Organization Administration

ZENworks® Mobile Management 2.8.x

November 2013

Novell®

Legal Notices

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

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

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) 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.

The Activity Monitor

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

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

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

You can choose which six to display from the following:

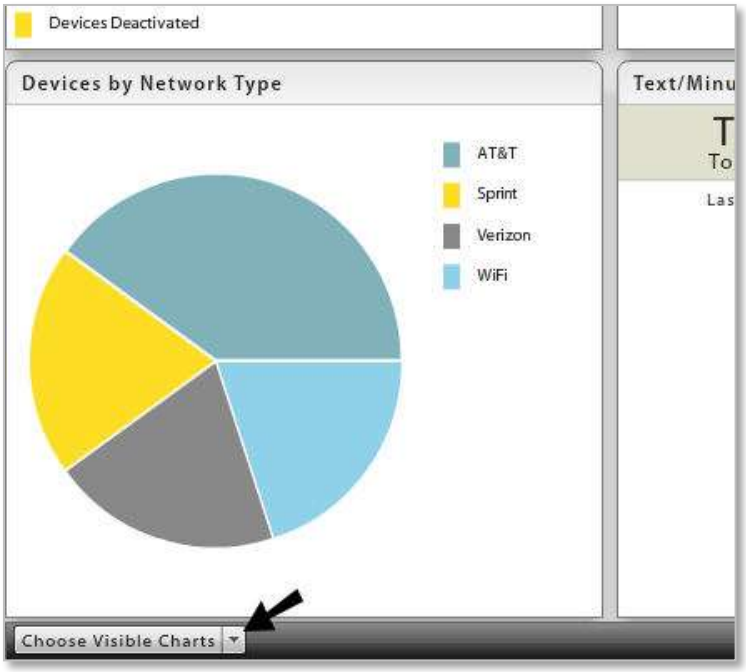
Configuration	
Activation/De-Activation History	Bar chart showing the number of devices activated and deactivated in the past seven days.
Active/Inactive Devices	Pie chart showing the percentage of active devices versus disabled devices.
Devices by Carrier	Pie chart showing the percentage of devices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

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

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

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

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



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

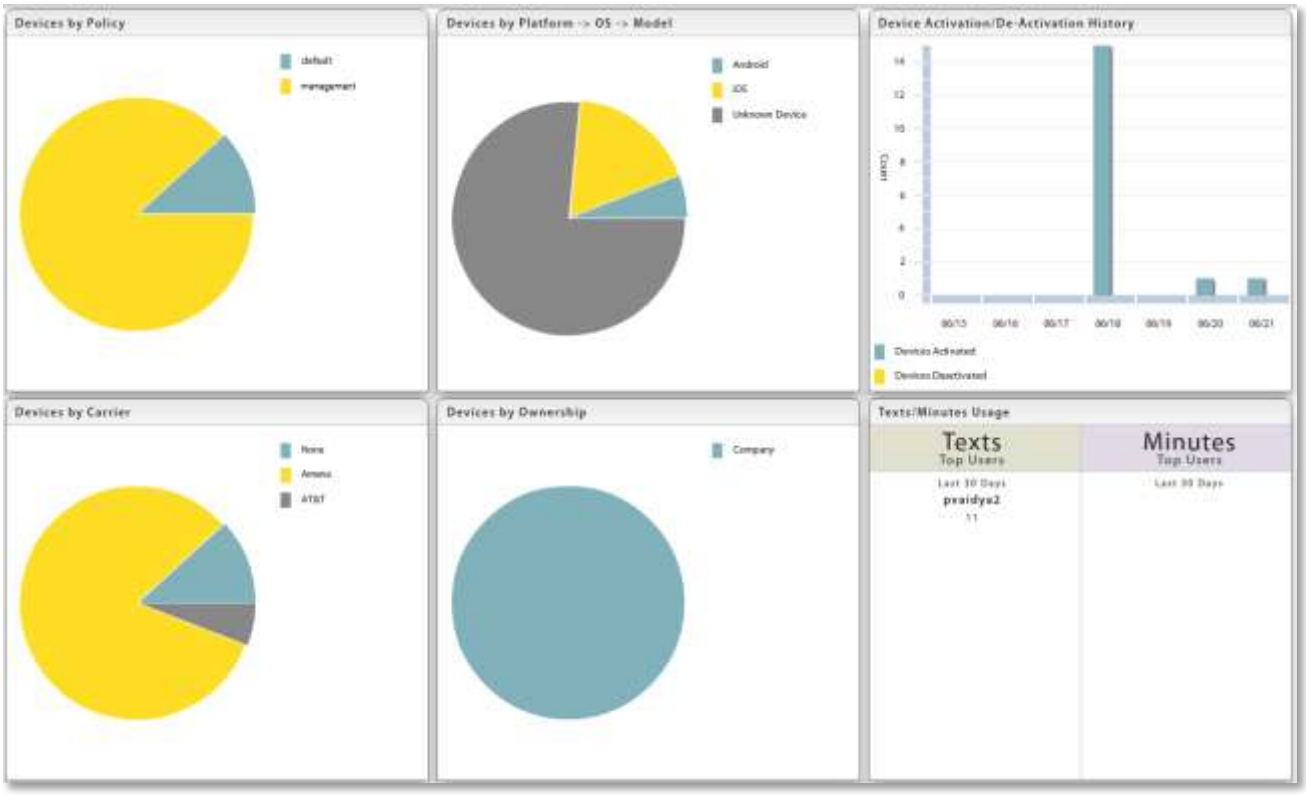
The Activity Monitor grid always displays six graphs. If fewer are chosen, the most recently deselected graphs will display along with your choices. You cannot select more than six graphs. You must deselect a graph before you can choose a different graph.

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

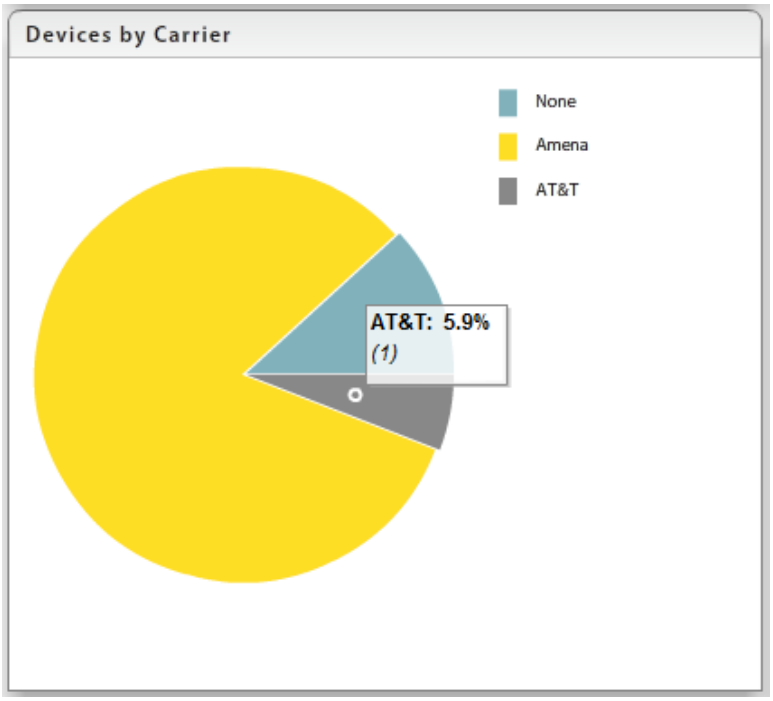
Chart Group Presets. You can choose a preset group of charts.

