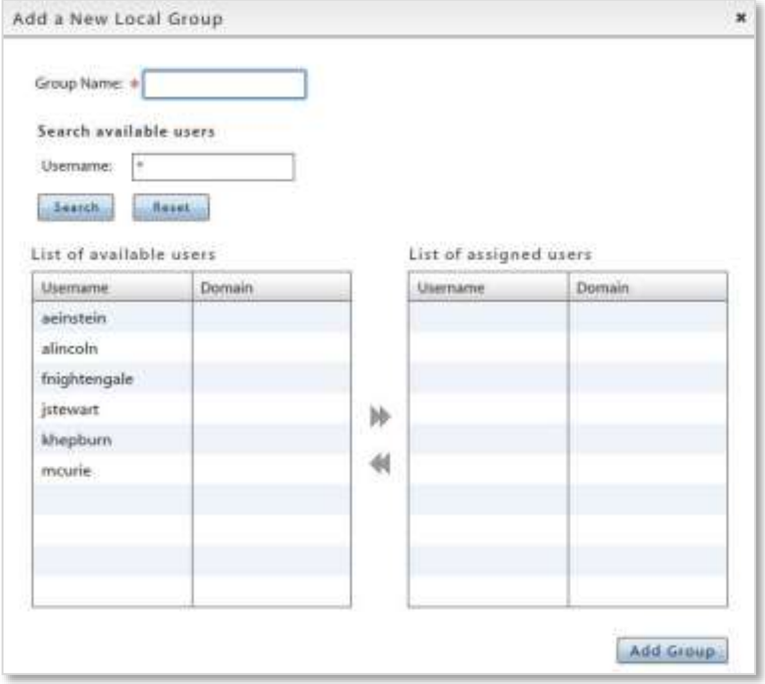
Select a group to make or edit Policy Suite, Connection Schedule, or Liability assignments. Use the arrows to change group priority. Priorities determine settings when a user belongs to more than one groups.

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

Group Name:	Department Heads
Policy Enforcement Type:	Standard
Policy Suite: *	Default
Connection Schedule:	Default
Liability:	○ Unknown ● Corporate ○ Individual
Novell Filr:	Select One...

Add a Group and Assign Users

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



Group Name: *

Search available users

Username: *

List of available users

Username	Domain
aeinstein	
alincoln	
fnightengale	
jstewart	
khepburn	
mcurie	

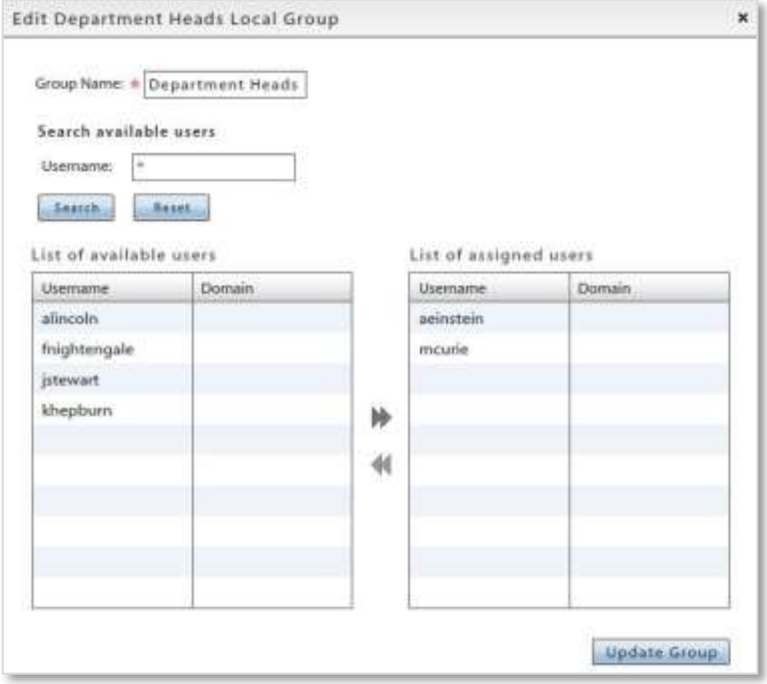
List of assigned users

Username	Domain

Edit a Group Name or Change Group Membership

1. To edit the name of a group or change the members of the group, click the ***Edit Group*** button.
2. Edit the name of the group if necessary or change the group members by using the arrows to move users to/from the available and assigned user columns.
3. Click the ***Update Group*** button.

   Changes to a user's group association will update the user's policy suite, connection schedule, and liability settings accordingly.



Group Name: * Department Heads

Search available users

Username: *

List of available users

Username	Domain
alincoln	
fnightengale	
jstewart	
khepburn	

List of assigned users

Username	Domain
aeinstein	
mcurie	

Prioritizing Groups

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

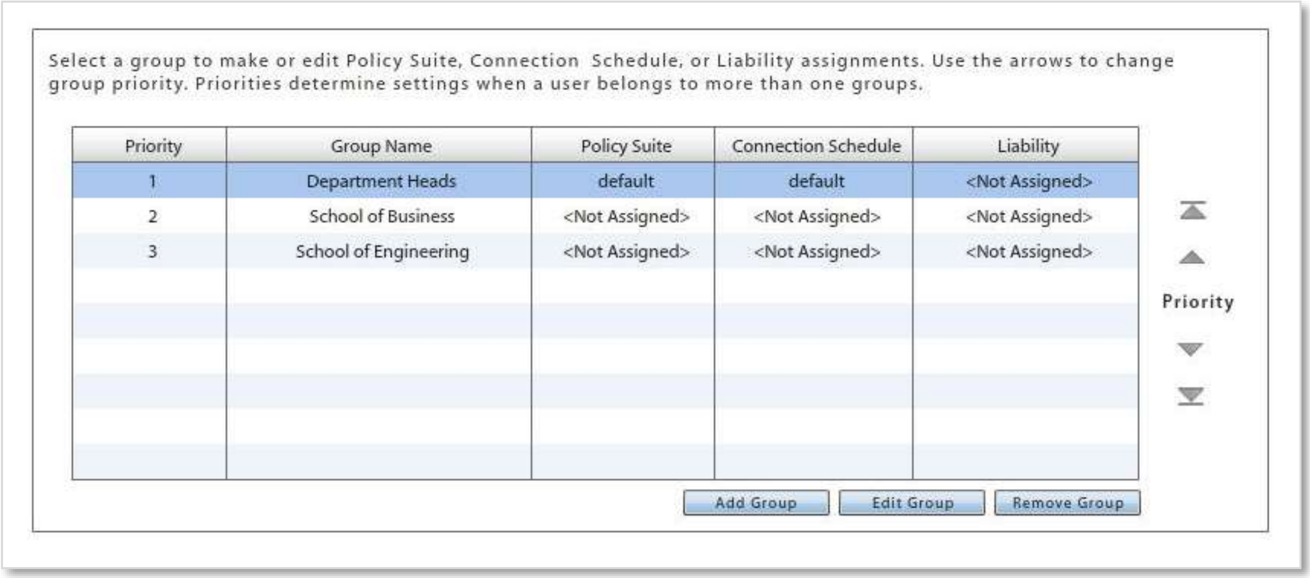
A user's assignments can be pulled from several sources. The sources are consulted in the following order:

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

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

A Prioritization Example

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



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

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

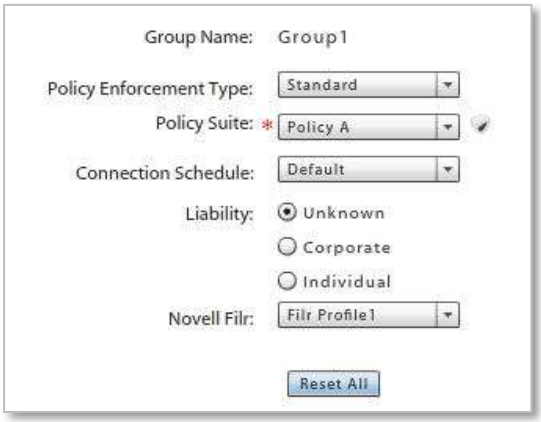
Configure the Group Settings

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

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

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

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



Group Name: Group1

Policy Enforcement Type: Standard

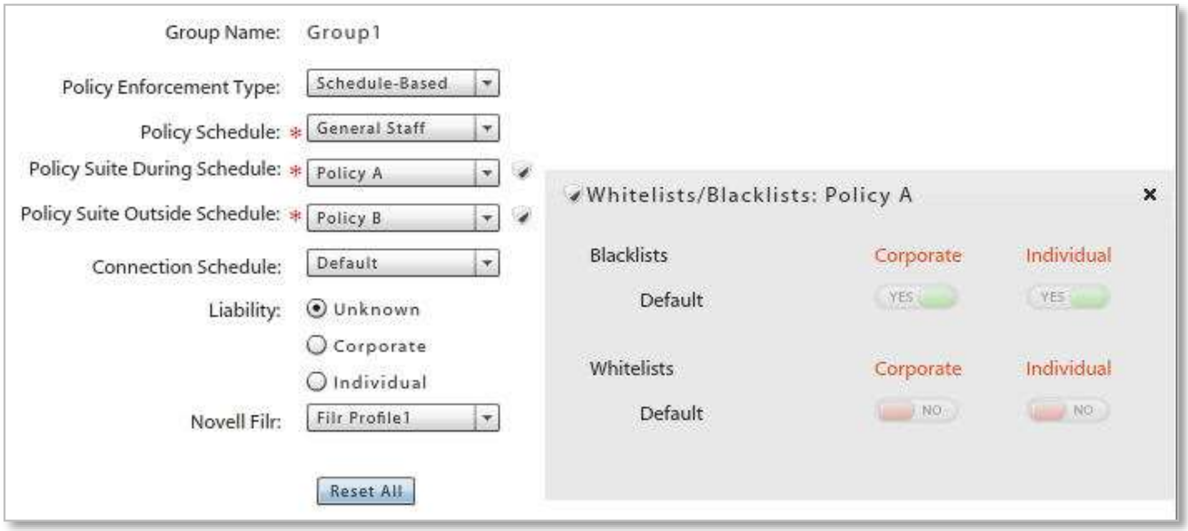
Policy Suite: * Policy A

Connection Schedule: Default

Liability: ● Unknown ○ Corporate ○ Individual

Novell Filr: Filr Profile1

Standard Policy Enforcement



Group Name: Group1

Policy Enforcement Type: Schedule-Based

Policy Schedule: * General Staff

Policy Suite During Schedule: * Policy A

Policy Suite Outside Schedule: * Policy B

Connection Schedule: Default

Liability: ● Unknown ○ Corporate ○ Individual

Novell Filr: Filr Profile1

Whitelists/Blacklists: Policy A ×

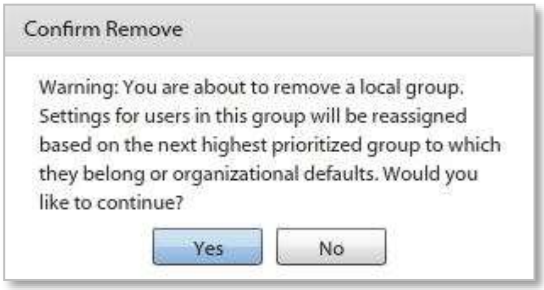
Blacklists	Corporate	Individual
Default	YES	YES

Whitelists	Corporate	Individual
Default	NO	NO

Schedule-Based Policy Enforcement

Remove a Group

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



Confirm Remove

Warning: You are about to remove a local group. Settings for users in this group will be reassigned based on the next highest prioritized group to which they belong or organizational defaults. Would you like to continue?

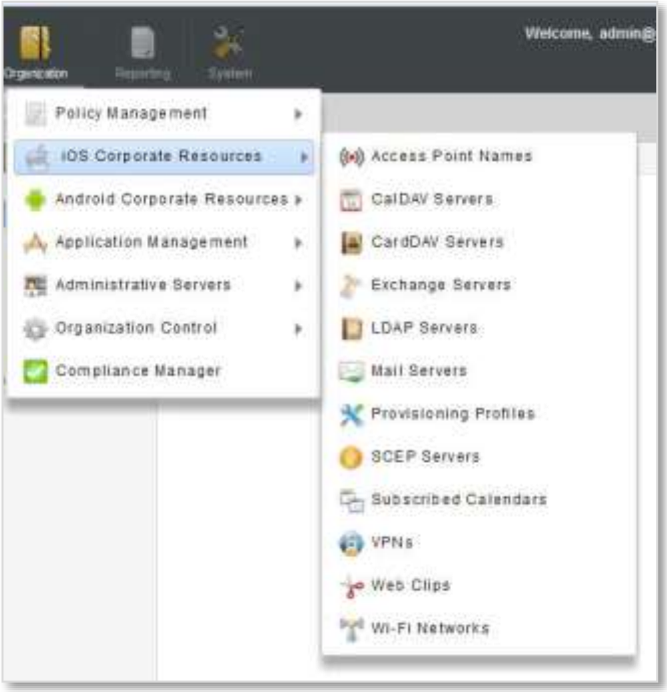
Corporate Resource Management

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

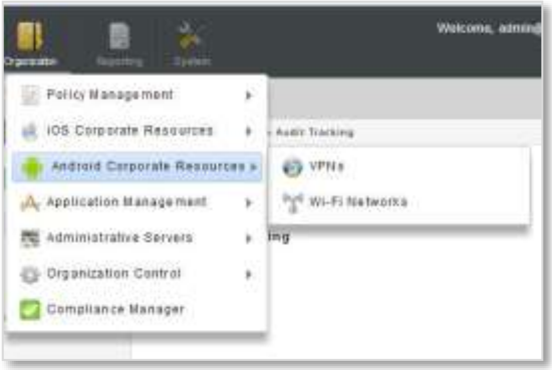
Use the resource tools in the dashboard's ***Organization*** view to define credentials for the server and network resources. Then use the resources in the *User Profile* to associate iOS or Android device users with a resource and configure user account settings to push out to devices.

