Organization Administration

ZENworks® Mobile Management 2.5.x

July 2012

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.

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

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

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

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 4

Managing Users 5

The Users View....5
Customizing the User List View....6
Exporting Data from the List....7
User Profiles....8
User Detail Panel....8
Device Compliance....9
Remote Security Commands....10
Enabling Password Recovery....12
User Profile Views....13
Searching Phone and Text Logs....15
iOS Device User Assignments....16
Viewing Logs....17
File Archive....22
Client Certificates....22
iOS MDM Settings....25
Adding / Removing / Disabling Users....29

The Activity Monitor 30

Reporting 37

Using the Reports....38
Sample Reports....39

Managing Corporate Resources 42

Server and Network Configurations....43
Simple Certificate Enrollment Protocol (SCEP) Servers....46

Organization Control 49

Group E-mailing....49
Send Group E-mail....49
Search Group E-mail....50
File Share....51
Mobile Apps....53
Managing Mobile Apps for iOS 5 Devices....56

Accessing the Dashboard

Access the Dashboard

ZENworks Mobile Management dashboard requirements:

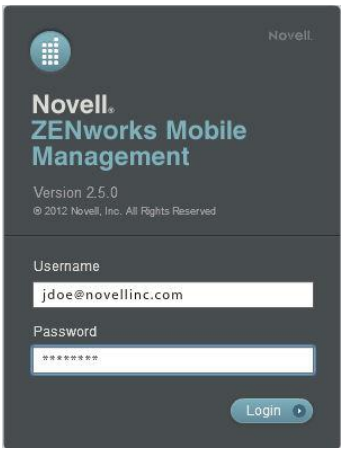
- Microsoft Internet Explorer or Firefox
- Adobe Flash Player 10.1.0
- Minimum screen resolution: 1024 x 768
- Desktop computer running Windows OS

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

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

Login

Log in to the *ZENworks Mobile Management* dashboard using the email address and password you designated as administrative login credentials when installing the *ZENworks Mobile Management Web/Http Server Component*.



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

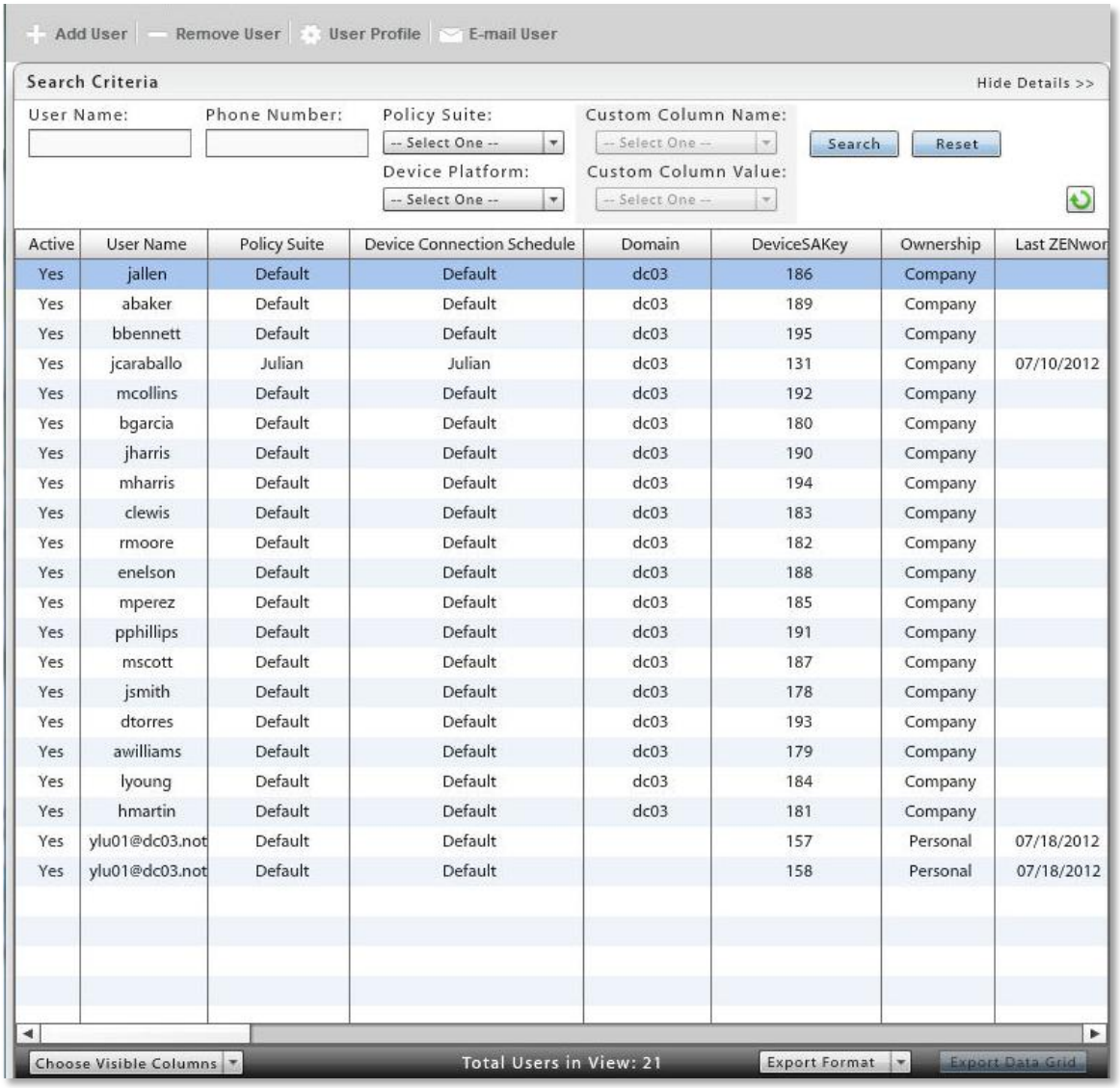
Managing Users

The Users View

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.