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

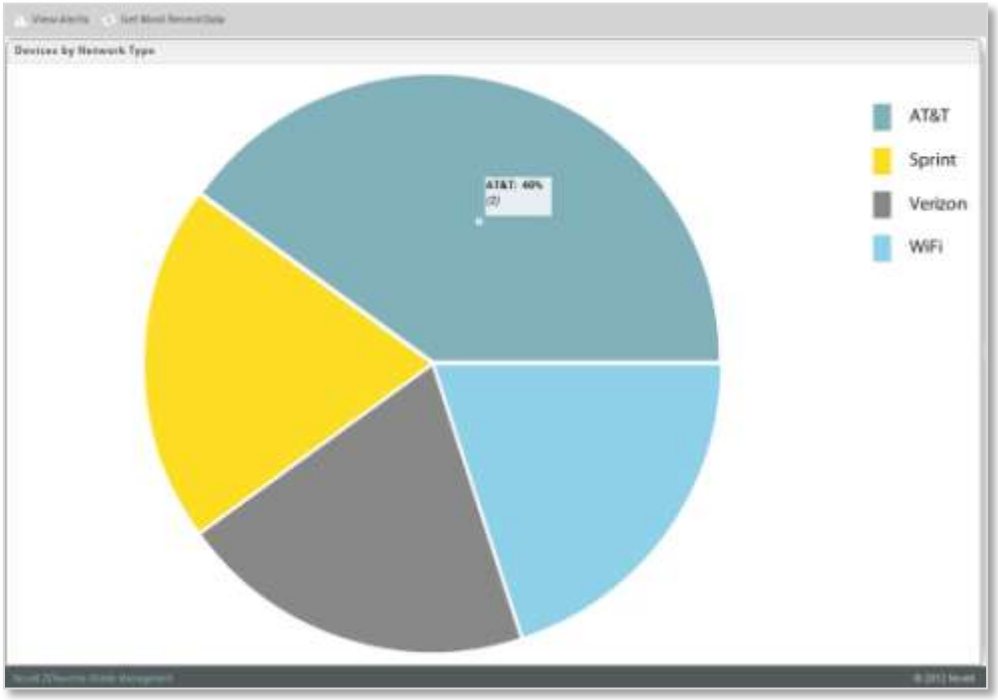
Rearrange Panels. You can rearrange the panels in the view by selecting a block and dragging it and dropping it where you prefer.



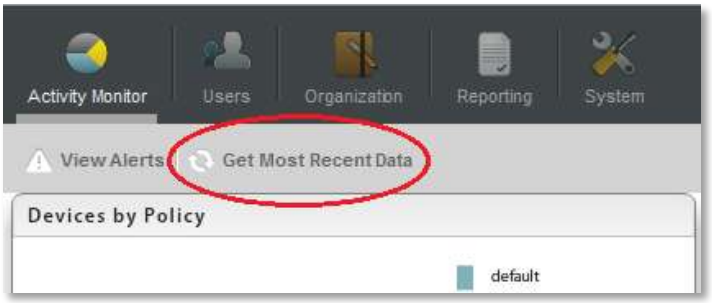
View Details. You can see detail of the statistics by hovering over a section of a graph or chart.



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

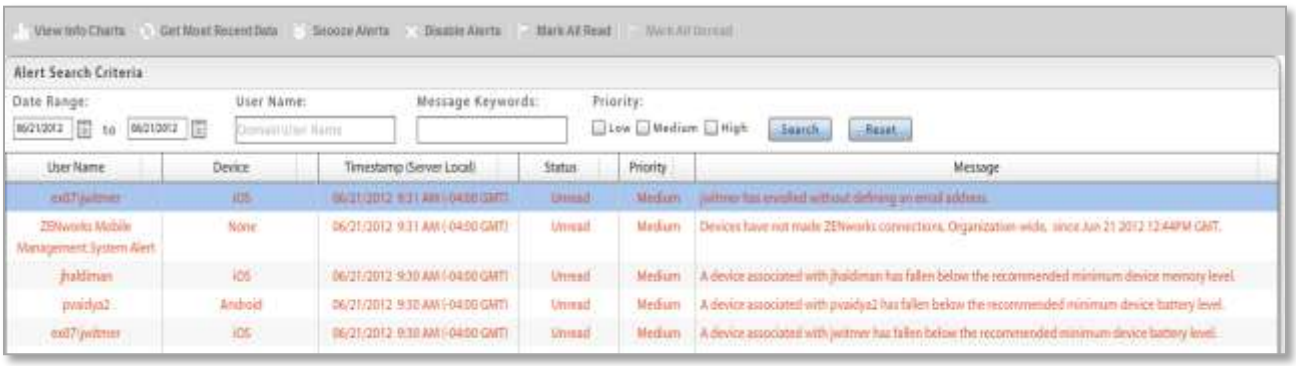


Refresh the View. You can refresh the Activity Monitor view with the most recent data by selecting *Get Most Recent Data* in the gray option bar.

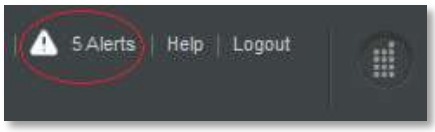


Flip to the *View Alerts* Grid. You can flip the Activity Monitor view to a table of alerts listed by user. Select ***View Alerts*** in the option bar. Select ***View Info Charts*** to return to the Activity Monitor view.

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



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



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

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

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

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

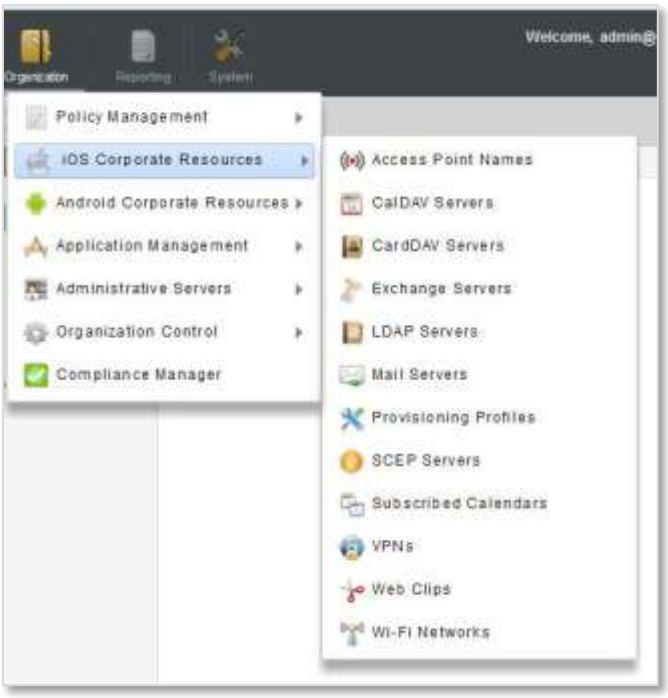
Corporate Resource Management

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.

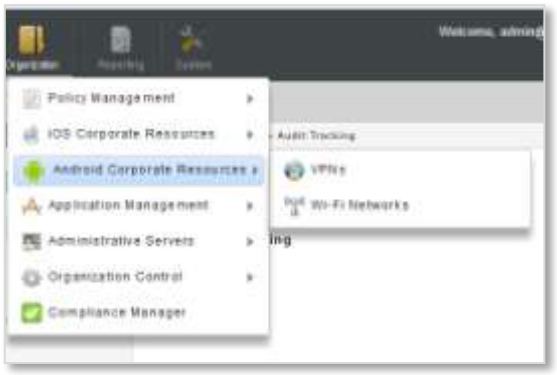
Use the resource tools in the dashboard's ***Organization*** view to define credentials for the server and network resources. Then use the resources in the *User Profile* to associate iOS or Android device users with a resource and configure user account settings to push out to devices.