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



Android Corporate Resources

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

Resource Configurations

You can define the following servers and networks:

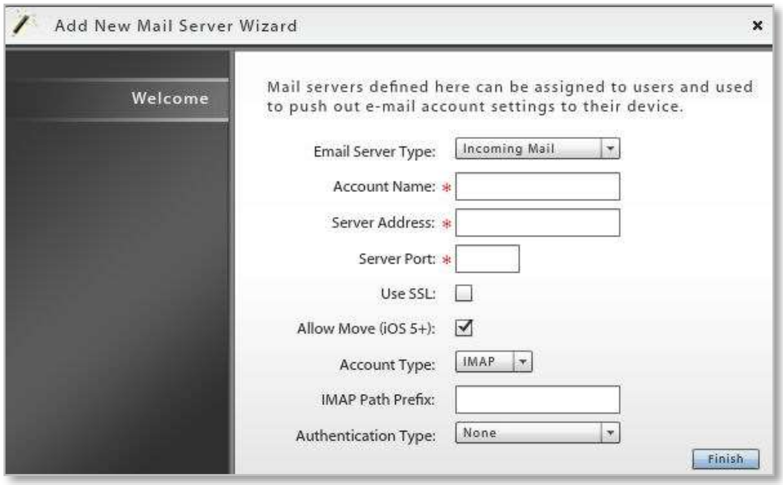
Resource	Description	Devices that Support
Access Point Names (APN)	The Access Point Name identifies the external cellular network a phone accesses for data. When you configure a new APN, you must have the correct settings for the carrier and type of account provisioning. Incorrect settings can result 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
Provisioning Profiles	Define and upload provisioning profiles that enable iOS device users to install in-house iOS apps. You can push out a provisioning profile to individual users or check *Apply to Organization* to assign to all iOS device users in the organization.	iOS
SCEP Servers	Define your Simple Certificate Enrollment Protocol (SCEP) server(s). Then associate a user with a SCEP server in order to issue digital certificates to devices using an automatic enrollment technique. This provides a method of delivering encrypted configuration profiles to iOS devices. See SCEP Servers for more information.	iOS
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 *Managed 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 Control* in the app's settings prior to receiving a VPN assignment from the *ZENworks*	Android (OS 4.0+)

	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 *Managed 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 -Account Type -IMAP Path Prefix -Authentication Type -Expiration (iOS 6+)	-Exchange Server Name -Exchange Server Address -Exchange Port -Use SSL -Use S/MIME -Allow Move -Use Only in Mail -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+)



Add New Mail Server Wizard

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

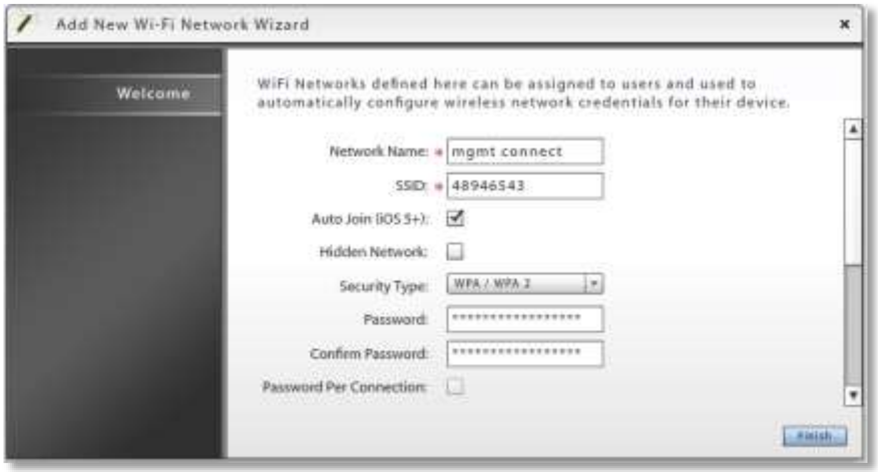
- **Allow Move** – When disabled, this option prevents an iOS device user from moving messages from corporate mail account folders to folders associated with other mailbox accounts. For example, a user could not move a message from the corporate mail account Inbox to a folder associated with his or her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

  This prevents messages created outside of the device's native *Mail* application from being sent from the corporate account. For example, if the user sends a photo from the device *Photo* application, it is not sent from the corporate mail account; nor can the user send an attached contact file from the device's *Contacts* application using the corporate mail account.
- **Allow Recent Address Syncing (iOS 6+)** – When enabled, recently used email addresses are stored on the device. They will then appear in a selection list if the user begins to type the address in a subsequent email.

Configuring Network Settings

The credentials for each network are defined using a wizard.

Wi-Fi Networks (iOS) **-**Resource Name -SSID -Auto Join -Hidden Network -Security Type -Password -Password Per Connection -Accepted EAP Types	-EAP-FAST -Allow Trust Exceptions -Inner Identity -Proxy Type -Proxy Address, Port, Username, Password -Expiration (iOS 6+)	**VPNs (iOS)** *Settings vary based on connection type* **-**Display Name -Connection Type -User Authentication -Remote Address -Proxy Type -Expiration (iOS 6+)	**Wi-Fi Networks (Android)** **-**Resource Name -SSID -BSSID -Hidden Network -Allowed Authentication -Allowed Group Cipher -Allowed Key Management	-Allowed Pairwise Cipher -Allowed Protocol -Pre-Shared Key -WEP Key	**VPNs (Android 4.0+)** *Cisco AnyConnect* or *F5 SSL* **-**Display Name -Connection Type -Remote Address



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: *****************

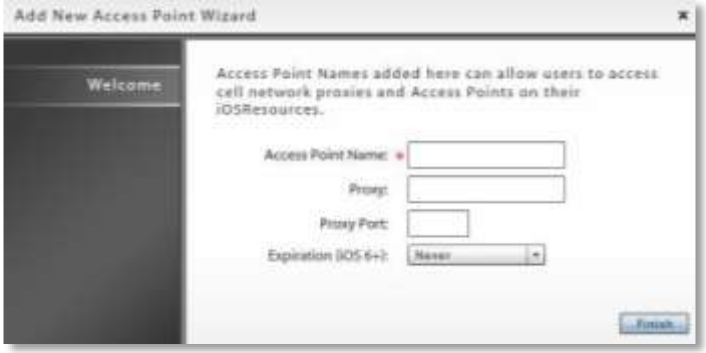
Confirm Password: *****************

Password Per Connection: □

Sample Add New Network Wizard

Configuring Other Resources

Access Point Names	Provisioning Profiles	Subscribed Calendars	Web Clips
-Access Point Name -Proxy -Proxy Port -Expiration (iOS 6+)	-Display Name -Provisioning Profile -Apply to Organization -Expiration (iOS 6+)	-Display Name -Host Name -Use SSL -Expiration (iOS 6+)	-Label -URL -Icon -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.

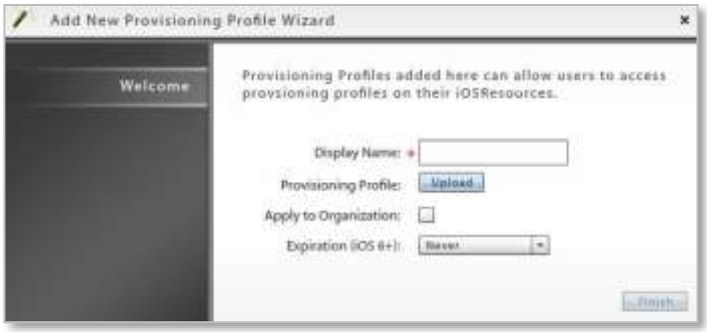
Access Point Name: *

Proxy:

Proxy Port:

Expiration (iOS 6+): Never

Access Point Name Wizard


Add New Provisioning Profile Wizard

Provisioning Profiles added here can allow users to access provsioning profiles on their iOSResources.

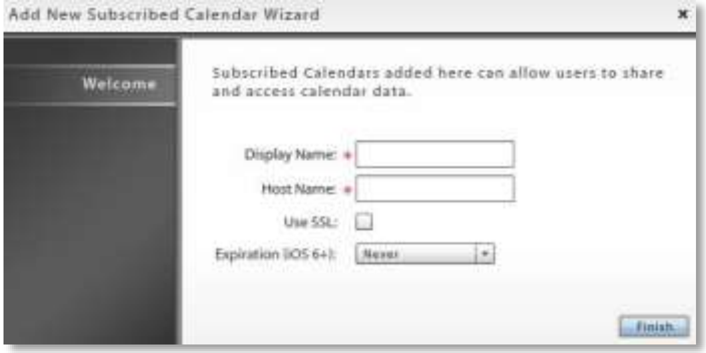
Display Name: *

Provisioning Profile: Upload

Apply to Organization: □

Expiration (iOS 6+): Never

Provisioning Profile


Add New Subscribed Calendar Wizard

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

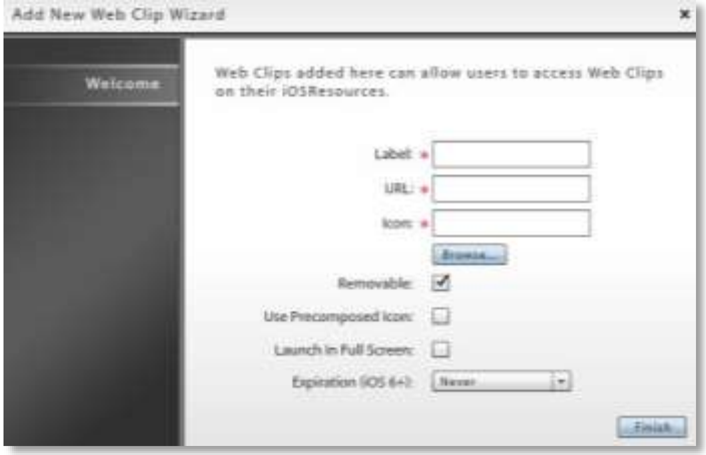
Display Name: *

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: * Browse...

Removable: ☑

Use Precomposed Icon: □

Launch in Full Screen: □

Expiration (iOS 6+): Never

Web Clip Wizard

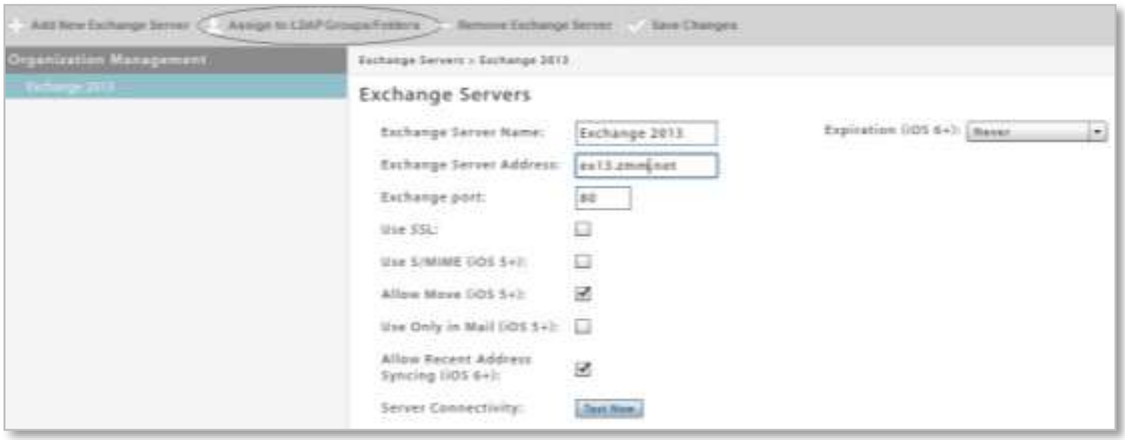
Assigning Resources to LDAP Groups and Folders

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



Exchange Servers

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+): □

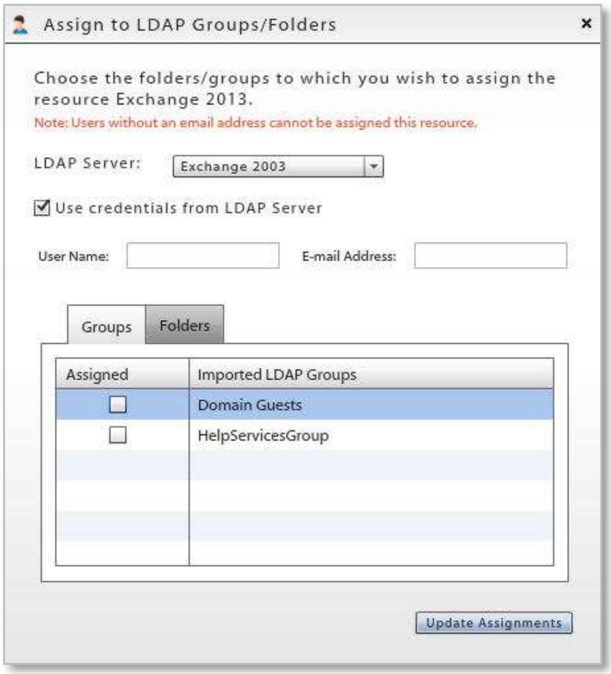
Allow Move (iOS 5+): ☑

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 the option checked to use credentials from LDAP.
    - Disable this option and enter the user authentication token(s) necessary for your Enterprise setup. Acceptable entries may include {domain}, {username}, or {emailaddress} or a combination of tokens such as, {domain}\{username}.
    - Disable this option to assign a resource to a group email address, then enter the shared User Name or shared User Name and Email Address. The assignment is made to that mail account only.
3. Click the *Groups* or *Folders* tab and navigate through the LDAP directory to select the groups 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.

SCEP Servers and the ZENworks Mobile Management System

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

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

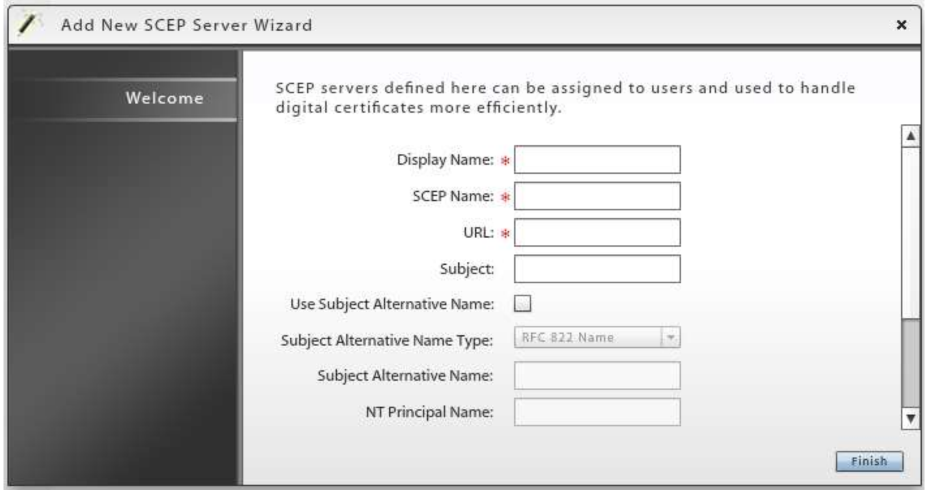
The initial configuration profile that the user accepts contains the address of the SCEP server. The device connects with both the *ZENworks Mobile Management* and SCEP servers to complete several configuration steps:

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

Define a SCEP Server

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

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



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:

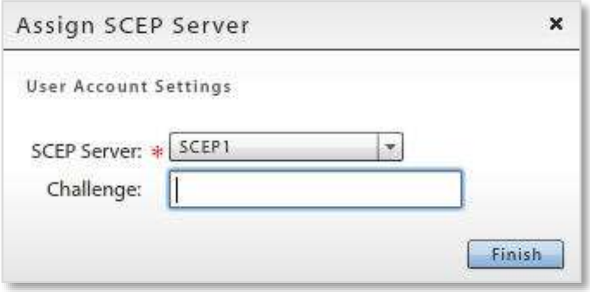
Now, use the *Corporate Resource* option in the **User Profile** to associate users with a SCEP server.

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*.

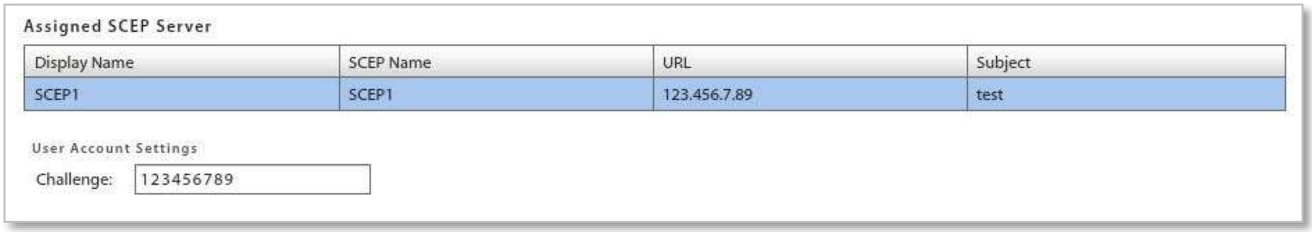
Select a SCEP server for the user from the drop-down list.

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.