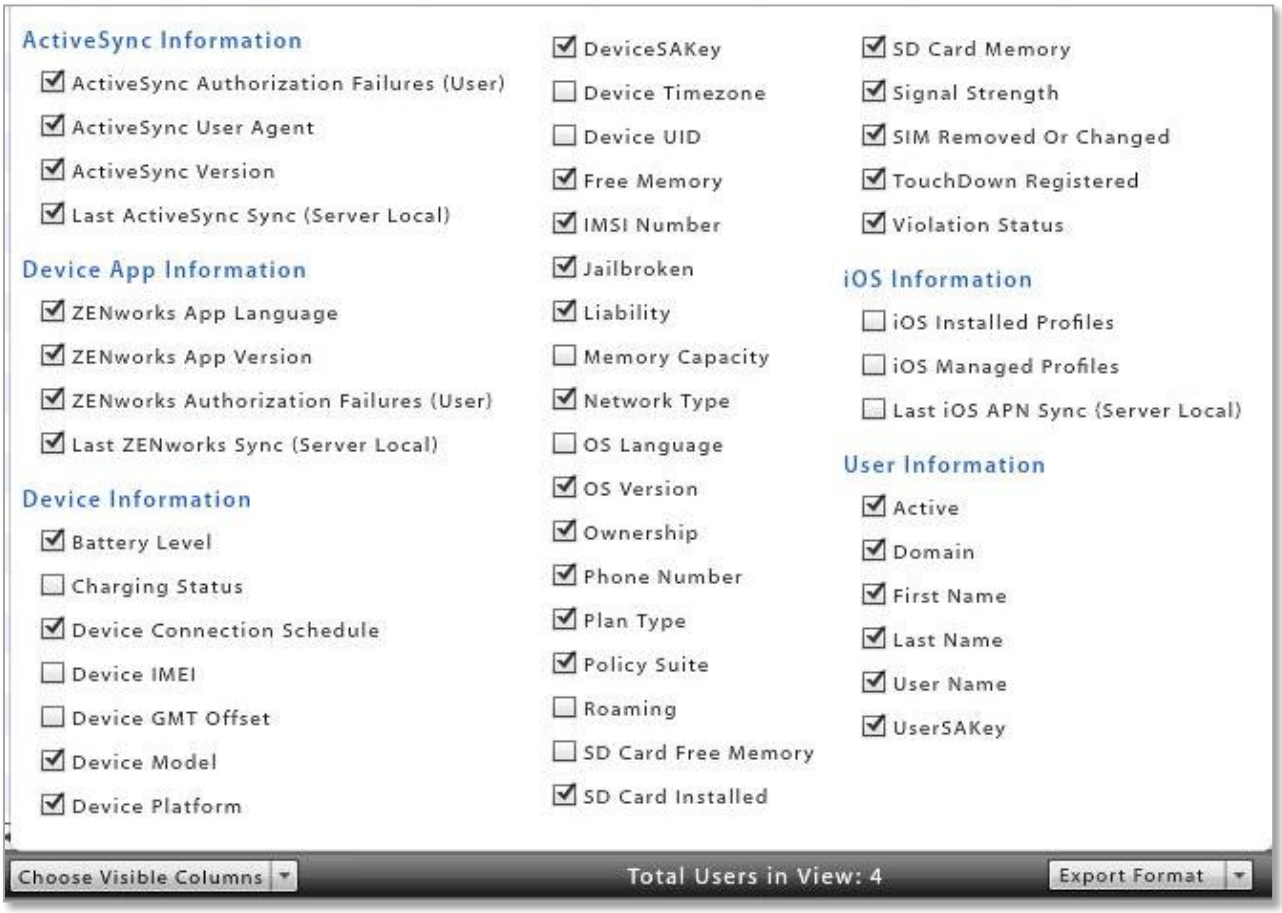


Customizing the User List View

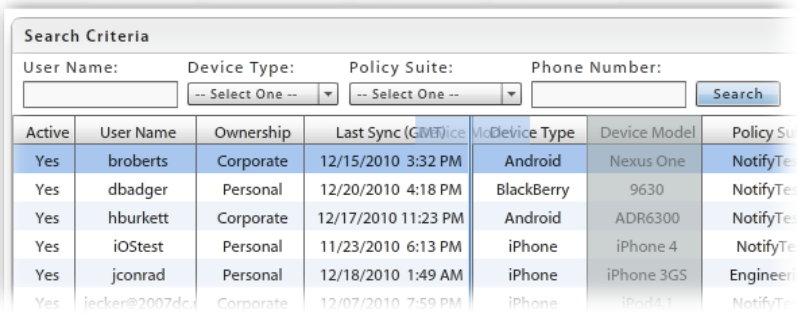
Customize the user list view by:

- Choosing the visible columns
- Rearranging columns
- Sorting columns
- Searching for and displaying a distinct group of users
- Hiding or revealing the user detail panel

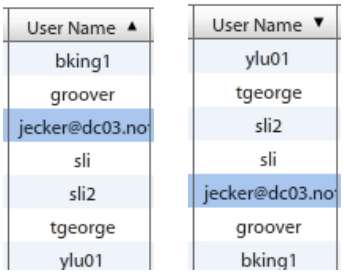
Choose the visible columns. Click the *Choose Visible Columns* button in the bottom left corner of the page and select or deselect the columns you want displayed or hidden. The dashboard saves the columns you choose to view.