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 (iOS 5+) -Account Type -IMAP Path Prefix -Authentication Type -Expiration (iOS 6+)	-Exchange Server Name -Exchange Server Address -Exchange Port -Use SSL -Use S/MIME (iOS 5+) -Allow Move (iOS 5+) -Use Only in Mail (iOS 5+) -Allow Recent Address Syncing (iOS 6+) -Expiration (iOS 6+)	-LDAP Display Name -LDAP Server Address -LDAP Port -Use SSL -LDAP Searches -Expiration (iOS 6+)	-Display Name -Server Address -Server Port -Use SSL -Expiration (iOS 6+)	-Display Name -Server Address -Server Port -Use SSL -Expiration (iOS 6+)

Sample Add New Server Wizard

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

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

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

Configuring Network Settings

The credentials for each network are defined using a wizard.

Wi-Fi Networks (iOS) **-**Resource Name -SSID -Auto Join (iOS 5+) -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)** **-**Resourcve 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

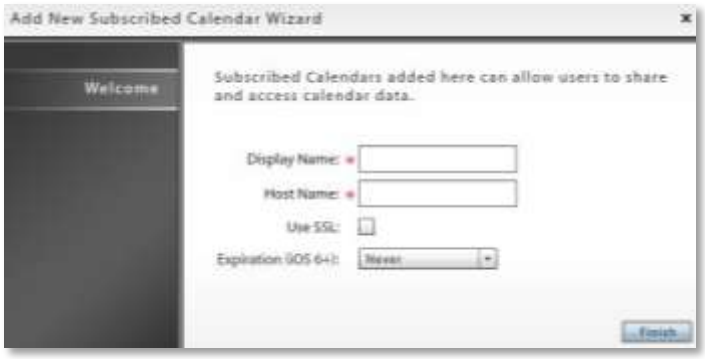
Sample Add New Network Wizard

Configuring Other Resources

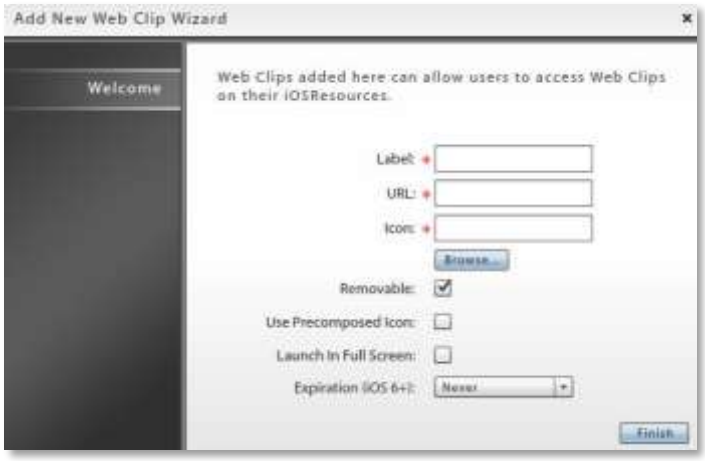
Access Point Names	Provisioning Profiles	Subscribed Calendars	Web Clips
-Access Point Name	-Display Name	-Display Name	-Label
-Proxy	-Provisioning Profile	-Host Name	-URL
-Proxy Port	-Apply to Organization	-Use SSL	-Icon
-Expiration (iOS 6+)	-Expiration (iOS 6+)	-Expiration (iOS 6+)	-Removable
			-Use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

Access Point Name Wizard

Provisioning Profile



Subscribed Calendar Wizard



Web Clip Wizard

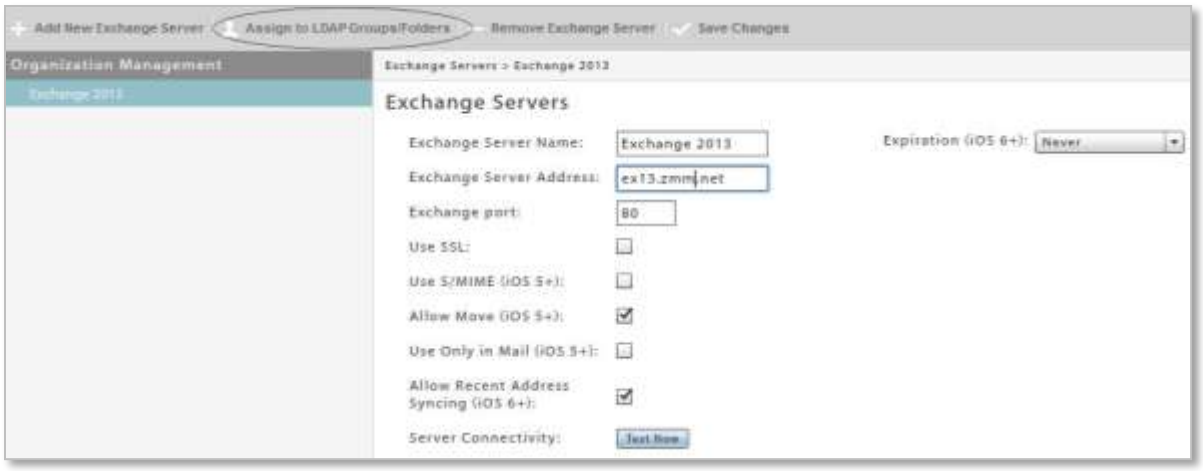
Assigning Resources to LDAP Groups and Folders

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.

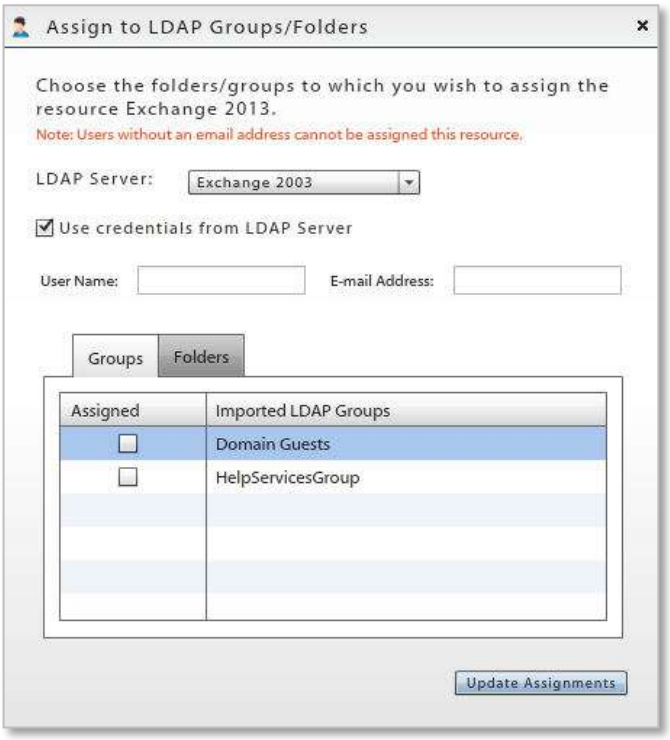
> ***Note:*** These methods cannot be used to assign the SCEP server resource to users, because of the unique challenge code required for each user.

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**.



1. Select an **LDAP Server** from the drop-down list.
2. Some resources have an option to **Use credentials from the LDAP Server**. Keep this option enabled unless you want to assign a resource to a group email address.

   If you disable the option, you must enter the shared User Name or shared User Name and Email Address. The assignment is made to that mail account only.
3. Click the *Groups* or *Folders* tab and navigate through the LDAP directory to select the groups of folders to which you will assign the resource.
4. Click the **Update Assignments** button.



Simple Certificate Enrollment Protocol (SCEP) Servers

What is SCEP?