SCEP Server: * SCEP1

Challenge:



Display Name	SCEP Name	URL	Subject
SCEP1	SCEP1	123.456.7.89	test

Challenge: 123456789

Application Management

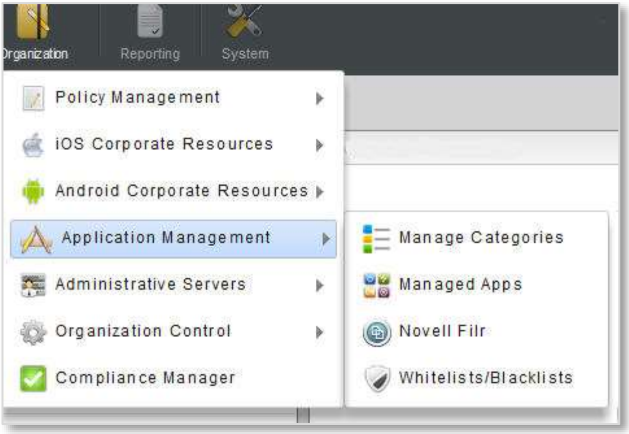
Application Management is located in the *Organization* view of the dashboard.

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

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

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

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



Application Categories

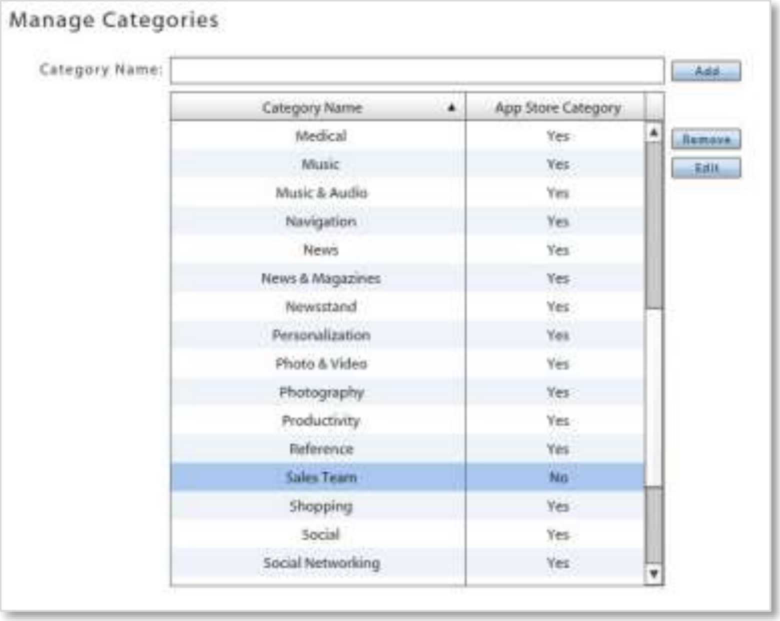
Managed Android and iOS applications can be grouped into categories so that multiple apps can be assigned in bundles to LDAP groups/folders or local groups.

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

Creating, Editing, or Removing Categories

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

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



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

Associating an Application with a Category

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

Choosing a Category for an Android App

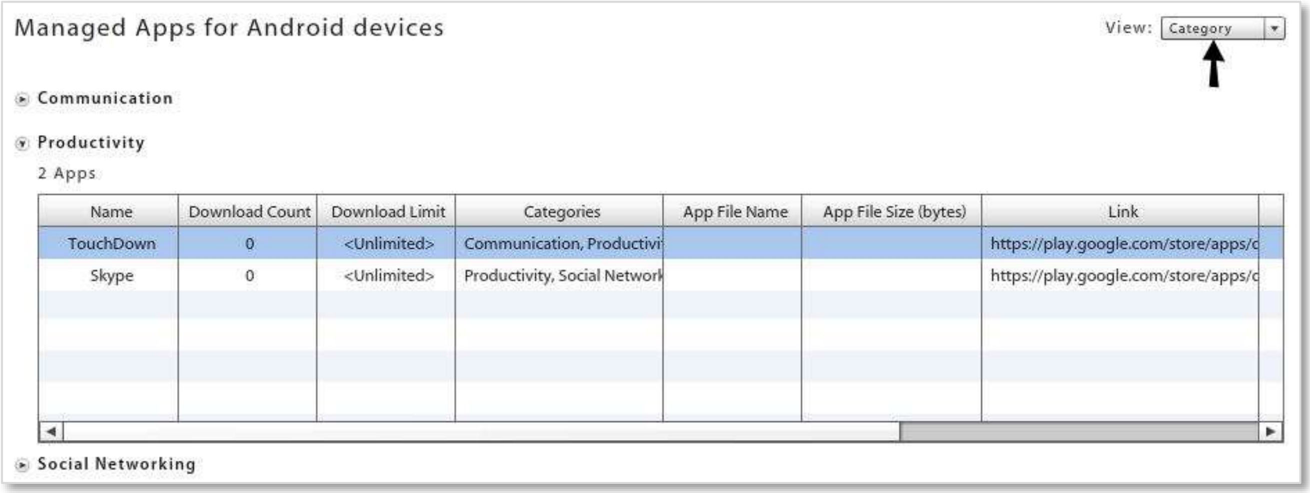
Choosing a Category for an iOS App

View Managed Apps by Category

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

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

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



Managed Apps for Android devices

View: Category

Communication

Productivity

2 Apps

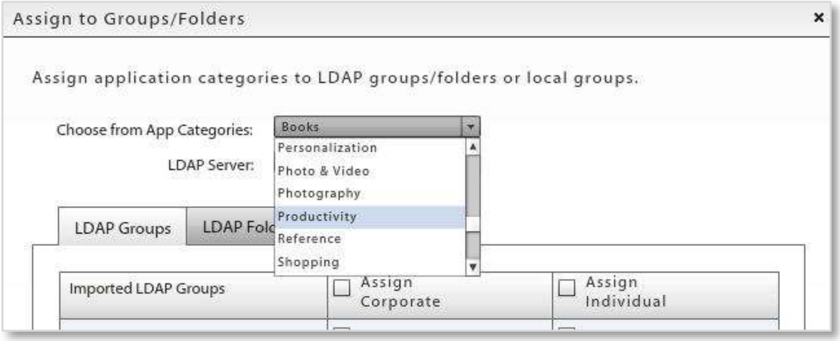
Name	Download Count	Download Limit	Categories	App File Name	App File Size (bytes)	Link
TouchDown	0	<Unlimited>	Communication, Productivi			https://play.google.com/store/apps/c
Skype	0	<Unlimited>	Productivity, Social Networ			https://play.google.com/store/apps/c

Social Networking

Assigning a Category to LDAP Groups/Folders or Local Groups

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

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



Assign to Groups/Folders

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

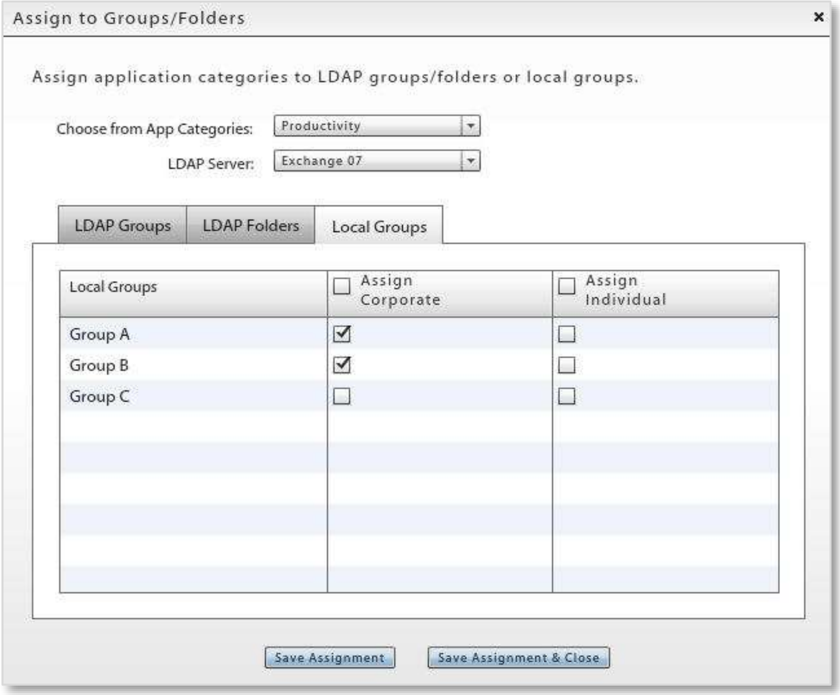
Choose from App Categories: Books

LDAP Server:

Imported LDAP Groups	☐ Assign Corporate	☐ Assign Individual

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

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



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

Choose from App Categories: Productivity

LDAP Server: Exchange 07

Local Groups	□ Assign Corporate	□ Assign Individual
Group A	☑	□
Group B	☑	□
Group C	□	□

7. In the group list, locate the group to which you are assigning the category and mark the check box.

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

8. Click **Save Assignment** before you assign another category.
   Click **Save Assignment & Close** when you are finished.

Managed Apps

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

When an administrator creates an app list for each supported device platform and enables the *Managed App Permissions* in the policy suite, users with that policy suite can access the recommended applications from the *ZENworks Mobile Management* device agent. For Android and iOS users, managed apps can also be made available to users via the LDAP group/folder or local group to which they belong.

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

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

If Managed Apps are accessed by users in different countries or regions, see this Knowledge Base article.

Accessing Managed Apps on a Device

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

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

In this section you will find information on:

- Enabling Managed App Permissions
- Adding and Managing Apps for Android Devices
- Kiosk Mode Apps
- Adding and Managing Apps for iOS Devices
- Adding Managed Apps for BlackBerry Devices

Enabling Managed App Permissions

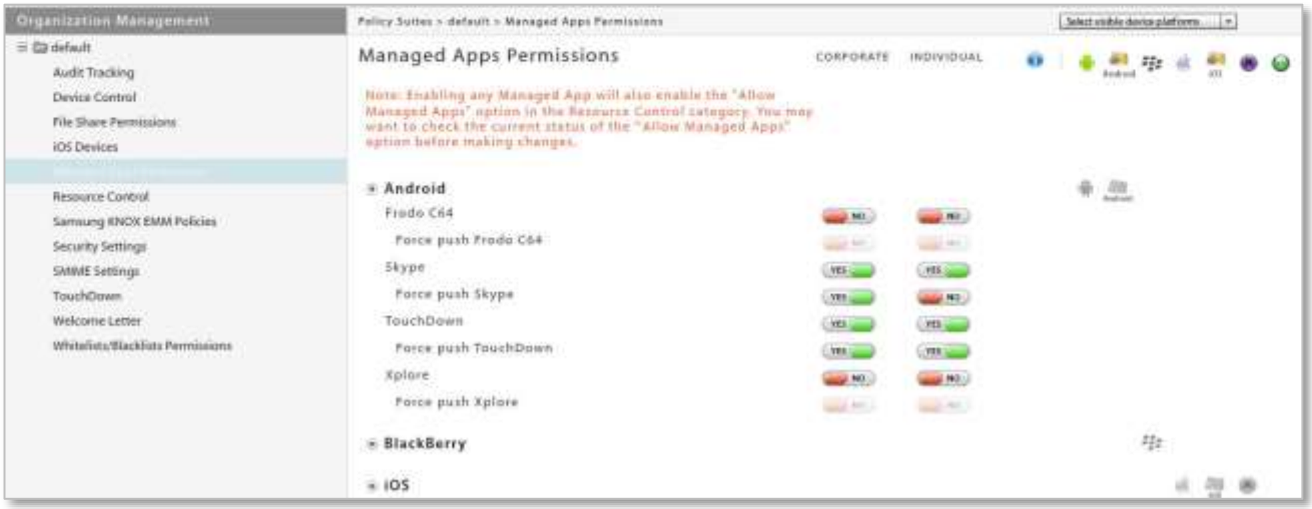
Applications on the Managed Apps list are not available to users until you enable the ***Managed App Permissions*** in the policy suites for each app on the list.

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

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

   Enable the ***Force Push*** option, for Android or iOS apps, to set the app to automatically prompt users associated with the policy suite to install the app. This makes it a required app.

2. Click the ***Save Changes*** button.



Organization Management

- default
  - Audit Tracking
  - Device Control
  - File Share Permissions
  - iOS Devices
  - Resource Control
  - Samsung KNOX EMM Policies
  - Security Settings
  - SMIME Settings
  - TouchDown
  - Welcome Letter
  - Whitelists/Blacklists Permissions

Policy Suites > default > Managed Apps Permissions

Select visible device platforms

Managed Apps Permissions

Note: Enabling any Managed App will also enable the "Allow Managed Apps" option in the Resource Control category. You may want to check the current status of the "Allow Managed Apps" option before making changes.

Android

	CORPORATE	INDIVIDUAL
Frodo C64	NO	NO
Force push Frodo C64	NO	NO
Skype	YES	YES
Force push Skype	YES	NO
TouchDown	YES	YES
Force push TouchDown	YES	YES
Xplore	NO	NO
Force push Xplore	NO	NO

BlackBerry

iOS

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

   These policies should be enabled:

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

Adding and Managing Apps for Android Devices

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

Management functionality includes:

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

In this section:

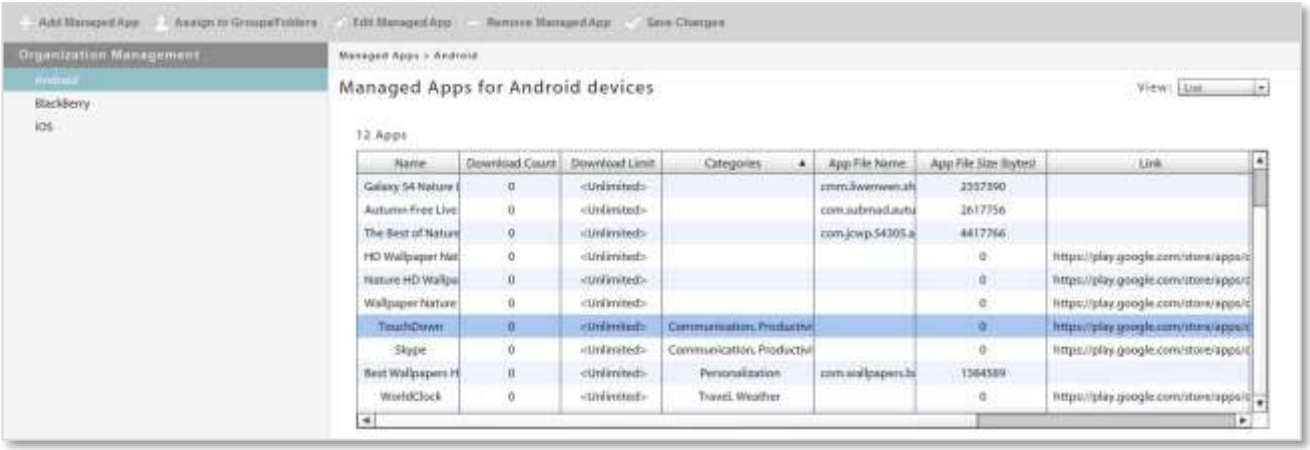
Managed App Permissions for Android

Adding Google Play Store Apps

Adding an Android Enterprise App

Updating Android App Versions

Android Kiosk Mode Apps



Managed Apps for Android devices

12 Apps

Name	Download Count	Download Limit	Categories ▲	App File Name	App File Size (bytes)	Link
Galaxy S4 Nature (	0	<Unlimited>		com.liwenwen.sh	2357390	
Autumn Free Live	0	<Unlimited>		com.subrnad.autu	2617756	
The Best of Nature	0	<Unlimited>		com.jcwp.S4305.a	4417766	
HD Wallpaper Nat	0	<Unlimited>			0	https://play.google.com/store/apps/c
Nature HD Wallpa	0	<Unlimited>			0	https://play.google.com/store/apps/c
Wallpaper Nature	0	<Unlimited>			0	https://play.google.com/store/apps/c
TouchDown	0	<Unlimited>	Communication, Productivi		0	https://play.google.com/store/apps/c
Skype	0	<Unlimited>	Communication, Productivi		0	https://play.google.com/store/apps/c
Best Wallpapers H	0	<Unlimited>	Personalization	com.wallpapers.b	1384589	
WorldClock	0	<Unlimited>	Travel, Weather		0	https://play.google.com/store/apps/c

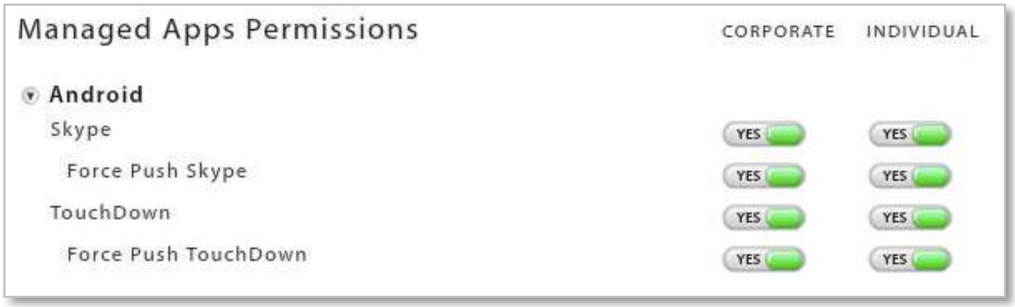
Managed App Permissions for Android

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

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

1. Choose the policy suite category ***Audit Tracking*** and verify that the following option is enabled:
   - ***Record managed applications*** – required for *Force Push* and administrator-initiated app installations.
2. Choose the policy suite category ***Managed 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.