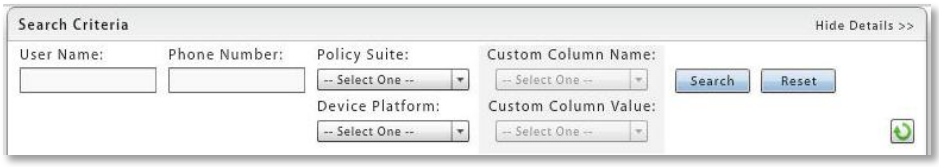
Rearrange columns. Drag and drop column headings to reorder the columns. The dashboard saves the order in which you arrange the columns.



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



Search for and display a single user or group of users. Use the search criteria above the grid to search for users by user name, phone number, policy suite, device platform, or custom column name and value. Wildcards entries, using an asterisk, are supported.



Hide or reveal the user detail panel. Click the ***Hide Details***/***Show Details*** button in the top right corner of the list to display or hide the user detail panel to the right of the user list.

Exporting Data from the List

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.

User Profiles

User Detail Panel

Select a user from the list. The detail panel for that user appears in a panel to the right of the list (click *Show Details* if the panel is not displayed.)

Panel Content

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

Device Compliance

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.

Administrative Action	Description	Result
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.
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.

Violation Details Pop-up

Remote Security Commands

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

The remote security commands are: *Full Wipe, Selective Wipe, Wipe Storage Card*, and *Lock Device*

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

When a security command is received and executed by the device, a confirmation email is sent to the user and administrator. Security commands that originate on an ActiveSync server are relayed to the device by *ZENworks Mobile Management*. In this instance, *ZENworks Mobile Management* does not send a confirmation because it might be duplicating similar notices from ActiveSync.

Security Command Functionality by Device

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

KEY

Anrd	Android devices	**S60**	Symbian S60 3rd edition devices
TD/A	*Android devices with TouchDown*	**WM**	Windows Mobile 6.1/6.5 devices
NS/BB	*NotifySync for BlackBerry*	**wOS**	webOS devices
iOS	iOS devices with multitasking capabilities	**WP7**	Windows Phone 7 devices

You may be able to perform some or all of the following actions based on the device type:

Action	Description	Devices Supported
Full Wipe	Administrators can issue a Full Wipe command. Functionality varies by device. *Android w/ native ActiveSync account (requires OS v2.2 or greater):* The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Does not erase the SD card. *Android w/TouchDown (requires OS v2.2 or greater):* The device returns to	***ZENworks Mobile Management* app:** Android, NS/BB, iOS, TD/A, WM, S60 **ActiveSync only:** wOS, WP7

	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 Selective Wipe. *BlackBerry*: Requires the *NotifySync for BlackBerry* application. Removes all mail and PIM data associated with the NotifySync application and removes the NotifySync account. Locks the device if *Require Password* is enabled. Erases NotifySync data from the SD card. *iOS*: The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. *Full Wipe* is applied immediately. *Symbian*: The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Some models (N95 and 6120c) wipe only *Mail for Exchange* data. Erases the SD card. *WM*: The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Erases the SD card only on Professional devices. *webOS and WP7:* 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.	
Selective Wipe	Administrators can issue a Selective Wipe command. Functionality varies by device. *Android w/ native ActiveSync account (requires OS v2.2 or greater):* Removes the ZENworks Mobile Management account information. *Android w/TouchDown (using any supported OS):* Removes all mail and PIM (calendar, contact, tasks) data associated with the TouchDown application and returns TouchDown to a pre-registration state. Erases TouchDown data from the SD card. Removes the ZENworks Mobile Management account information. *BlackBerry:* Requires the *NotifySync for BlackBerry* application. Removes all mail and PIM data associated with the NotifySync application, and locks the device if *Require Password* is enabled. *iOS*: Removes all mail and PIM (calendar and contacts) data controlled by ZENworks Mobile Management. *Selective Wipe* is applied immediately; however, the device is capable of postponing the action. *Symbian:* Removes the *ZENworks Mobile Management* account information.	***ZENworks Mobile Management* app:** Android, NS/BB, TD/A, S60, iOS
Wipe Storage Card	Remotely wipes all data from the device's storage card.	**ZENworks Mobile Management app:** Android, NS/BB, TD/A, WM
Lock Device	Remotely locks the device, requiring a password to be entered before the device can be used. *Android or Android w/TouchDown:* Requires OS v2.2 or greater. *iOS* allows for *Lock Device* to be applied immediately to iOS devices.	***ZENworks Mobile Management* app:** Android, NS/BB, TD/A, WM, iOS
Disable / Enable Device	Disables/ Enables device connection with the *ZENworks Mobile Management* server. (Turns a user's *Active* status off or on.)	***ZENworks Mobile Management* app:** Android, NS/BB,

		iOS, TD/A, WM, S60 **ActiveSync only:** 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.	***ZENworks Mobile Management* app:** NS/BB, TD/A
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

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.