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

Benefits of a SCEP Server in your Environment

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

SCEP Limitations

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

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

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

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

SCEP Servers and the ZENworks Mobile Management System

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

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

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

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

Define a SCEP Server

From the dashboard, select ***Organization*** > ***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.

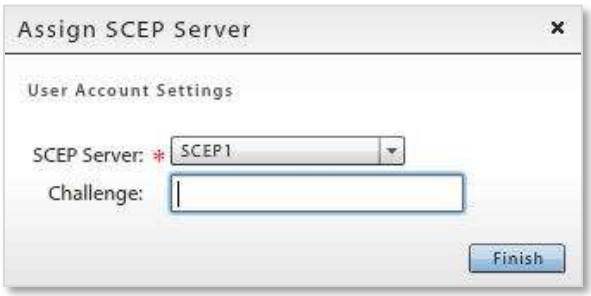
Now, use the *Corporate Resource* option in the **User Profile** to associate users with a SCEP server.

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.

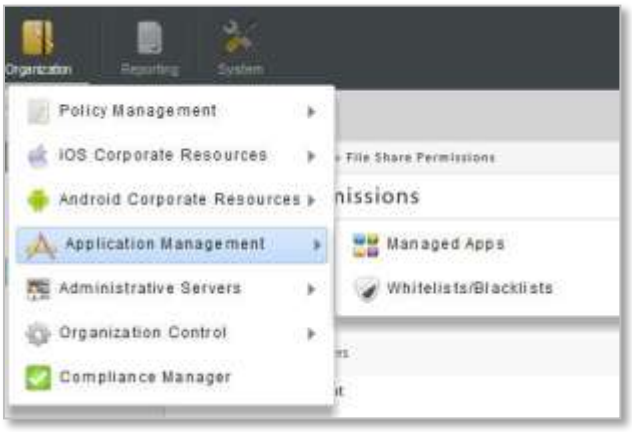
To obtain a challenge password, browse to the SCEP URL. Enter the authentication credentials (by default Integrated Windows Authentication). Copy the *Enrollment Challenge Password* and paste it into the *Challenge* field.



Application Management

Application Management settings are located in the *Organization* view of the dashboard. They include options that give you the ability to make a list of recommended applications available to users or to restrict the apps a user may install on the device and still have access to create custom column fields for the user base, communicate information to users, and manage the file share.

- Whitelists/Blacklists
- Managed Apps



Whitelists/Blacklists

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

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

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

Add Strings to the Blacklist/Whitelist

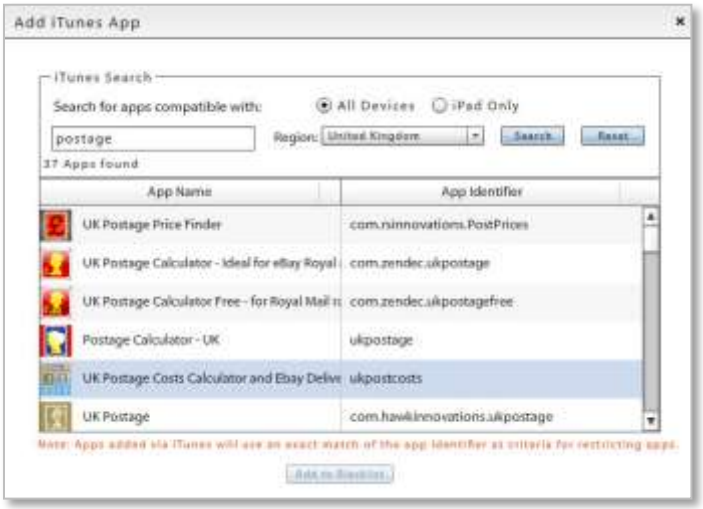
First, create the list of strings. Select ***Organization*** > ***Application Management*** > ***Whitelists/Blacklists*** > ***Blacklists*** or ***Whitelists***.

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.

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 eed to search exclusively for iPad applications, then click ***Search***. Apps added in this way are matched against their *App Identifier*.



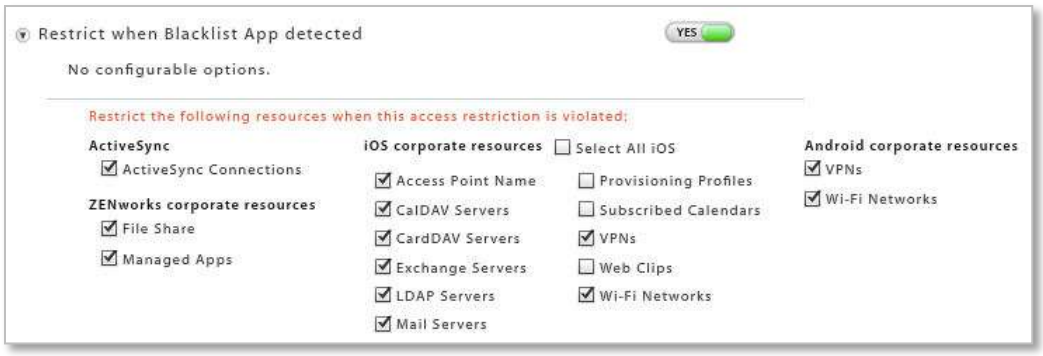
Activating a Blacklist or Whitelist

Blacklists or Whitelists will not affect users until the *Restricted App Permissions* and the Blacklist or Whitelist Compliance Restriction option have been enabled. In addition, the *Record application data usage* option is enabled automatically and must be remain enabled in order to monitor application usage.

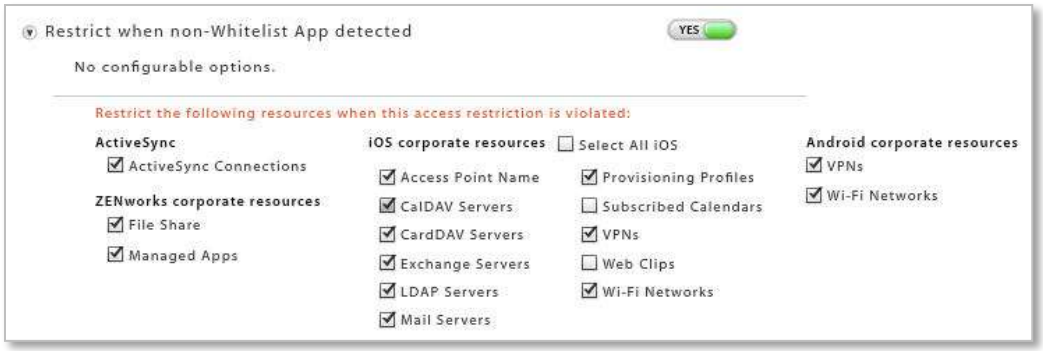
Enable the Whitelists/Blacklists Permissions. Once the list is created, enable the *Blacklist Permissions* in the policy suite(s). Select *Organization* > *Policy Management* > *Policy Suites* > (expand a policy suite) > **Whitelists/Blacklists *Permissions***. Enable either the Blacklist or Whitelist 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.

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.



or



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

In this section you will find information on:

Accessing Managed Apps on a Device

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

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

Adding Managed Apps: An Overview

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

User Installed Apps

Apps can be added to the list as a link to the download page where the user can obtain the app, or as an actual app file that the user can install.

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

Enforced Application Management

Enforced application management is supported for the Android and iOS 5+ device platforms. Administrators can force push Android and iOS applications on the Managed App list to the device and users will be required to install them.

- For ***iOS 5+*** 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.)

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. 

   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.