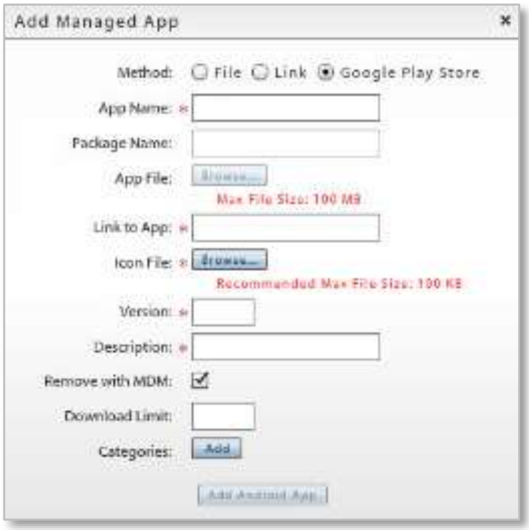
Managed Apps Permissions

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

Enabling Force Push for required apps

Adding Google Play Store Apps

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



Add Managed 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: ☑

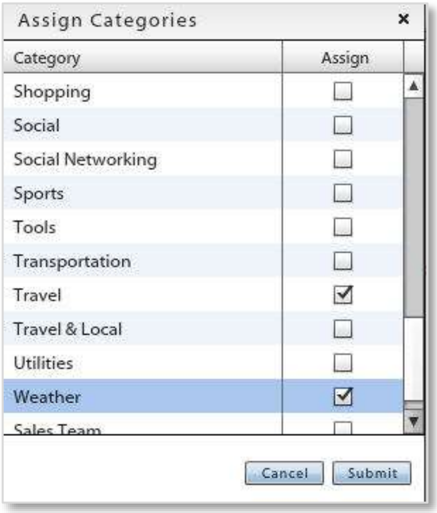
Download Limit:

Categories: Add

Add Android App

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

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



Assign Categories ×

Category	Assign
Shopping	□
Social	□
Social Networking	□
Sports	□
Tools	□
Transportation	□
Travel	☑
Travel & Local	□
Utilities	□
Weather	☑
Sales Team	□

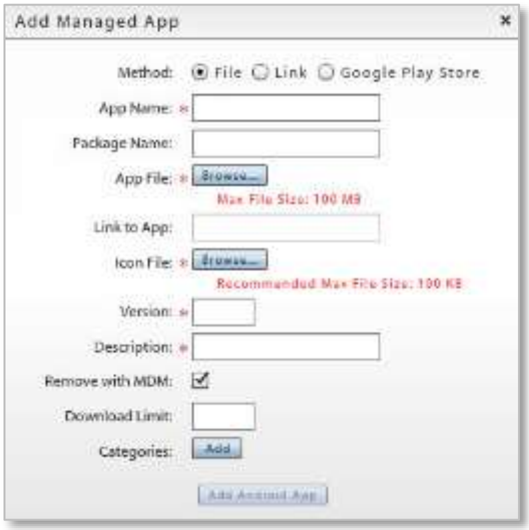
Cancel Submit

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

Adding an Android Enterprise App

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

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



Add Managed App

Method: ● File ○ Link ○ Google Play Store

Remove with MDM: ☑

3. Choose *File* or *Link* as the ***Method*** to add the app. Apps can be added as a link to the download page where the user can obtain the app, or as an actual app file that the user can install.
4. Enter the ***App Name***, ***Version***, and ***Description*** for the app. What you enter displays on the device.
5. For *Links*, provide a URL for the application in the ***Link to App*** field.

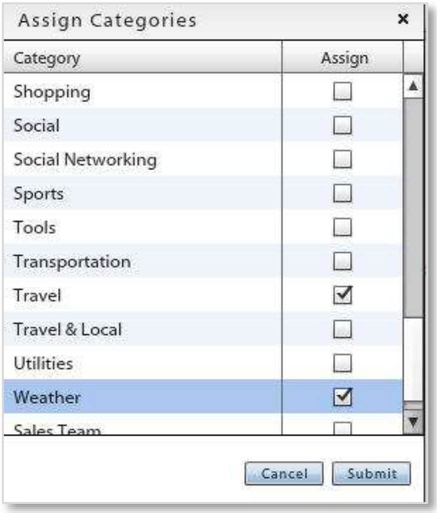
   For *Files*, browse to select an .apk file at the ***App File*** field.
6. Enter the ***Package Name*** for the app. This is the unique identifier associated with the app. It must be accurate. For the ***Novell Filr*** app, enter: com.novell.filr.android

   Note: When Force Push is on, *ZENworks Mobile Management* uses this to verify whether the app is installed on the device. If entered incorrectly, it will try to verify by comparing the value in the *App Name* field with the actual application name sent from the device. If Force Push fails to verify that the app is installed, the user will be continually prompted to install.
7. Browse your image files at the ***Icon File*** field and select an icon to associate with the application.
8. Select ***Remove With MDM*** if you want the app to be deleted from the device when the MDM configuration profile is removed.
9. Enter the ***Download Limit*** if you want to track downloads of a managed app purchased in bulk. Users can no longer download the app once the limit has been reached.

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

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

11. Click ***Add Android App*** to add the App to the Android Managed App list.

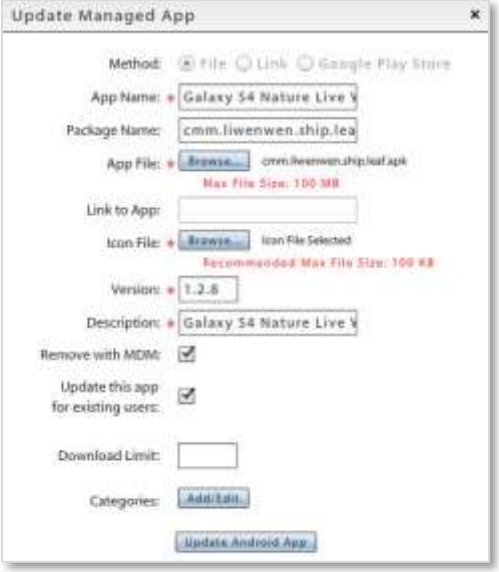


Assign Categories ×

Category	Assign
Shopping	☐
Social	☐
Social Networking	☐
Sports	☐
Tools	☐
Transportation	☐
Travel	☑
Travel & Local	☐
Utilities	☐
Weather	☑
Sales Team	☐

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.



Update Managed App ×

Method: ● File ○ Link ○ Google Play Store

App Name: * Galaxy S4 Nature Live W

Package Name: cmm.liwenwen.ship.lea

App File: * Browse... cmm.liwenwen.ship.leaf.apk

Max File Size: 100 MB

Link to App:

Icon File: * Browse... Icon File Selected

Recommended Max File Size: 100 KB

Version: * 1.2.8

Description: * Galaxy S4 Nature Live W

Remove with MDM: ☑

Update this app for existing users: ☑

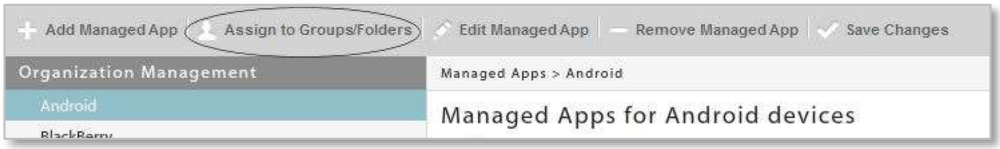
Download Limit:

Categories: Add/Edit

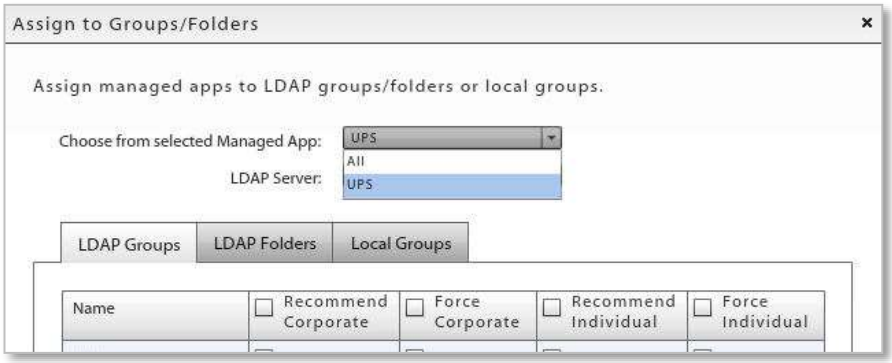
Assigning Android Apps to LDAP Groups/Folders or Local Groups

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

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



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

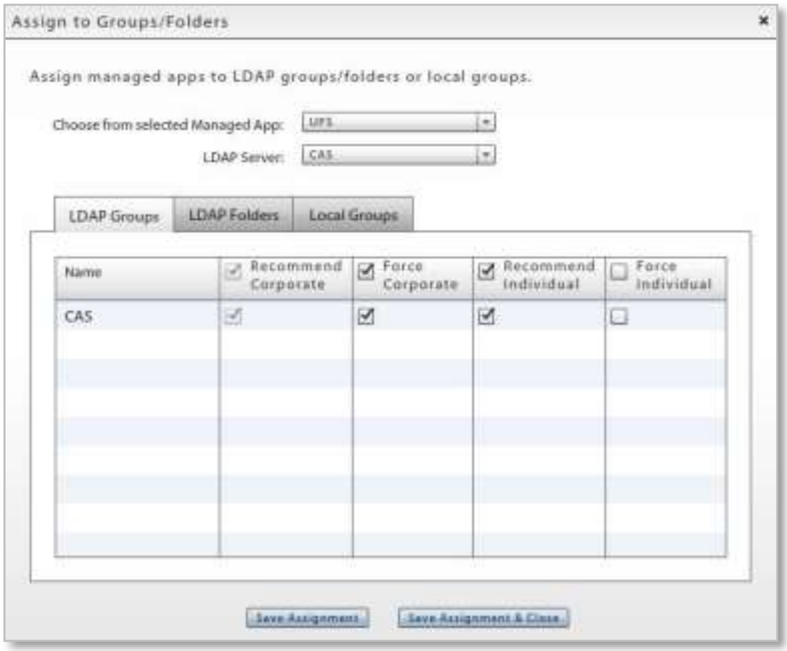


Choose from selected Managed App: UPS

LDAP Server:

Name	□ Recommend Corporate	□ Force Corporate	□ Recommend Individual	□ Force Individual

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



Choose from selected Managed App: UPS

LDAP Server: CAS

Name	☑ Recommend Corporate	☑ Force Corporate	☑ Recommend Individual	□ Force Individual
CAS	☑	☑	☑	□

6. In the group list, locate the group to which you are assigning the app(s) and determine whether or not the app(s) will be required on user devices.

   - Check the ***Recommend*** box to make the app(s) available to users in this group.

     Or check the *Recommend* box in the header to make the app(s) available to users in all groups.

   - Check the ***Force*** box to force push the app(s) to devices. Users will be required to install the app(s). Checking this box will automatically mark the *Recommend* box as well.

     Or check the *Force* box in the header to force push the app(s) to devices of all groups.

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

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

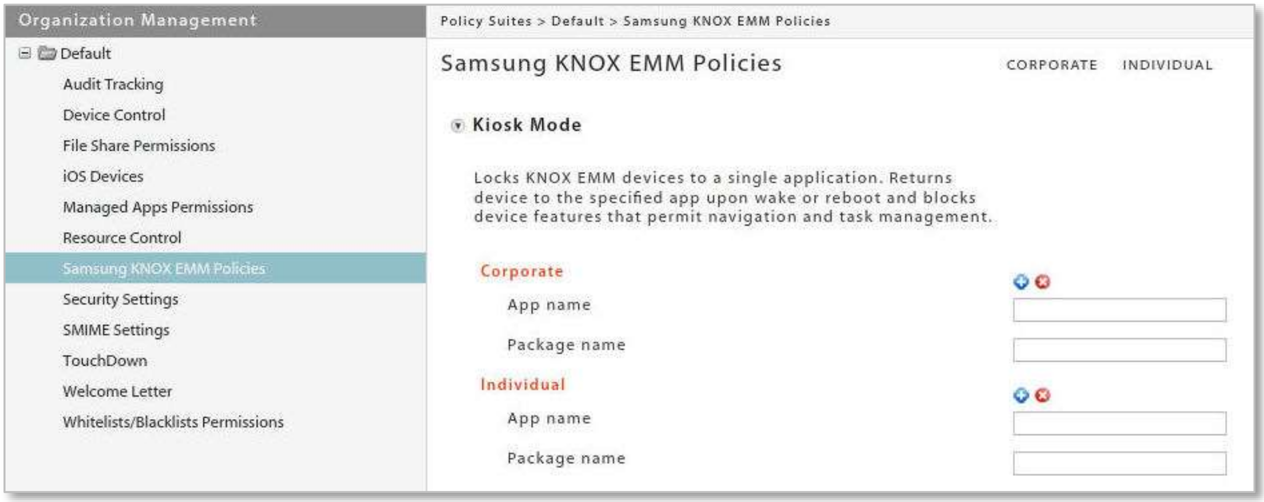
Android Kiosk Mode Apps

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

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

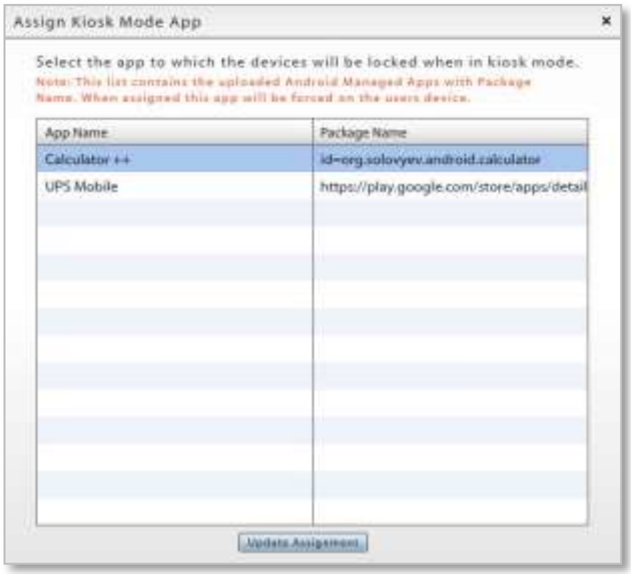
To Define a Kiosk Mode App

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



Locks KNOX EMM devices to a single application. Returns device to the specified app upon wake or reboot and blocks device features that permit navigation and task management.