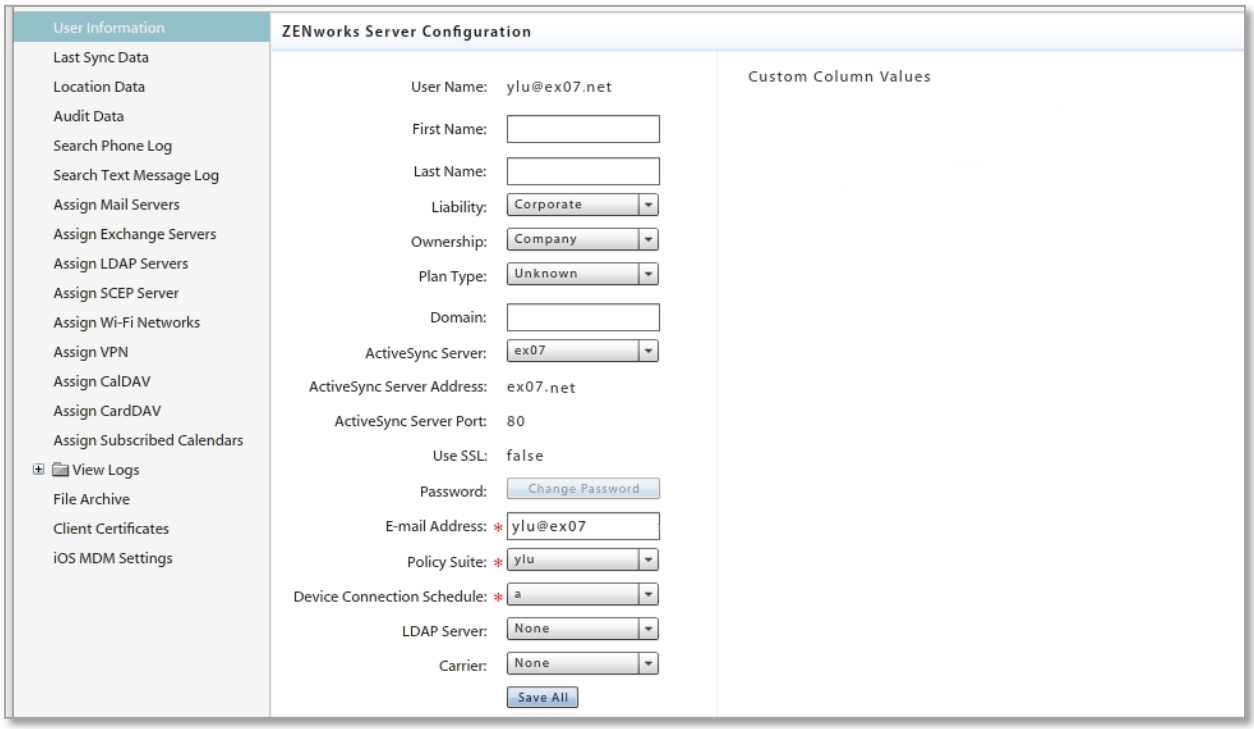
Password Recovery is supported with Exchange 2007 or 2010. It requires ActiveSync protocol 12.0 and 12.1.

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.