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 Managed Apps for BlackBerry, Symbian, and Windows Mobile

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

Add Apps for BlackBerry

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

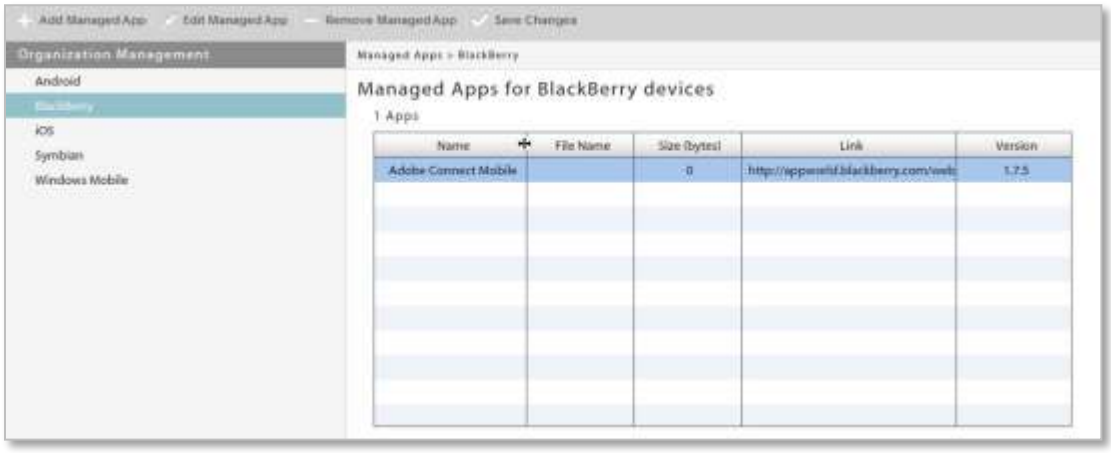
3. Select ***File*** or ***Link***. If you are adding a BlackBerry app, the default is the *Link* method.
4. Enter a ***Name***, ***Version***, and ***Description*** for the app. What you enter displays on the device.
5. For *Links*, provide the application store URL in the ***Link to App*** field.

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

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

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

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



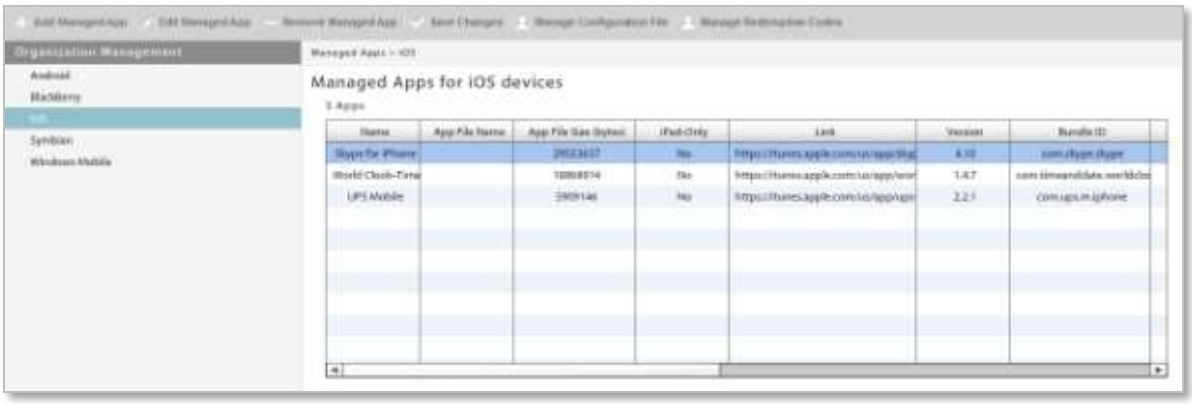
Adding and Managing Apps for iOS 5+ Devices

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:



Configuration File 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

```
<dict>
        <key>key1</key>
        <string>value1</string>
        <key>key2</key>
        <string>value2</string>
</dict>
```

Example

```
<dict>
        <key>username</key>
        <string>username</string>
        <key>password</key>
        <string>password</string>
</dict>
```

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

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.

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.
    a. 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***.
    b. 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.

    If adding a ***Configuration File*** to configure a third party app, click the browse button and select your configuration file.
5. Select ***Remove With MDM*** if you want the app to be deleted from the device when the MDM configuration profile is removed.
6. Select ***Prevent Backup*** if you want the user to be able to save the app via iTunes.
7. Click ***Add iOS App*** to add the App to the iOS Managed App list.

Search iTunes to add an app

Manually add an app

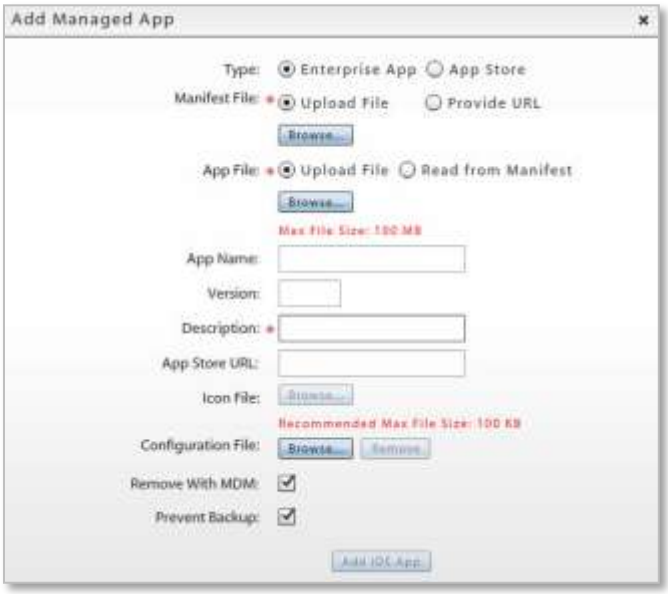
Adding an iOS Enterprise App

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

1. Select ***Organization*** > ***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. If using a ***Configuration File***, to configure a third party app, click the browse button and select your configuration file.
7. Select ***Remove With MDM*** if you want the app to be deleted from the device when the MDM configuration profile is removed.
8. Select ***Prevent Backup*** if you want a user to be able to save the app via iTunes.
9. Click ***Add iOS App*** to add the app to the iOS Managed App list.



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.

Managing Application Redemption Codes

For apps on your list that have been purchased through the Apple Volume Purchase Program (VPP), add the redemption codes to the server. There will be one redemption code for every copy of the app purchased.

Apple's Volume Purchase Program is available in the United States and in nine countries outside the US. Redemption codes are different for each country, so you must add multiple sets of codes if you have purchased apps for users in more than one country.

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

To Add Redemption Codes:

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

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

   If you are entering each code individually, choose Manual.

   Enter each code on a new line.

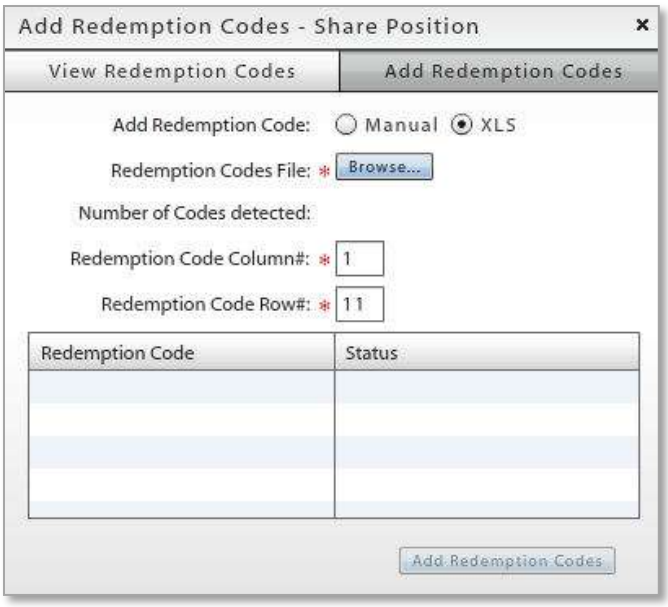
5. Click the ***Add Redemption Codes*** button.