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

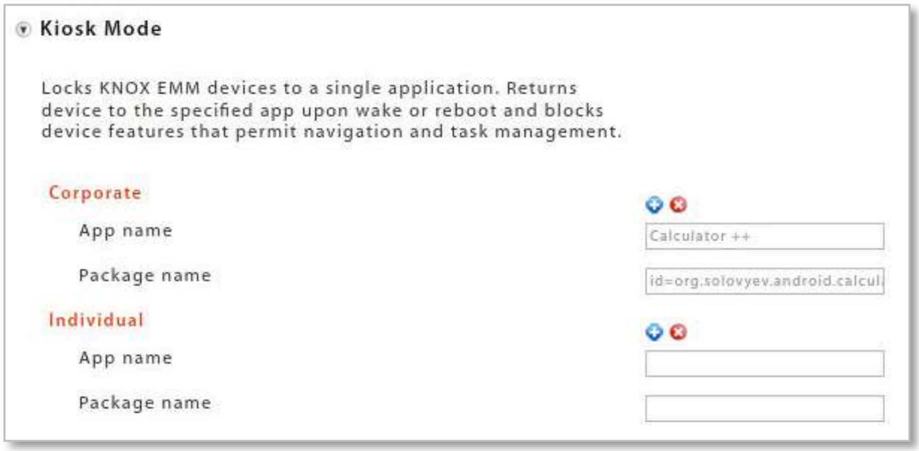


Assign Kiosk Mode App

Select the app to which the devices will be locked when in kiosk mode.
Note: This list contains the uploaded Android Managed Apps with Package Name. When assigned this app will be forced on the users device.

App Name	Package Name
Calculator ++	id=org.solovyev.android.calculator
UPS Mobile	https://play.google.com/store/apps/detail

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



Kiosk Mode

Locks KNOX EMM devices to a single application. Returns device to the specified app upon wake or reboot and blocks device features that permit navigation and task management.

Corporate

App name: Calculator ++

Package name: id=org.solovyev.android.calcul

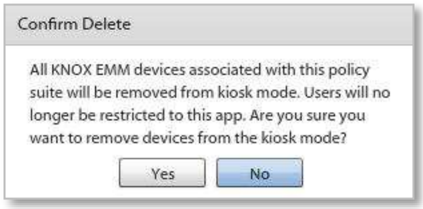
Individual

App name:

Package name:

To Remove the Kiosk Mode App

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



Confirm Delete

All KNOX EMM devices associated with this policy suite will be removed from kiosk mode. Users will no longer be restricted to this app. Are you sure you want to remove devices from the kiosk mode?

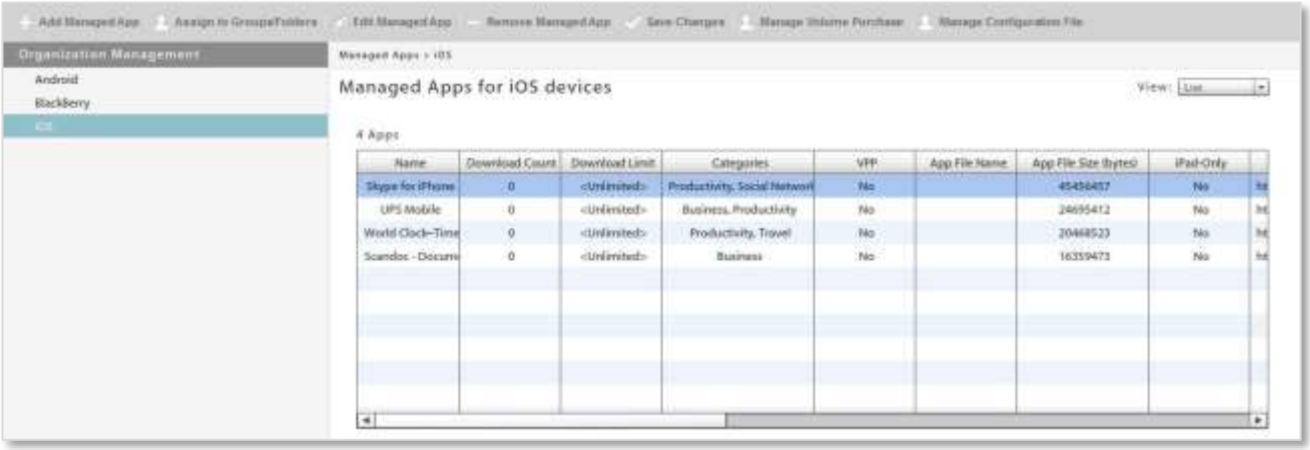
Adding and Managing Apps for iOS Devices

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

Management functionality includes:

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

In this section:



Managed Apps for iOS devices

4 Apps

Name	Download Count	Download Limit	Categories	VPP	App File Name	App File Size (bytes)	iPad-Only	
Skype for iPhone	0	<Unlimited>	Productivity, Social Networ	No		45456457	No	ht
UPS Mobile	0	<Unlimited>	Business, Productivity	No		24695412	No	ht
World Clock–Time	0	<Unlimited>	Productivity, Travel	No		20468523	No	ht
Scandoc - Docum	0	<Unlimited>	Business	No		16359473	No	ht

Managed App Permissions for iOS

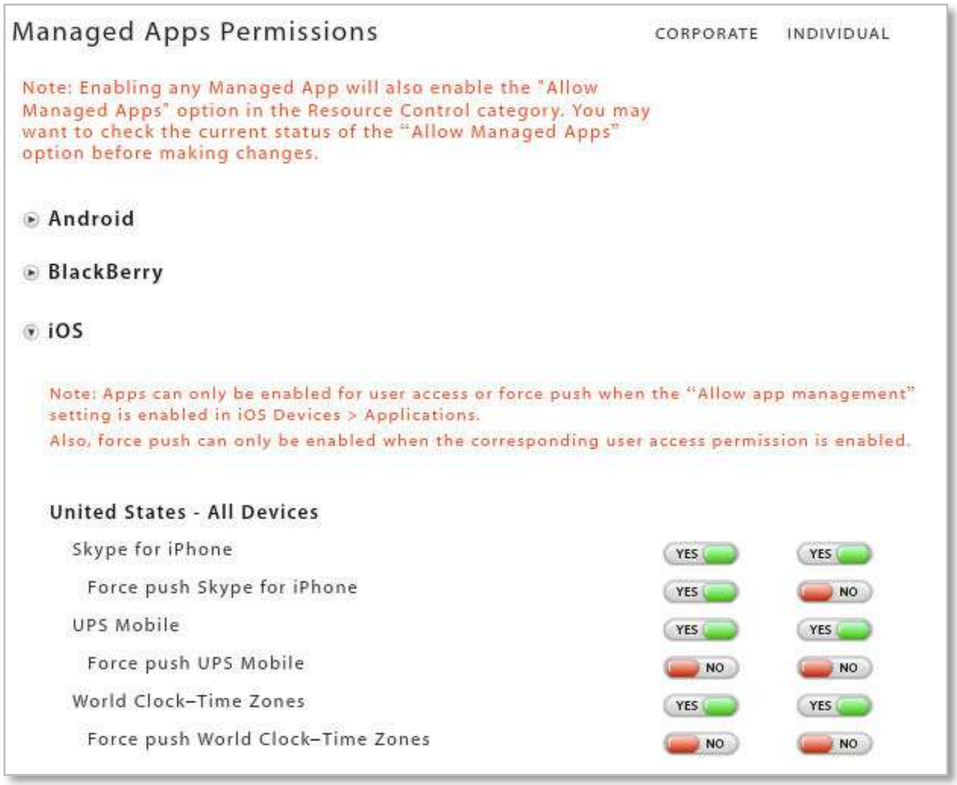
Several policy suite rules must be enabled for Managed App functionality.

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

1. Choose the policy suite category ***iOS Devices*** > ***Applications*** and enable the following option:
    - ***Allow app management*** – Required for Force Push and administrator initiated app installations.

- ***Allow application installation*** – Required for Force Push and administrator initiated app installations.
- ***Allow iTunes*** – Required for Force Push and administrator initiated App Store app installations.

2. If you want to use a Configuration File to configure a third party iOS application, verify that the following policy is enabled
   Select ***Organization Management*** > ***Policy Management*** > ***Policy Suites*** > (*select policy suite)* > ***iOS Devices*** > ***Management***. Enable:
   - ***Allow Management of Settings***
3. Choose policy suite category ***Managed App Permissions*** > ***iOS***. For each mobile app listed under the iOS platform:
   - Enable the app to make it available to users associated with the policy suite.
   - 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.



Managed Apps Permissions

Note: Enabling any Managed App will also enable the "Allow Managed Apps" option in the Resource Control category. You may want to check the current status of the "Allow Managed Apps" option before making changes.

Note: Apps can only be enabled for user access or force push when the "Allow app management" setting is enabled in iOS Devices > Applications.
Also, force push can only be enabled when the corresponding user access permission is enabled.

United States - All Devices	CORPORATE	INDIVIDUAL
Skype for iPhone	YES	YES
Force push Skype for iPhone	YES	NO
UPS Mobile	YES	YES
Force push UPS Mobile	NO	NO
World Clock–Time Zones	YES	YES
Force push World Clock–Time Zones	NO	NO

Enabling Force Push for Required Apps

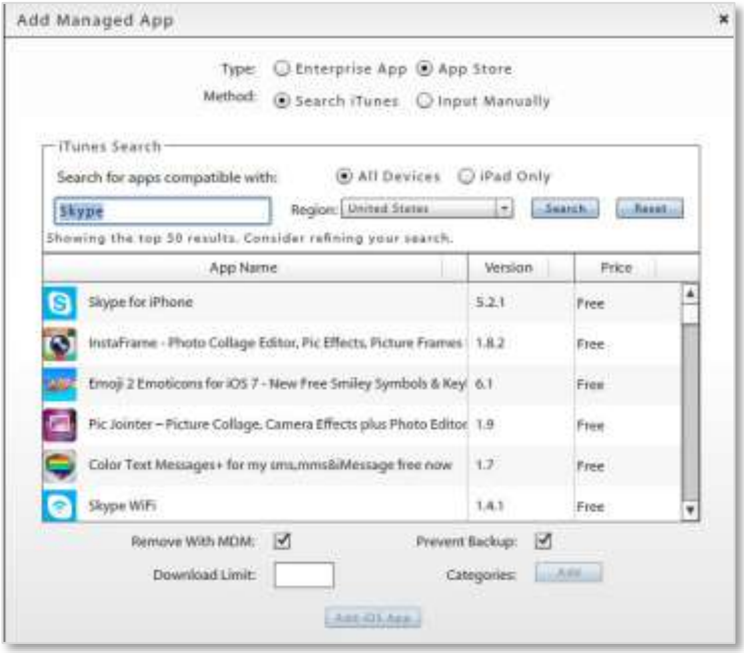
Adding iOS App Store Apps

If Managed Apps are accessed by users in different countries or regions, read this Knowledge Base article.

1. Select ***Organization*** > ***Application Management*** > ***Managed Apps***.
2. Select ***iOS*** from the left panel, then click ***Add Managed App***.
3. Choose ***App Store*** as the Mobile app *Type*.

4. Choose ***Search iTunes*** or ***Input Manually*** as the *Method* by which to add the app.

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



Add Managed App ×

Type: ○ Enterprise App ● App Store

Method: ● Search iTunes ○ Input Manually

iTunes Search

Search for apps compatible with: ● All Devices ○ iPad Only

Skype Region: United States Search Reset

Showing the top 50 results. Consider refining your search.

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

Remove With MDM: ☑ Prevent Backup: ☑

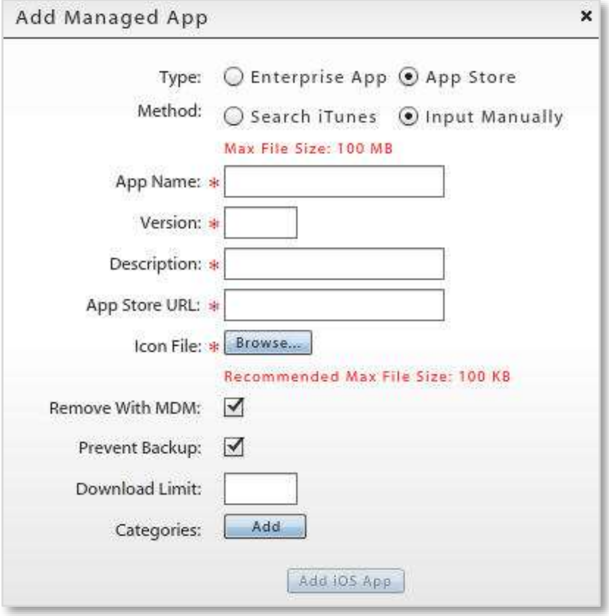
Download Limit: Categories: Add

Add iOS App

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

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

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



Add Managed App ×

Type: ○ Enterprise App ● App Store

Method: ○ Search iTunes ● Input Manually

Max File Size: 100 MB

App Name: *

Version: *

Description: *

App Store URL: *

Icon File: * Browse...

Recommended Max File Size: 100 KB

Remove With MDM: ☑

Prevent Backup: ☑

Download Limit:

Categories: Add

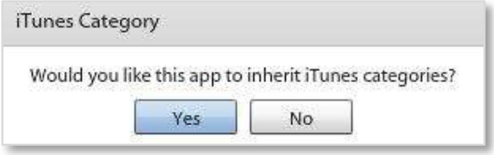
Add iOS App

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

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

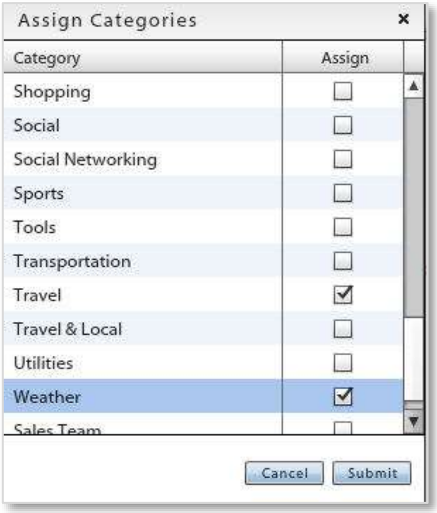
8. If you want to assign the app to an application category, click the ***Add*** button next to the ***Categories*** field.

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



iTunes Category

Would you like this app to inherit iTunes categories?