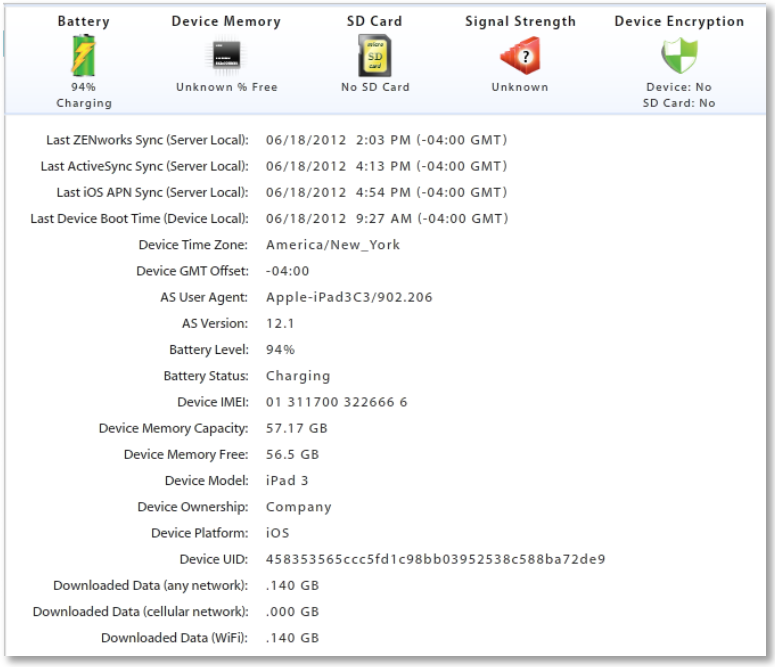
User Profile Views

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

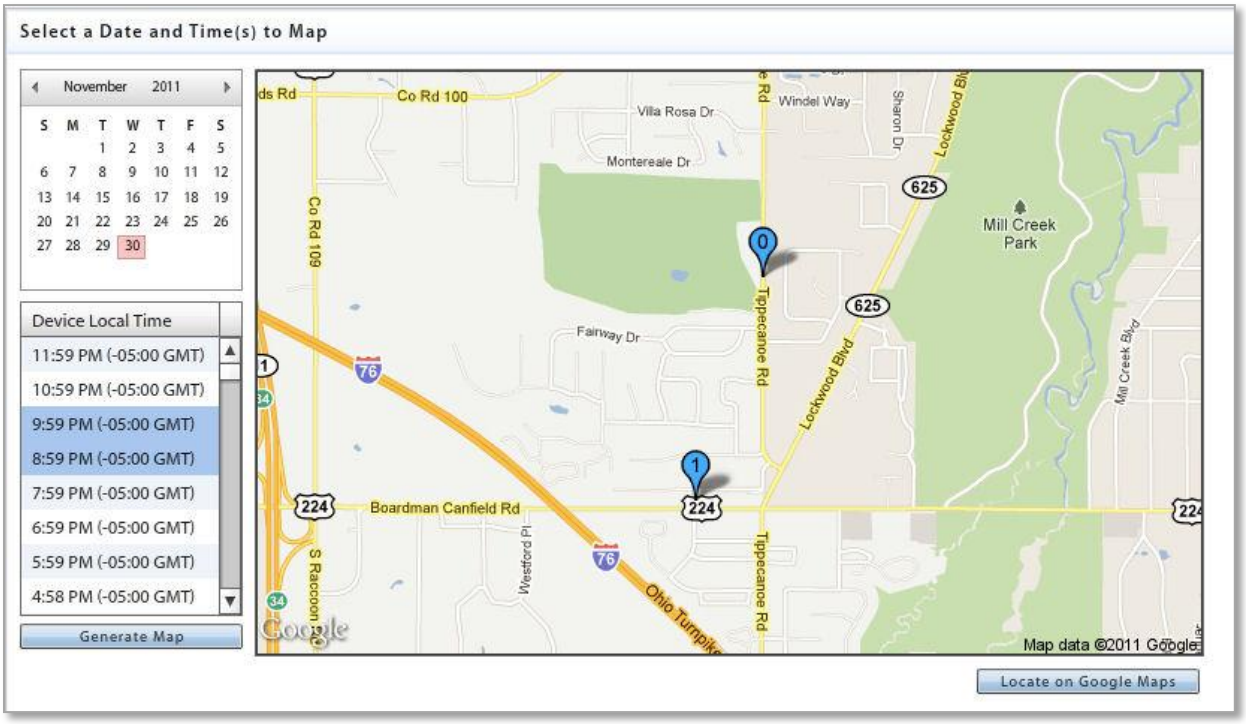
User Information. Select *User Information* from the left panel of the User Profile. This view displays basic user information that can be edited. In addition, server address information obtained by ActiveSync Autodiscover displays for users interfacing with servers using ActiveSync protocol version 12.0 or higher.



Last Sync Data. Select *Last Sync Data* from the left panel of the User Profile. This view displays the latest device statistics synchronized. The information available varies by device platform. If a device does not report a statistic, this view might display a zero (0), a blank space, or *Unknown*.

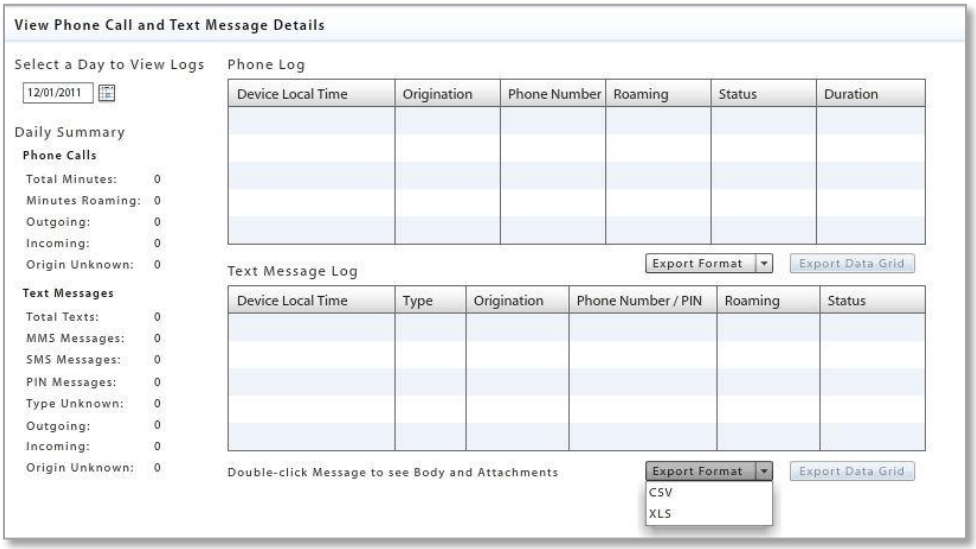


Location Data. Select *Location Data* from the left panel of the User Profile. This view gives the location of the device using GPS or triangulation on the device. Information is displayed using Google Maps. Select the date and times you want to view and click ***Generate Map*** (or double click the time to generate the map). Click the ***Locate on Google Maps*** button to view a single location in Google Maps.