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.

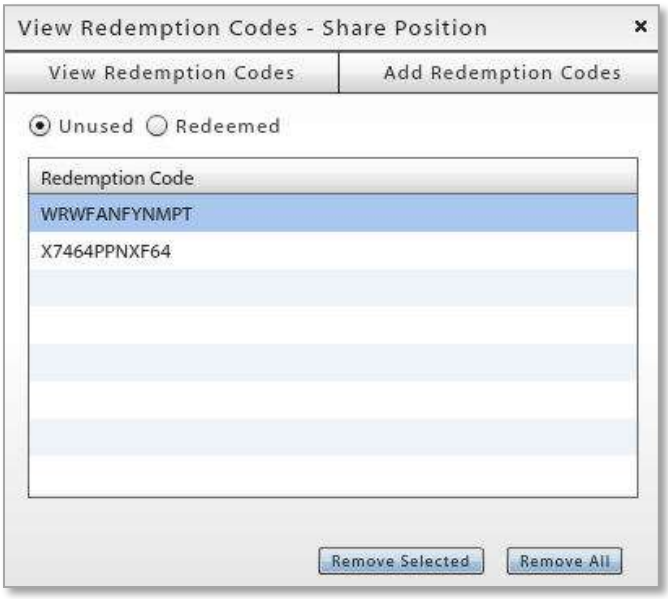
7. Click the *Add Redemption Codes* button.



To View or Remove Redemption Codes:

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

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



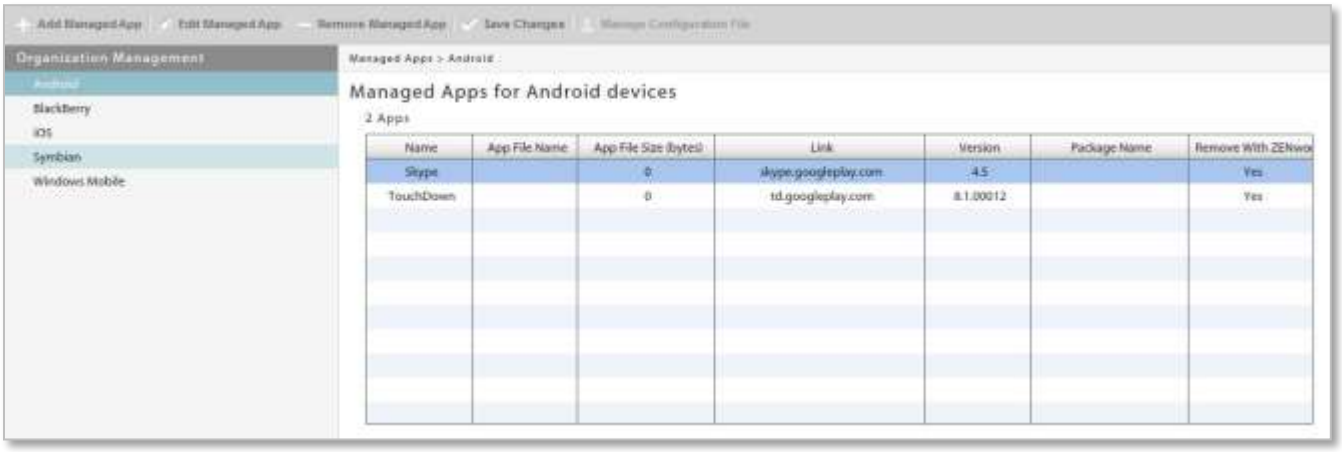
Adding and Managing Apps for Android Devices

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

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

Select ***Organization Management*** > ***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.

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***.
3. Choose *Google Play Store* as the ***Method*** to add the app.
4. Enter the ***App Name***, ***Version***, and ***Description*** for the app. What you enter displays on the device.
5. Enter the Play Store URL in the **Link to App** field.
6. Browse your image files at the ***Icon File*** field and select an icon to associate with the application.
7. Select ***Remove With MDM*** if you want the app to be deleted from the device when the MDM configuration profile is removed.
8. Click ***Add Android App*** to add the App to the Android 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***.
3. Choose *File* or *Link* as the ***Method*** to add the app.
4. Enter the ***App Name***, ***Version***, and ***Description*** for the app. What you enter displays on the device.
5. For *Links*, provide a URL for the application in the ***Link to App*** field.

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

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

7. Browse your image files at the ***Icon File*** field and select an icon to associate with the application.
8. Select ***Remove With MDM*** if you want the app to be deleted from the device when the MDM configuration profile is removed.
9. Click ***Add Android App*** to add the App to the Android Managed App list.

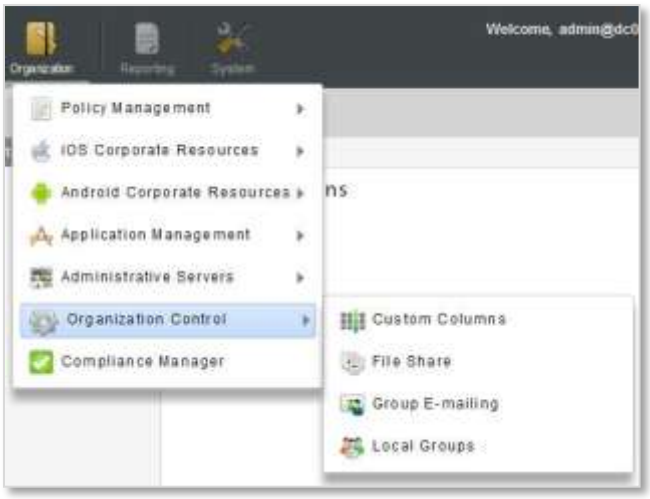
Updating Android App Versions

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

Organization Control

Organization Control Options

Organization Control settings are located in the *Organization* view of the dashboard. They include options that give you the ability to create custom column fields for the user base, communicate information to users, manage the file share, and create local groups.



Custom Column Management
(see *Configuration Guides*)

- Custom Columns

Email and File Share Management Options
(documented in this guide)

- File Share
- Group E-mailing

Local Groups
(see *User Management Guide*)

- Local Groups

File Share

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

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

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

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

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

Adding Folders and Files to the Directory

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

Adding Folders

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

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

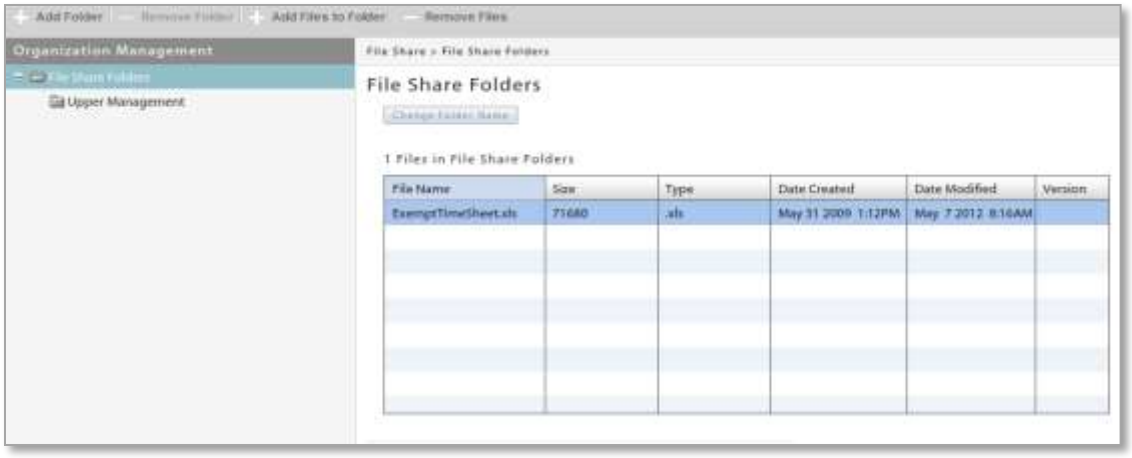
You can edit a folder label by highlighting a folder and clicking the ***Change Folder Name*** button.