Assign Categories

Category	Assign
Shopping	☐
Social	☐
Social Networking	☐
Sports	☐
Tools	☐
Transportation	☐
Travel	☑
Travel & Local	☐
Utilities	☐
Weather	☑
Sales Team	☐

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

Adding an iOS Enterprise App

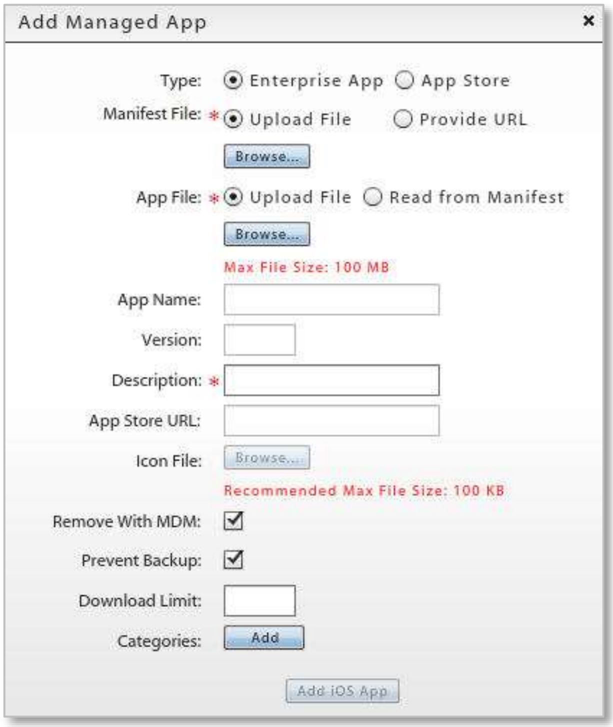
An enterprise (or in-house) app is one that has been created by an organization by using development tools available through the Apple Developer Enterprise Program (iDEP).

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

Location of the Enterprise App	Manifest File Field	App File Field	Other Required Fields
Manifest and app files are on the *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.
8. Enter the ***Download Limit*** if you want to track downloads of a managed app purchased in bulk. Users can no longer download the app once the limit has been reached.

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



Add Managed App ×

Type: ● Enterprise App ○ App Store

Manifest File: * ● Upload File ○ Provide URL

Browse...

App File: * ● Upload File ○ Read from Manifest

Browse...

Max File Size: 100 MB

App Name:

Version:

Description: *

App Store URL:

Icon File: Browse...

Recommended Max File Size: 100 KB

Remove With MDM: ☑

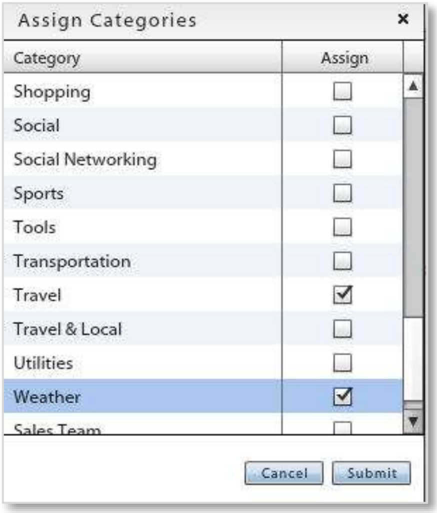
Prevent Backup: ☑

Download Limit:

Categories: Add

Add iOS App

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



Assign Categories ×

Category	Assign
Shopping	□
Social	□
Social Networking	□
Sports	□
Tools	□
Transportation	□
Travel	☑
Travel & Local	□
Utilities	□
Weather	☑
Sales Team	□