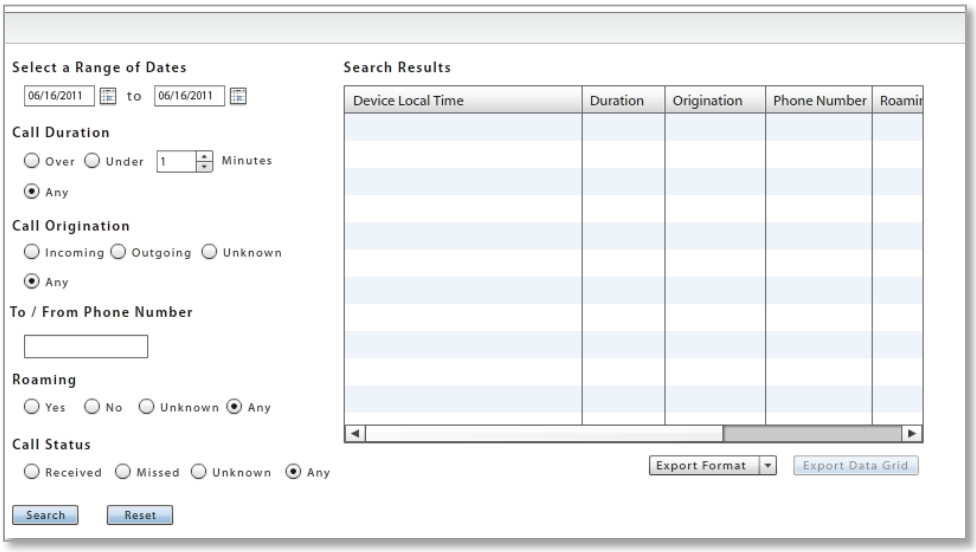
Audit Data. Select *Audit Data* from the left panel of the *User Profile*. This view displays phone and text message logs synchronized from the device. Select the day you want to view. Double-click a text message record to view the body of text in the message with any attachments that were sent or received.

The *Phone Log* or the *Text Message Log* can be exported to a CSV or XLS file.

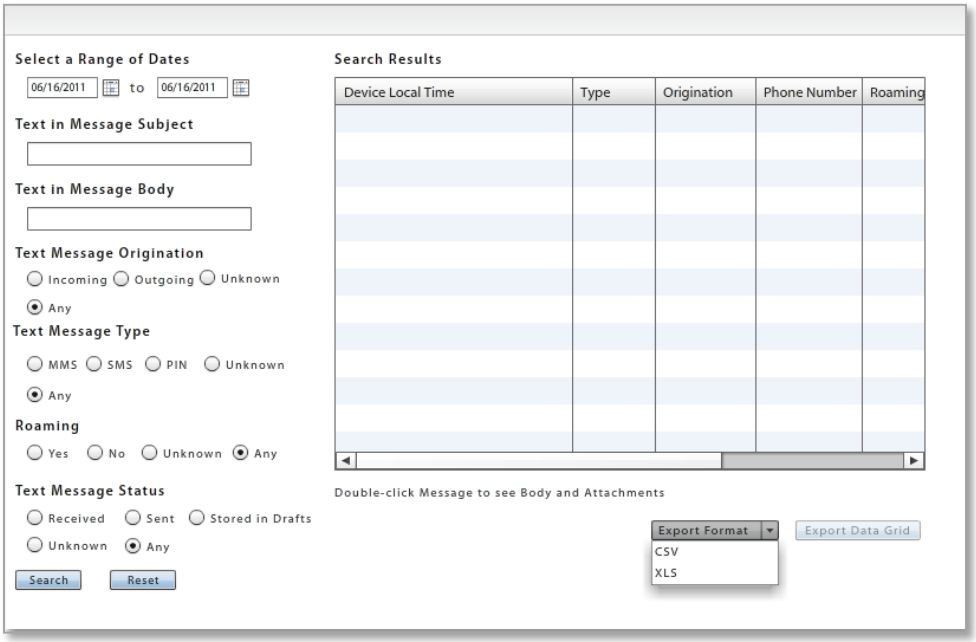


Searching Phone and Text Logs

Search Phone Log. Select *Search Phone Log* from the left panel of the *User Profile*. This view allows you to search the phone logs by date/time, call duration, call origination, To/From phone number, roaming status, or call status. The search results can be exported to a CSV or XLS file.



Search Text Message Log. Select *Search Text Message Log* from the left panel of the *User Profile*. This view allows you to search the text message logs by date/time, text in the message subject or body, message origination, message type, roaming status, or message status. The search results can be exported to a CSV or XLS file.

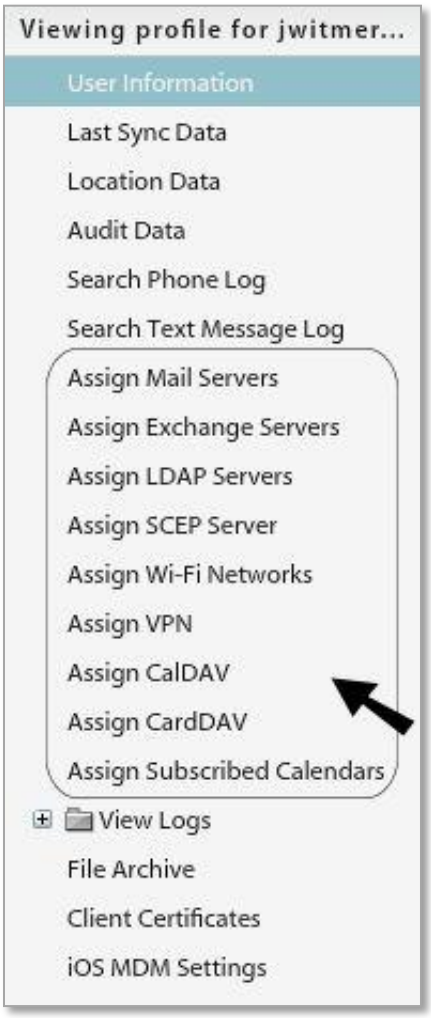


iOS Device User Assignments

You can associate iOS device users with servers or networks in the enterprise system and configure user account settings to push out to devices.