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

Adding Files

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

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



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

Enabling the File Share Permissions

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

Group E-mailing

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

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

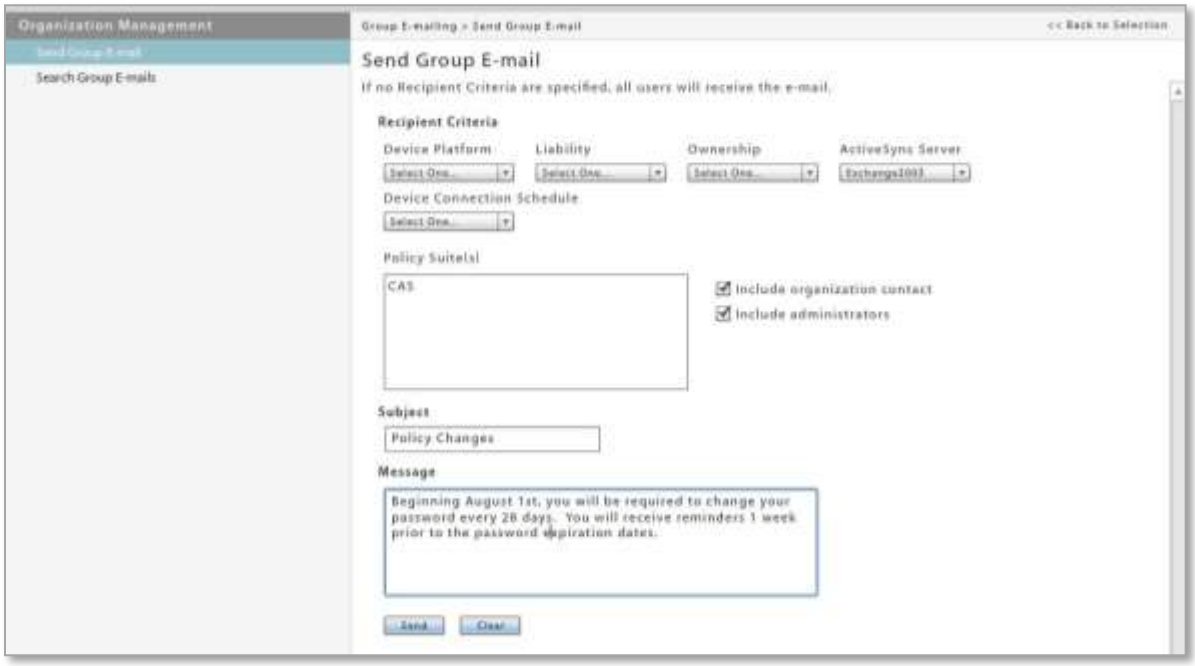
Send Group E-mail

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

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

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

1. To send a group email, select ***Organization***. From the drop-down menu, select Organization control > ***Group E-mailing.***
2. Select ***Send Group E-mail*** from the left panel.

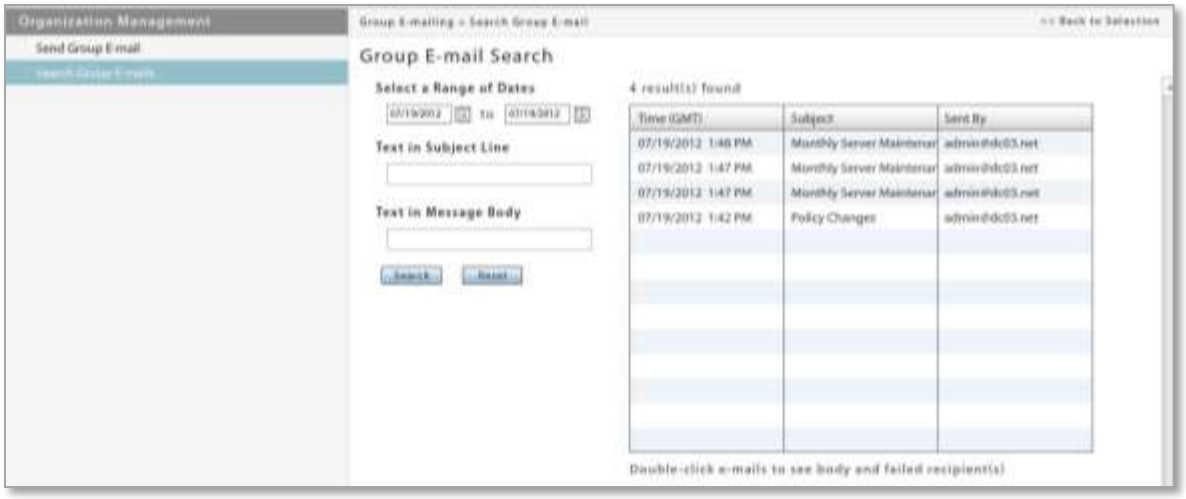


Search Group E-mail

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 E-mailing***.

2. Select ***Search Group E-mails*** from the left panel.



Other Organization Administration Options

Several of the options in the dashboard's *Organization* view are not documented in this guide. Information on these topics can be found by clicking the link provided below.

Organization Configuration Guide

- Policy Management
- Administrative Servers

System Administration Guide

- OpenID Provider

Compliance Manager Guide

- Compliance Manager

Reporting

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

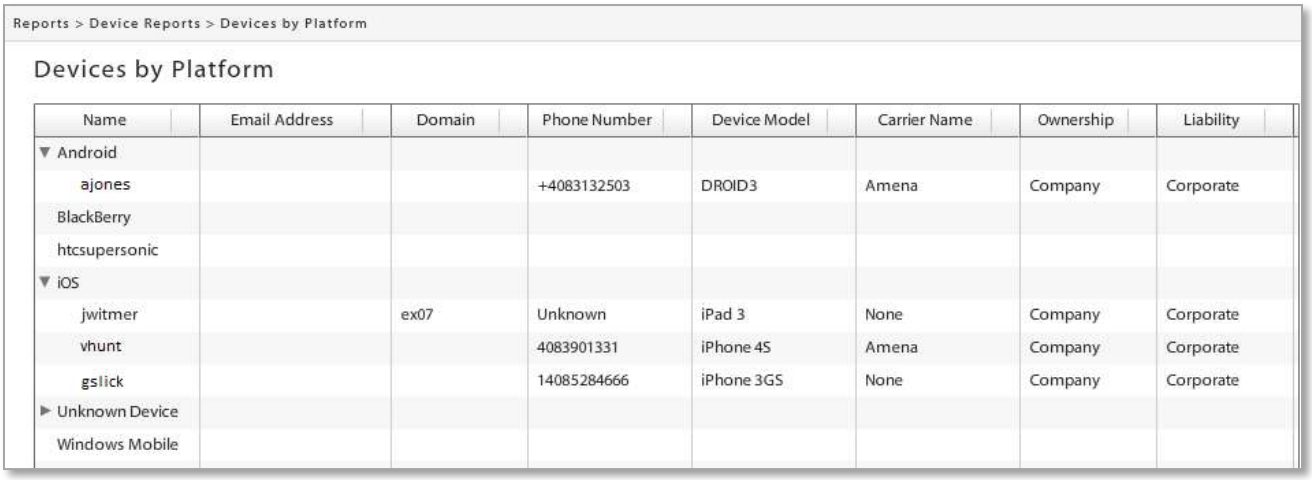
The reports are as follows:

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

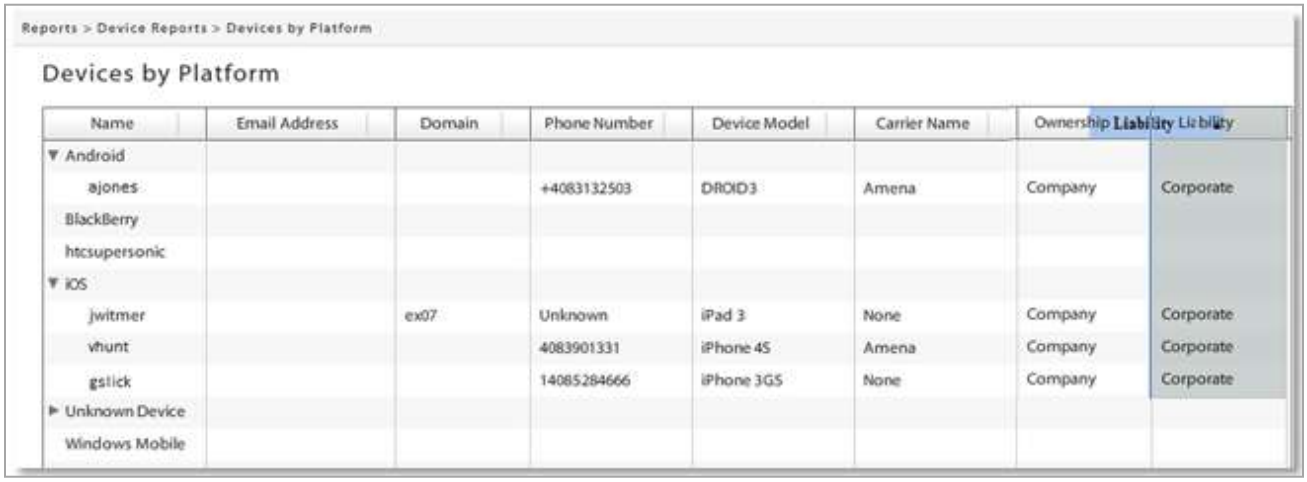
Using the Reports

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

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



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



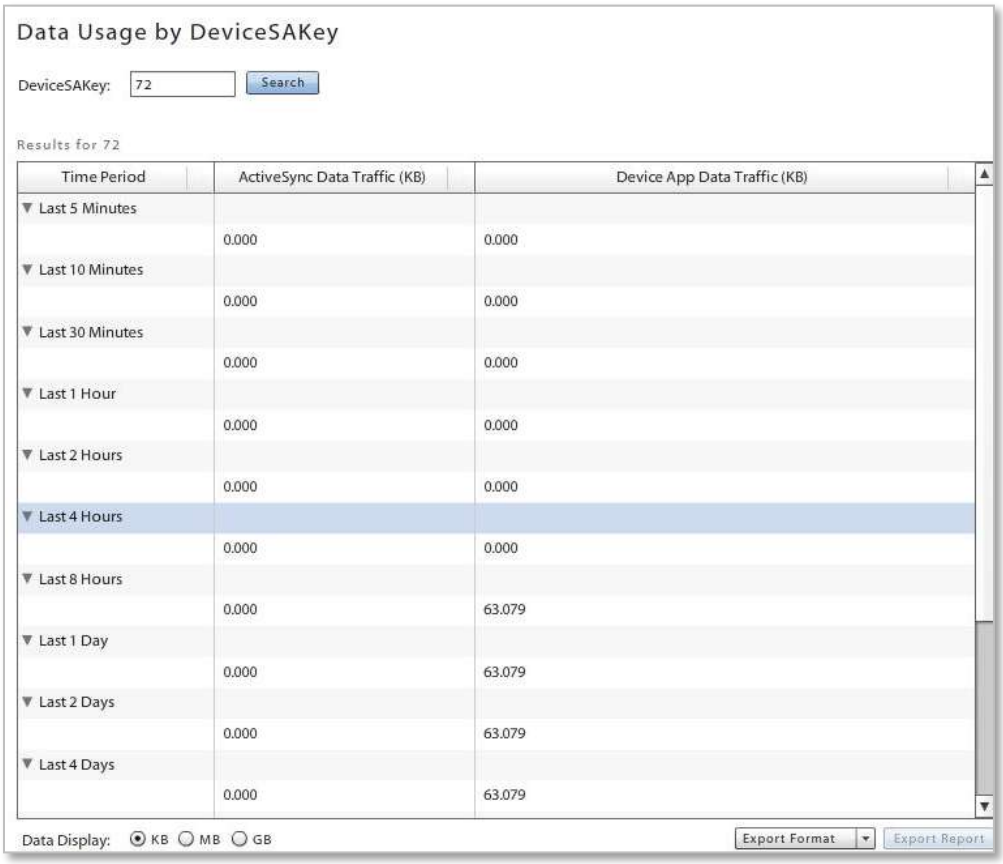
Export Report Data. Export data from the report to a comma separated values (CSV) or Excel (XLS) file. Choose the ***Export Format***, then click the ***Export Report*** button to save the current report to a file.

Sample Reports

Sample Device/User Reports

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

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



Sample iOS Resource Report

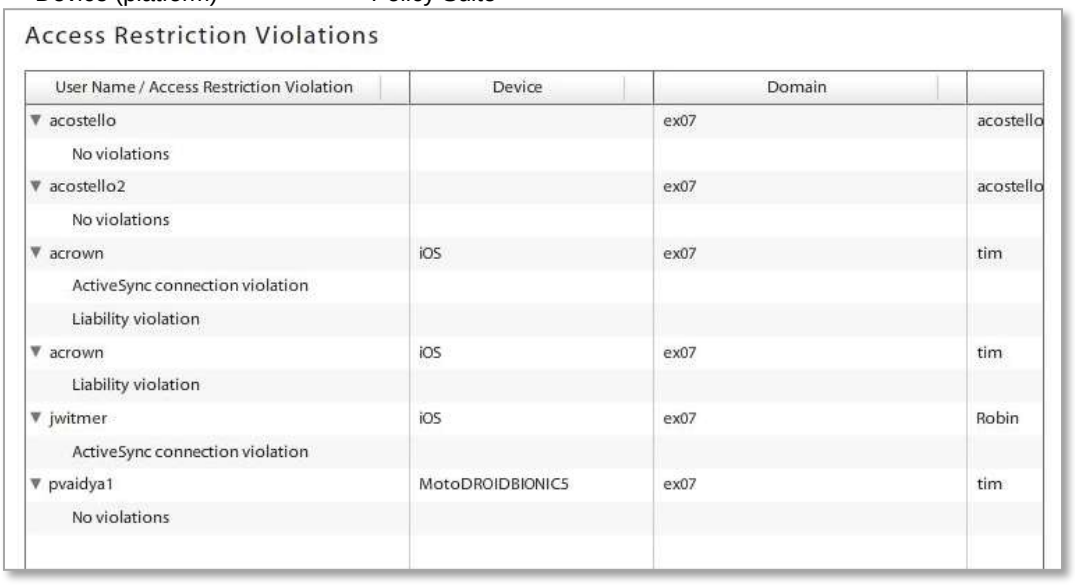
Information included in ***iOS Resource*** reports:

- Resource Name
- Domain
- User Name
- Expiration Dates

Sample Compliance Report

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

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



Sample Administrative Roles Report

Information included in ***Administrative Roles*** reports:

- Administrator Name
- Administrative Role Name
- Permissions