Cancel Submit

Configuration File Management

Format

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

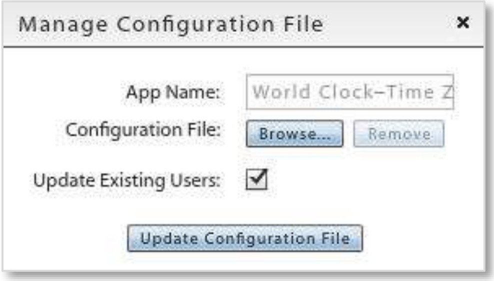
```
          General Format                              Example
<dict>                                        <dict>
        <key>key1</key>                               <key>username</key>
        <string>value1</string>                      <string>username</string>
        <key>key2</key>     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

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

Applying the Configuration File

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

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



Manage Configuration File

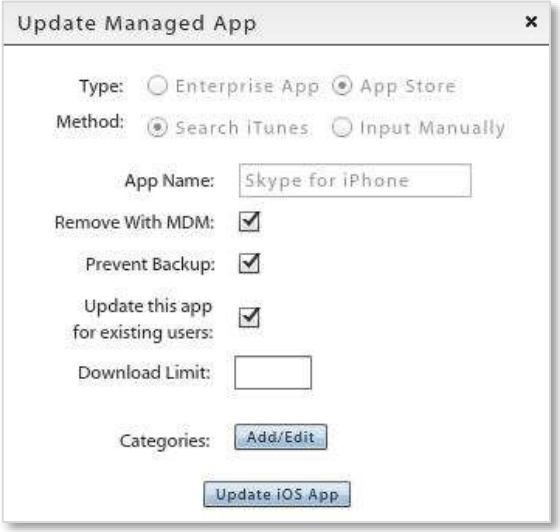
App Name: World Clock–Time Z

Configuration File:

Update Existing Users: ☑

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.



Update Managed App

Type: ○ Enterprise App ● App Store

Method: ● Search iTunes ○ Input Manually

App Name: Skype for iPhone

Remove With MDM: ☑

Prevent Backup: ☑

Update this app for existing users: ☑

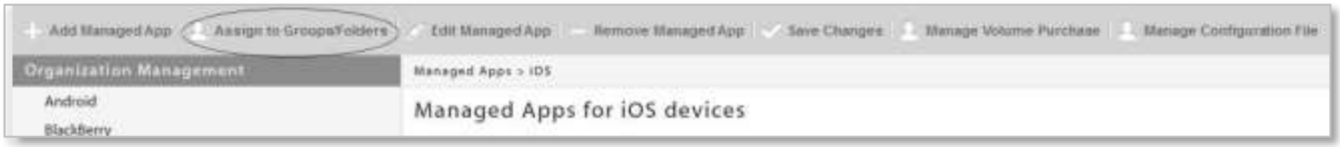
Download Limit:

Categories:

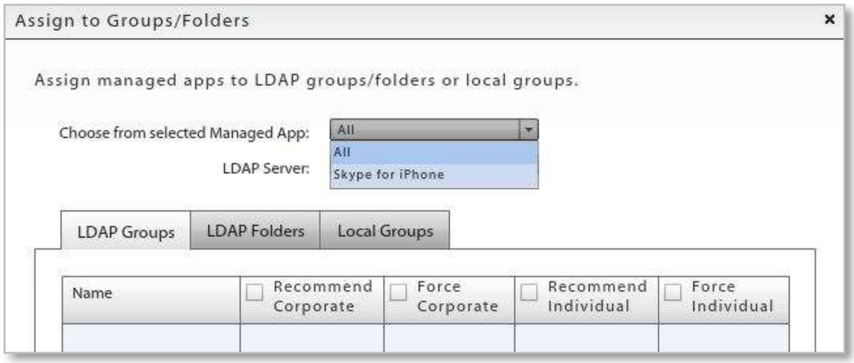
Assigning iOS Apps to LDAP Groups/Folders or Local Groups

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

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



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


Assign to Groups/Folders ×

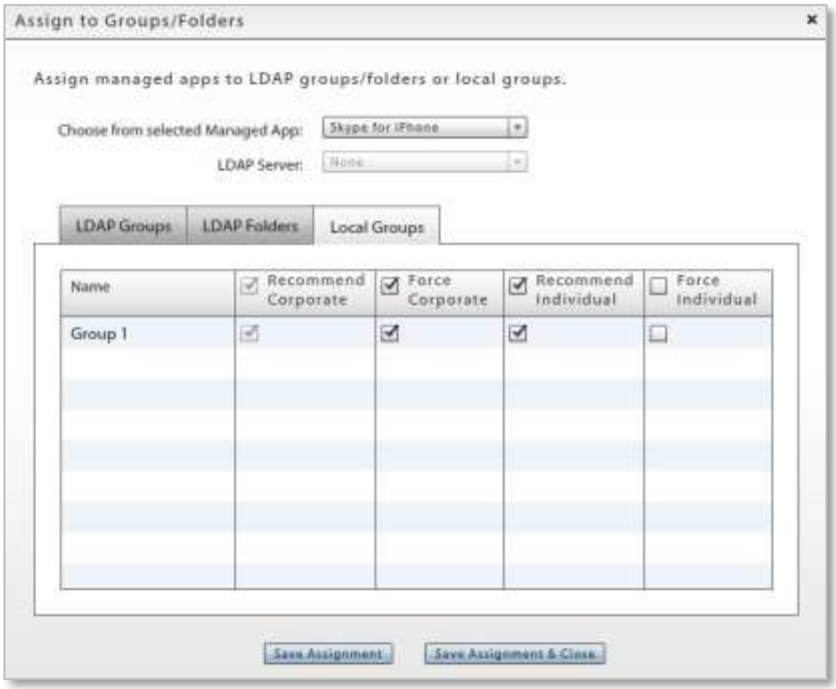
Assign managed apps to LDAP groups/folders or local groups.

Choose from selected Managed App: All

LDAP Server:

Name	☐ Recommend Corporate	☐ Force Corporate	☐ Recommend Individual	☐ Force Individual

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


Assign to Groups/Folders ×

Assign managed apps to LDAP groups/folders or local groups.

Choose from selected Managed App: Skype for iPhone

LDAP Server: None

Name	☑ Recommend Corporate	☑ Force Corporate	☑ Recommend Individual	☐ Force Individual
Group 1	☑	☑	☑	☐

6. In the group list, locate the group to which you are assigning the app(s) and determine whether or not the app(s) will be required on user devices.

    - Check the ***Recommend*** box to make the app(s) available to users in this group.

      Or check the *Recommend* box in the header to make the app(s) available to users in all groups.

    - Check the ***Force*** box to force push the app(s) to devices. Users will be required to install the app(s). Checking this box will automatically mark the *Recommend* box as well.

      Or check the *Force* box in the header to force push the app(s) to devices of all groups.

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

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

Managing Volume Purchase Program Licenses

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

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

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

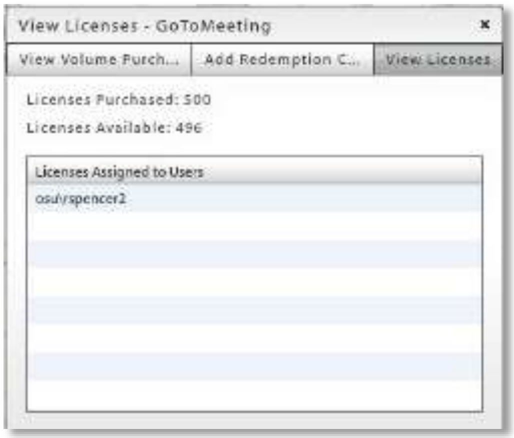
To View VPP License Counts:

1. Select the app and click ***Manage Volume Purchase***.

2. Select the ***View Licenses*** tab.

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

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



Licenses Purchased: 500

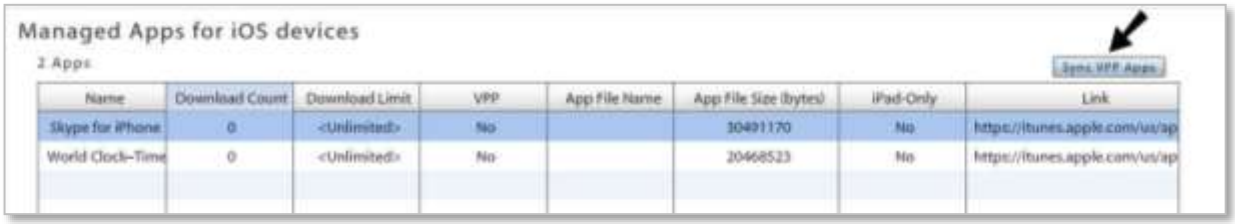
Licenses Available: 496

Licenses Assigned to Users
osu\rspencer2

To Synchronize VPP Applications:

Each time a VPP token is added to the server or edited and each time you access the iOS section of the *Managed Apps* grid, the server automatically connects to the Apple server to retrieve the list of licenses associated with the VPP token to obtain the latest information.

You can also initiate this synchronization by clicking the ***Sync VPP Apps*** button.

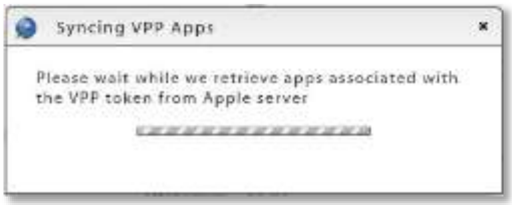


Managed Apps for iOS devices

2 Apps

Name	Download Count	Download Limit	VPP	App File Name	App File Size (bytes)	iPad-Only	Link
Skype for iPhone	0	<Unlimited>	No		30491170	No	https://itunes.apple.com/us/ap
World Clock–Time	0	<Unlimited>	No		20468523	No	https://itunes.apple.com/us/ap

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



Syncing VPP Apps

Please wait while we retrieve apps associated with the VPP token from Apple server

Managing Volume Purchase Program Redemption Codes

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

Apple’s Volume Purchase Program is available in 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.

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

To Add Redemption Codes:

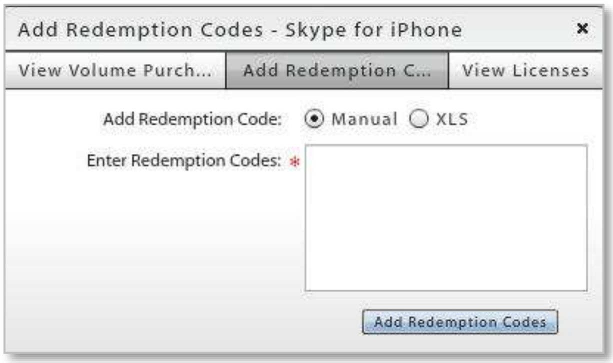
1. Add the app to the iOS Managed App list.
2. Select the app, then click ***Manage Volume Purchase***.
3. Select the ***Add Redemption Codes*** tab.

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

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

   Enter each code on a new line.

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



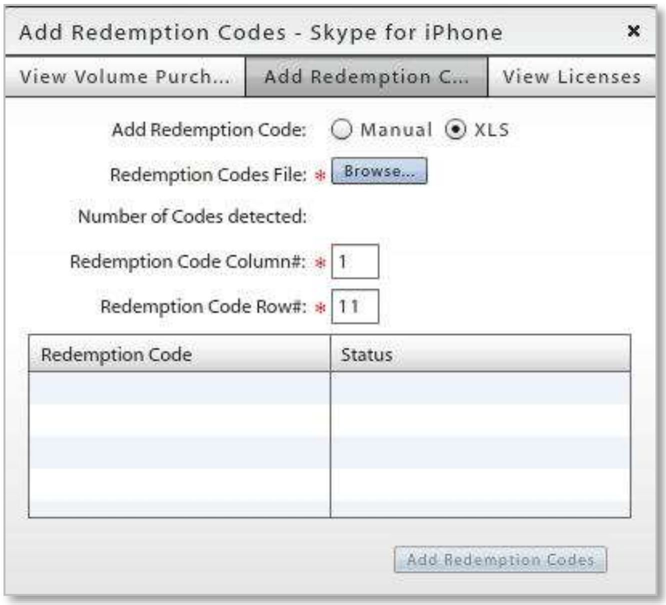
Add Redemption Code: ● Manual ○ XLS

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 Code Column#: * 1

Redemption Code Row#: * 11

Redemption Code	Status

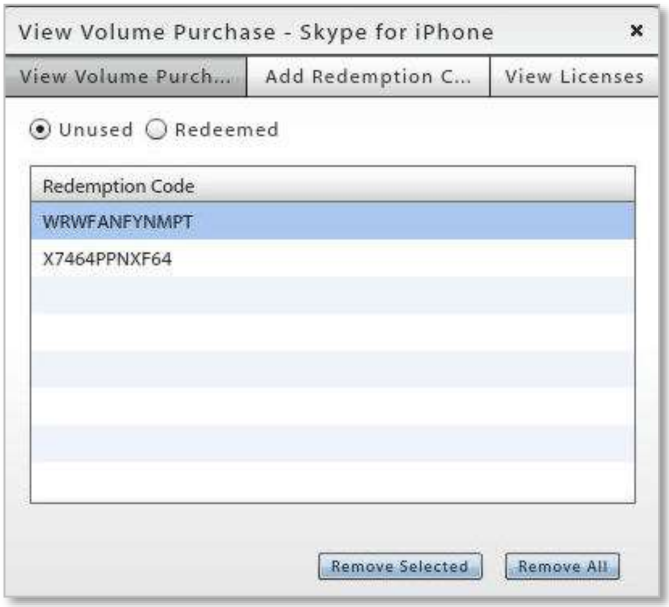
To View or Remove Redemption Codes:

1. Select an app from the iOS Managed App list, then click ***Manage Volume Purchase***.

2. Select the ***View Redemption Codes*** tab.

3. Choose to view either the ***Unused*** or ***Redeemed*** codes.

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

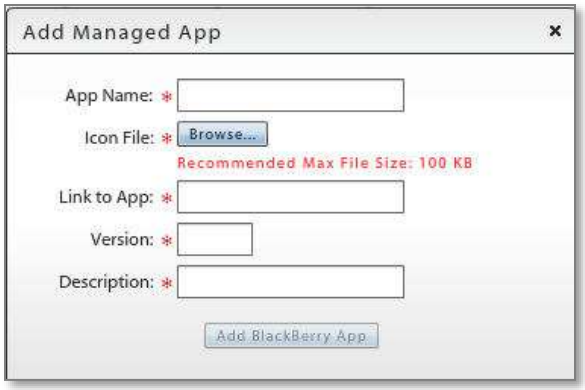


● Unused ○ Redeemed

Redemption Code
WRWFANFYNMPT
X7464PPNXF64

Adding Managed Apps for BlackBerry Devices

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



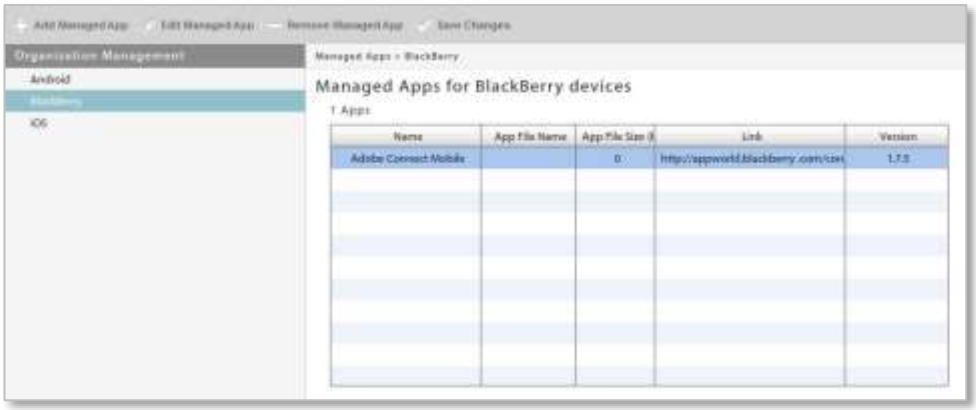
Recommended Max File Size: 100 KB

Add Apps for BlackBerry

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

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

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



Managed Apps for BlackBerry devices

1 Apps

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

Novell Filr

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

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

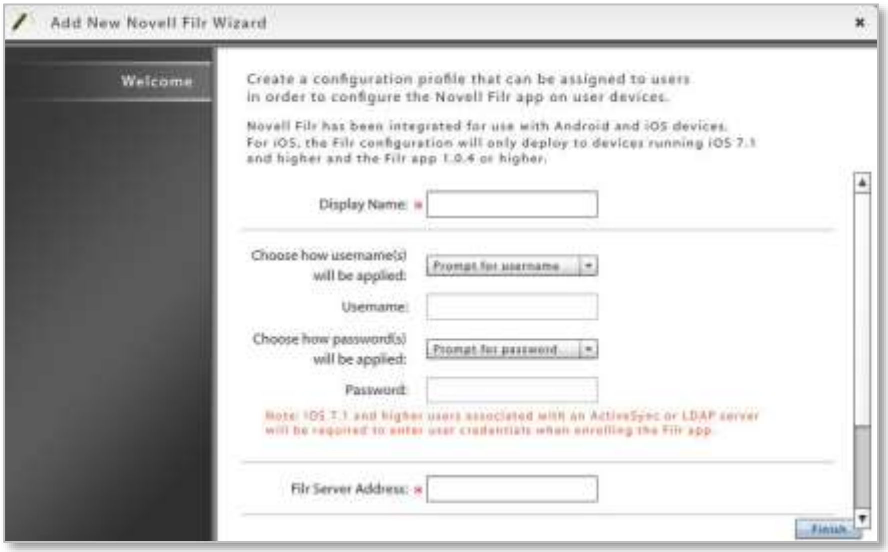
Assigning the Profile. Novell Filr profiles can be assigned to individual users (see Adding Users Guide) or to groups of users via LDAP groups/folders (see Organization Configuration Guide) or local groups, or as organization default settings (see Organization Configuration Guide).

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

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

To create a Novell Filr configuration

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



Create a configuration profile that can be assigned to users in order to configure the Novell Filr app on user devices.

Novell Filr has been integrated for use with Android and iOS devices. For iOS, the Filr configuration will only deploy to devices running iOS 7.1 and higher and the Filr app 1.0.4 or higher.

Display Name: *

Choose how username(s) will be applied: Prompt for username

Username:

Choose how password(s) will be applied: Prompt for password

Password:

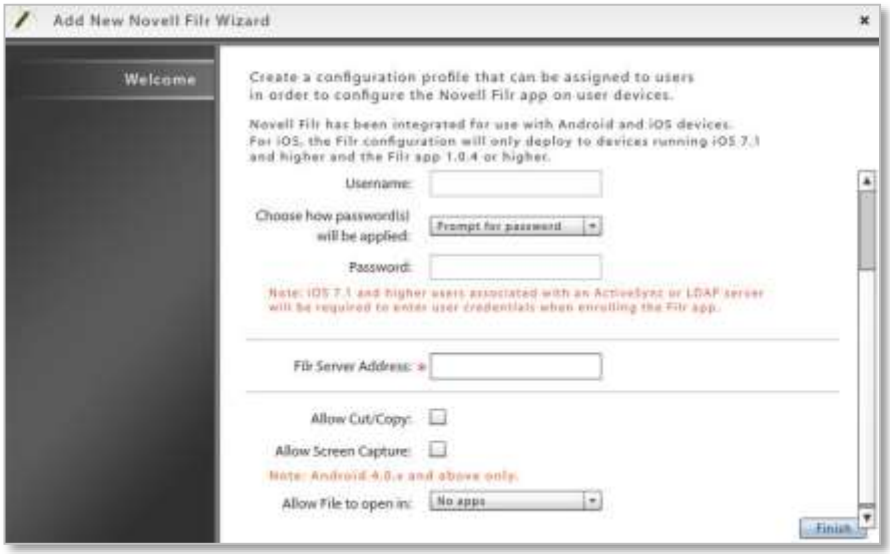
Note: iOS 7.1 and higher users associated with an ActiveSync or LDAP server will be required to enter user credentials when enrolling the Filr app

Filr Server Address: *

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

   Note: iOS 7.1 or higher users associated with an ActiveSync or LDAP server will be required to enter user credentials when enrolling the Filr app, regardless of what is chosen here.
5. Determine how user passwords will be applied:
   - Prompt for password – Prompt the user to enter a password.
   - Enter generic password – Enter a generic password in the **Password** field.
   - Use ZMM password – Apply the password used for authentication with *ZENworks Mobile Management****.***