Credentials for these server and network resources can be defined from the *Organization* view.

Select the assignment options from the left panel of the *User Profile*.



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

Assign 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.

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

Assign 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.

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

Assign VPN. Associate the user with a VPN Network and define the network credentials to push out to the user's device. *Note: Current functionality: IPSec (Cisco protocol)*

Assign CalDAV. Associate the user with a CalDAV server and configure calendar account settings (username, password, and principal address) to push out to the user's device.

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

Assign 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.

Assign Mail Servers and ***Assign Exchange Servers*** have two options that can be enabled/disabled to govern how the mail account can be used by an iOS 5+ user.

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

  This prevents messages created outside of the device's native *Mail* application from being sent from the corporate account. For example, if the user sends a photo from the device *Photo* application, it is

not be sent from the corporate mail account; nor can the user send an attached contact file from the device's *Contacts* application using the corporate mail account.

Viewing Logs

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.

To view the logs associated with a user's device:

Select the **Users** view. Double-click on the user you want to view.

Select **View Logs** from the left panel of the *User Profile* view. Choose one of the logs.

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

Synchronization Logs

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

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

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

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

The logs display:

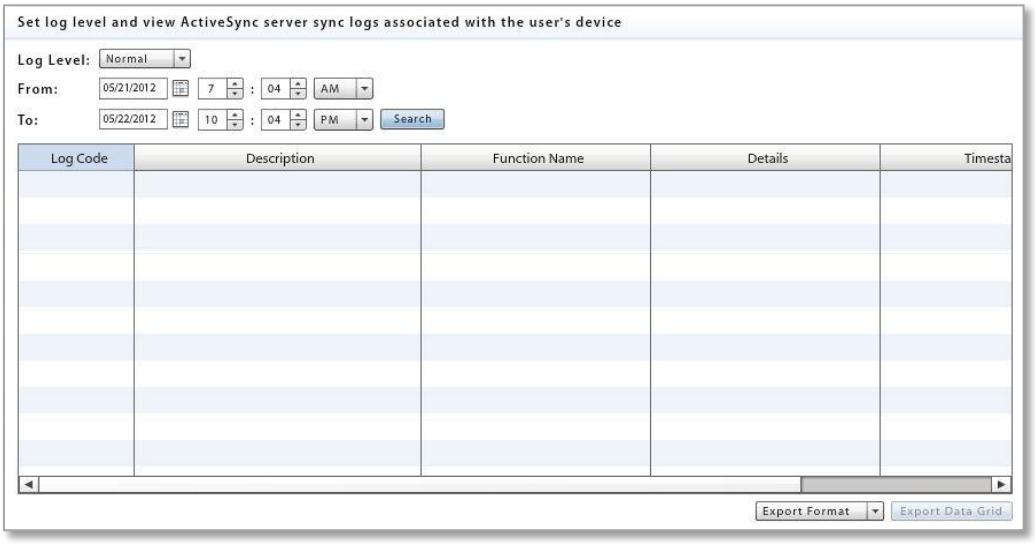
- Log code – Code number associated with the logged event
- Description – Description of the log event
- Function Name – Displays a returned error; blank when log event is successful
- Details – Description or reason for the error; blank when log event is successful
- Time stamp – Date and time of the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

Select ***ActiveSync Log***, ***ZENworks Sync Log***, or ***iOS MDM Sync Log***.

The **Log Level** defaults to **Normal** and the log populates the grid with data from the past hour.

If you change the log level to **Verbose** or edit the **From/To** filter, click **Search**.
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.

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.



Sample Server 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.

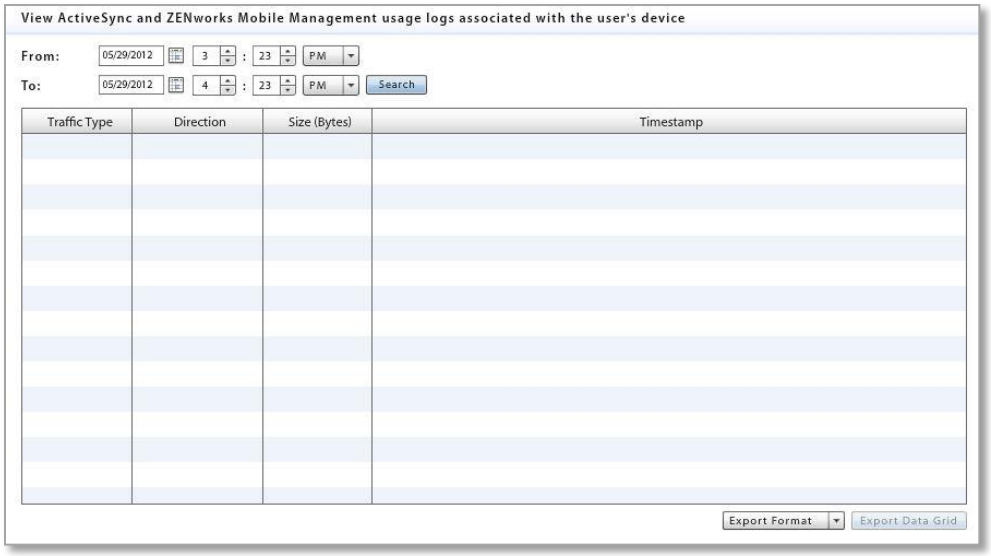
The log displays:

- 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*** the left panel of the *User Profile* view.