   Note: iOS 7.1 or higher users associated with an ActiveSync or LDAP server will be required to enter user credentials when enrolling the Filr app, regardless of what is chosen here.
6. Enter the **Filr Server Address**. You might need to enter the address in the format, serveraddress:port
7. Set additional security options.
   - **Allow Cut/Copy** – Leave this unchecked to ensure that users do not circumvent Filr sharing limitations by cutting and copying file content.
   - **Allow Screen Capture** – Leave this unchecked to ensure users do not circumvent Filr sharing limitations by taking screen shots of file content. *(Applicable only for Android devices running OS 4.0.x or higher.)*
   - **Allow File to open in** – Ensure that users do not open a secure file in a non-secure application by selecting **No apps**, or choose **Whitelisted apps** and designate the application in which they are permitted to open secure file.



Create a configuration profile that can be assigned to users in order to configure the Novell Filr app on user devices.

Novell Filr has been integrated for use with Android and iOS devices. For iOS, the Filr configuration will only deploy to devices running iOS 7.1 and higher and the Filr app 1.0.4 or higher.

Username:

Choose how password(s) will be applied: Prompt for password

Password:

Note: iOS 7.1 and higher users associated with an ActiveSync or LDAP server will be required to enter user credentials when enrolling the Filr app.

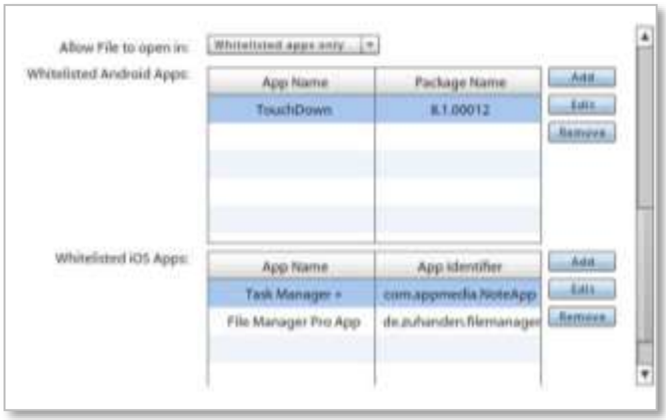
Filr Server Address: *

Allow Cut/Copy: □

Allow Screen Capture: □

Note: Android 4.0.x and above only.

Allow File to open in: No apps



Allow File to open in: Whitelisted apps only

Whitelisted Android Apps:

App Name	Package Name
TouchDown	8.1.00012

Whitelisted iOS Apps:

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

8. Click **Finish**.

Whitelists/Blacklists

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

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

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

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

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

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

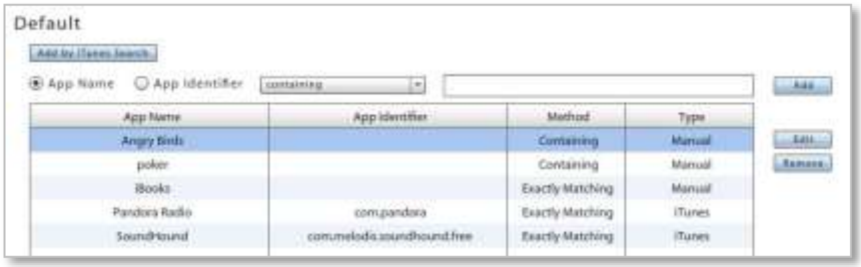
Add Strings to the Blacklist/Whitelist

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

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

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

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



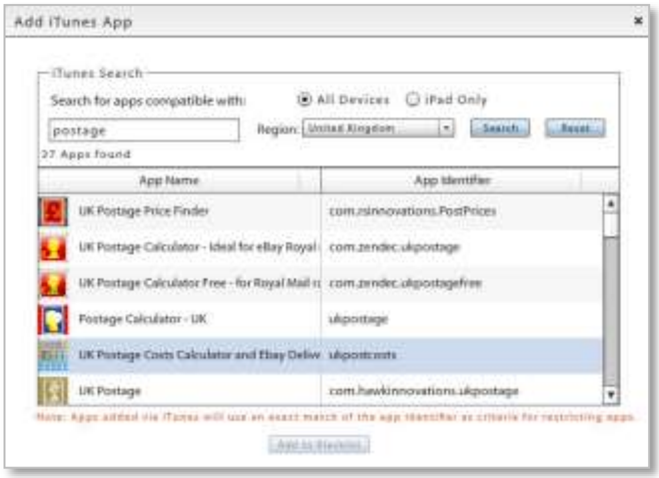
Default

● App Name ○ App Identifier — containing

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

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

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



Add iTunes App

iTunes Search

Search for apps compatible with: ● All Devices ○ iPad Only

postage Region: United Kingdom Search Reset

27 Apps found

App Name	App Identifier
UK Postage Price Finder	com.rsinnovations.PostPrices
UK Postage Calculator - Ideal for eBay Royal	com.zendec.ukpostage
UK Postage Calculator Free - for Royal Mail	com.zendec.ukpostagefree
Postage Calculator - UK	ukpostage
UK Postage Costs Calculator and Ebay Deliv	ukpostcosts
UK Postage	com.hawkinnovations.ukpostage

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

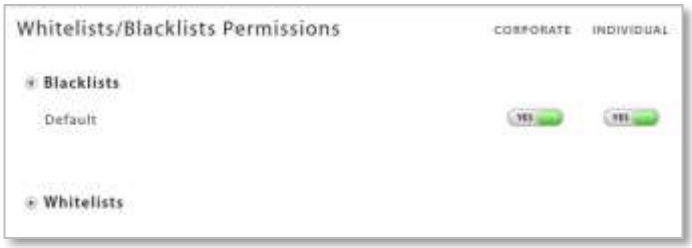
Add to Blacklist

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

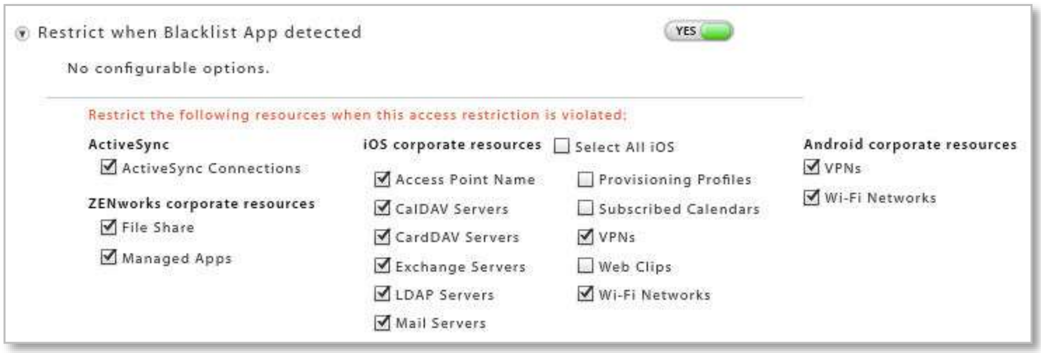
> *Note:* When you enable either the blacklist or the whitelist permission, the ***Record installed applications*** option (under the policy suite category *Audit Tracking*) is automatically enabled. This option must remain enabled in order to monitor application usage.



Whitelists/Blacklists Permissions

	CORPORATE	INDIVIDUAL
Blacklists		
Default	YES	YES
Whitelists		

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:

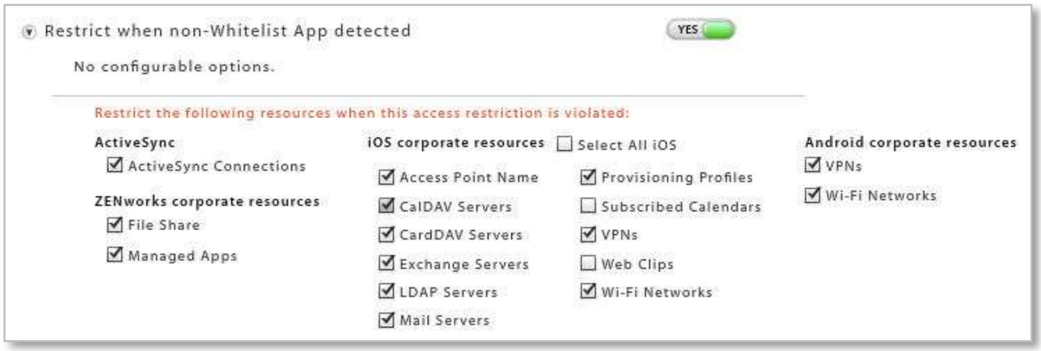
ActiveSync
- ☑ ActiveSync Connections

ZENworks corporate resources
- ☑ File Share
- ☑ Managed Apps

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

Android corporate resources
- ☑ VPNs
- ☑ 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
- ☑ Managed Apps

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

Android corporate resources
- ☑ VPNs
- ☑ 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 *GO!NotifySync* application.

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

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

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

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

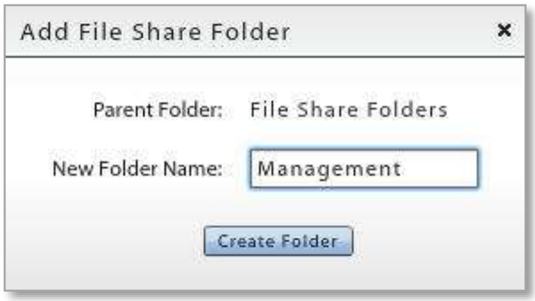
Adding Folders and Files to the Directory

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

Adding Folders

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

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



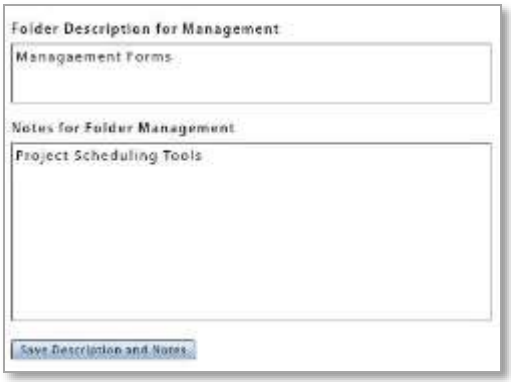
Parent Folder: File Share Folders

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

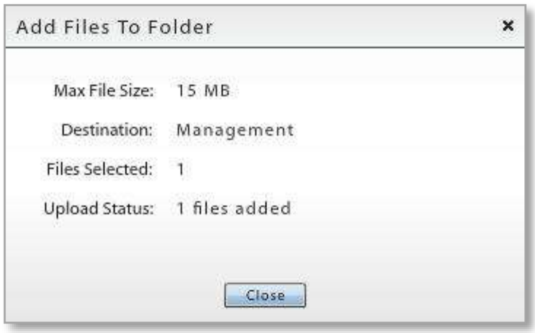
Notes for Folder Management

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.

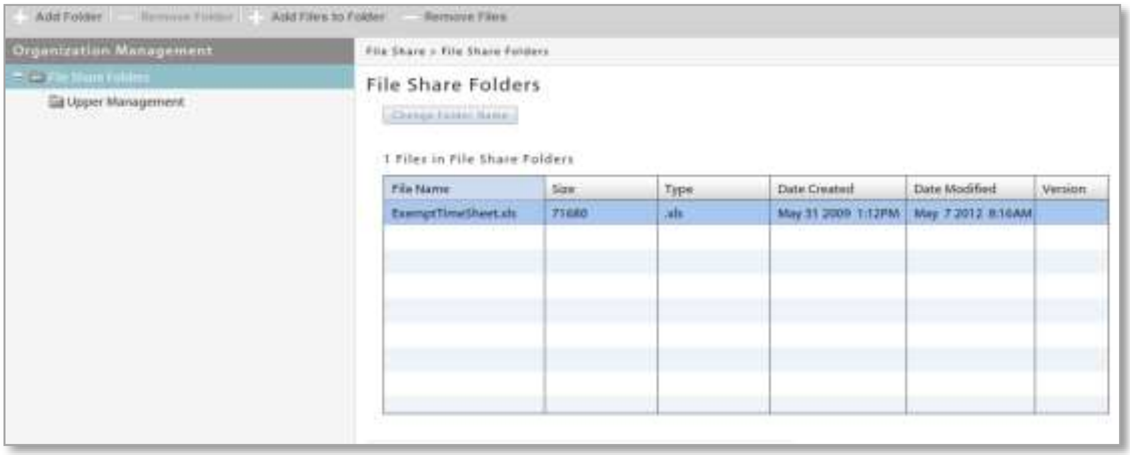


Max File Size: 15 MB

Destination: Management

Files Selected: 1

Upload Status: 1 files added



File Share Folders

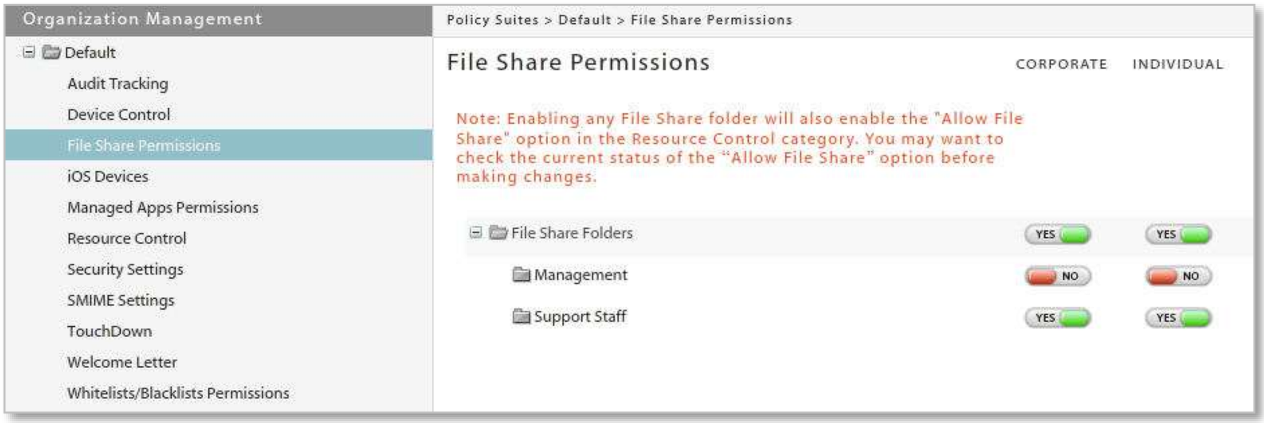
1 Files in File Share Folders

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



File Share Permissions

Note: Enabling any File Share folder will also enable the "Allow File Share" option in the Resource Control category. You may want to check the current status of the "Allow File Share" option before making changes.

	CORPORATE	INDIVIDUAL
File Share Folders	YES	YES
Management	NO	NO
Support Staff	YES	YES

Group Notifications

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

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

Send Group Notifications

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

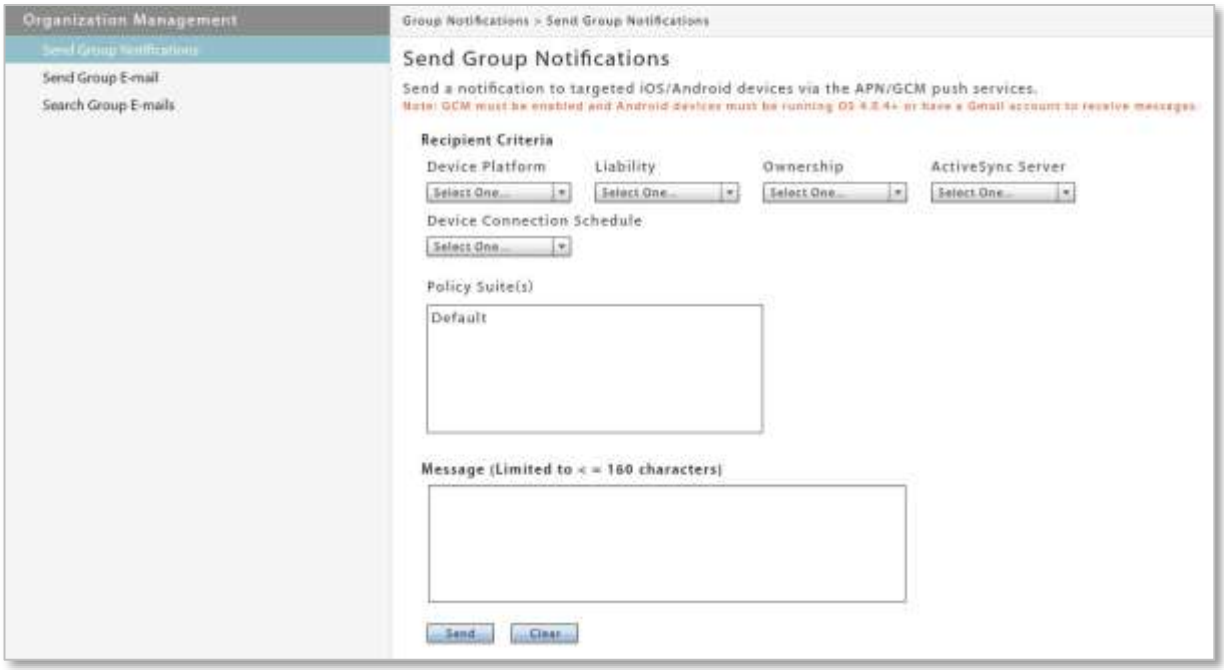
> ***Notes:*** You must upload a NPNS Certificate to the ZENworks Mobile Management server in order to send Group Notifications to iOS devices. (From the dashboard, select ***System*** > ***Organization*** and click the *Upload* button next to the ***NPNS Certificate*** field.)
>
> Google Cloud Messaging must be enabled and Android users must be running OS 4.0.4+ or have a Gmail account registered on the device to receive messages.

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

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

Notification messages are limited to 160 characters or less.

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



Send Group Notifications

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

Recipient Criteria

Device Platform: Select One...

Liability: Select One...

Ownership: Select One...

ActiveSync Server: Select One...

Device Connection Schedule: Select One...

Policy Suite(s): Default

Message (Limited to < = 160 characters)

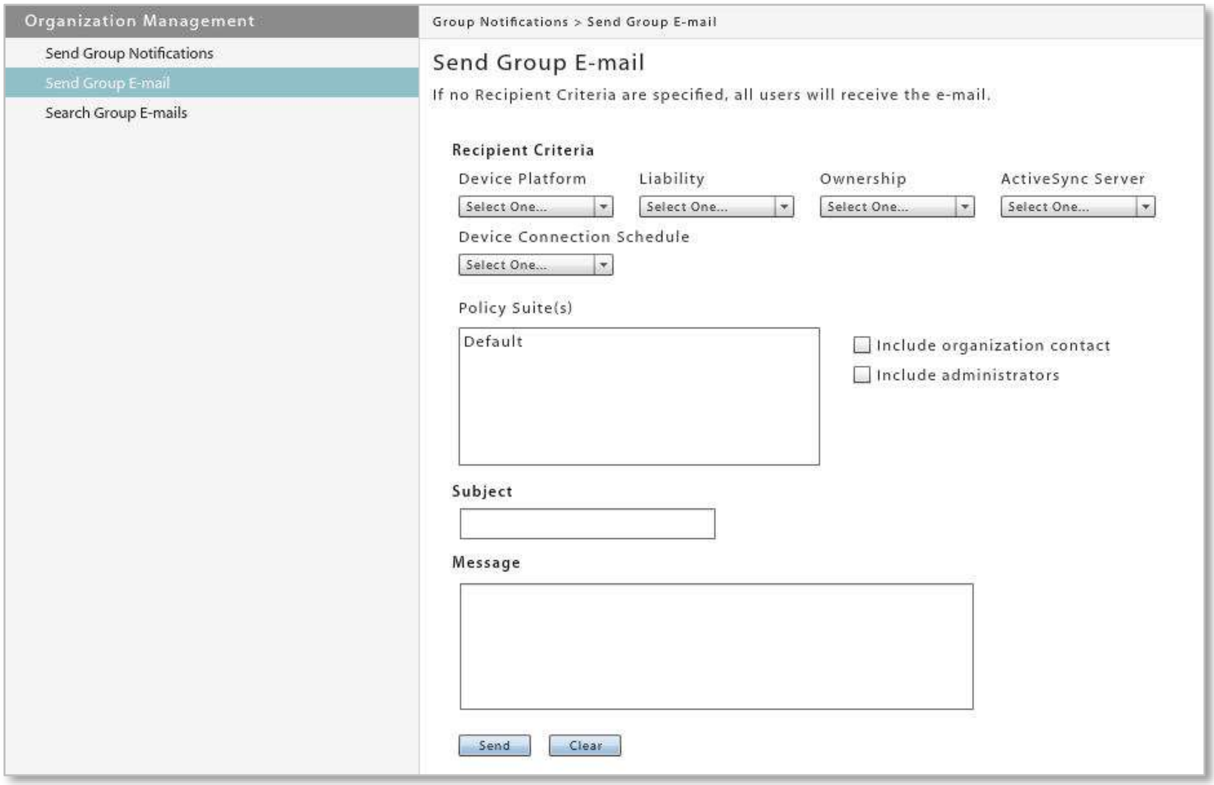
Send Group E-mail

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

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

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

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



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: Select One...

Device Connection Schedule: Select One...

Policy Suite(s): Default

□ Include organization contact

□ Include administrators

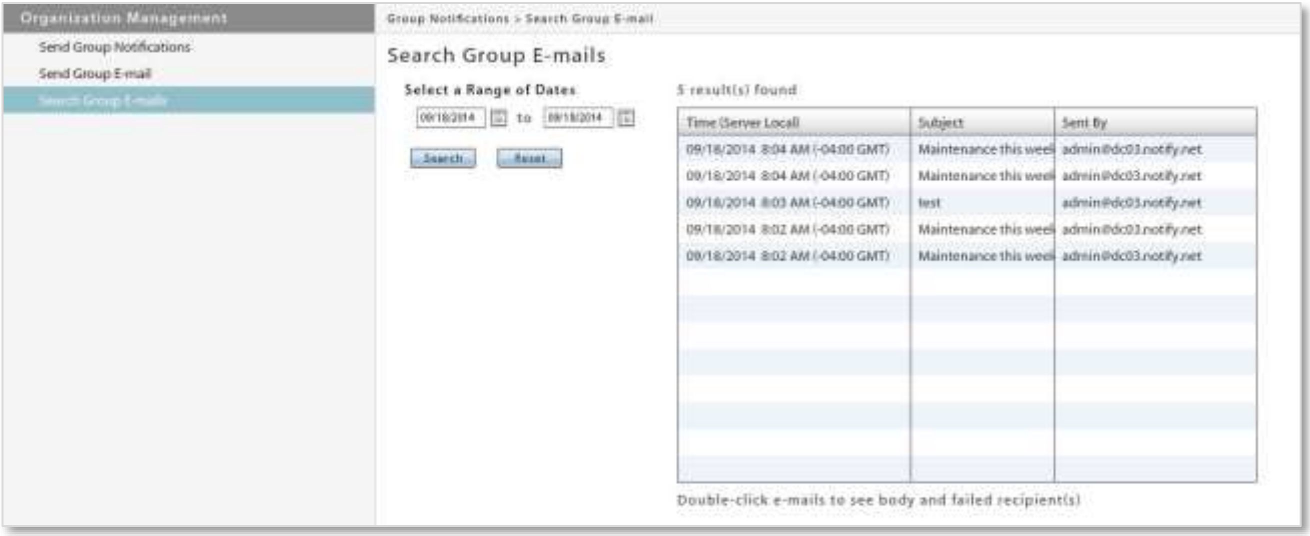
Subject

Message

Search Group E-mail

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

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



Search Group E-mails

Select a Range of Dates

09/18/2014 to 09/18/2014

5 result(s) found

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

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

Appendix A: Recovering User Information

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

```
USE [MDM]
GO

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

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