The log populates the grid with data from the past hour. If you edit the **From/To** filter, click **Search**.
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.

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



Device Logs

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

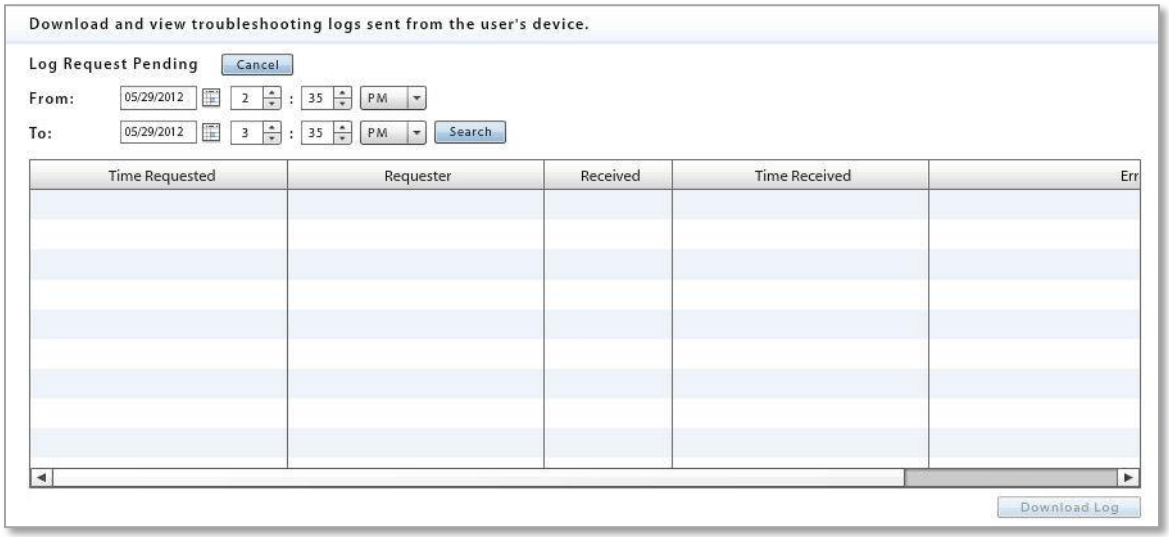
Device Type	Device Requirements / Behavior
Android	The device sends only the logcat log to the dashboard. *ZENworks* logging must be enabled on the device (*Log Settings*). The *ZENworks* log is written to the SD card.
BlackBerry (with *NotifySync*)	BlackBerry devices must have logging enabled on the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

Select ***Device Log*** from the left panel of the *User Profile* view.

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



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*.

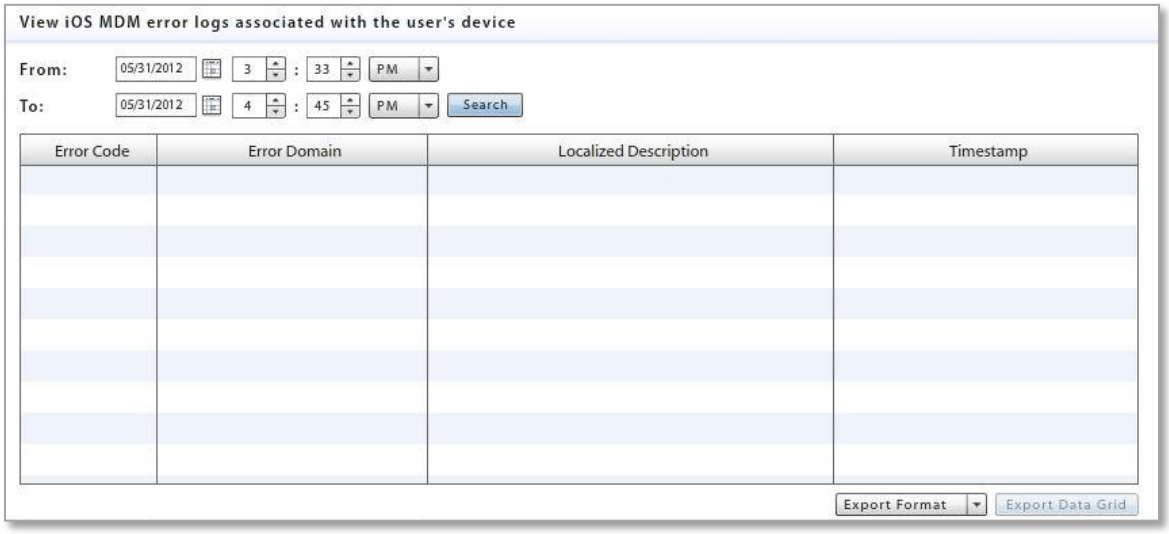
The log displays:

- 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 Usage Log* from the left panel of the *User Profile* view.

The log populates the grid with data from the past hour. If you edit the **From/To** filter, click **Search**. 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.

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.



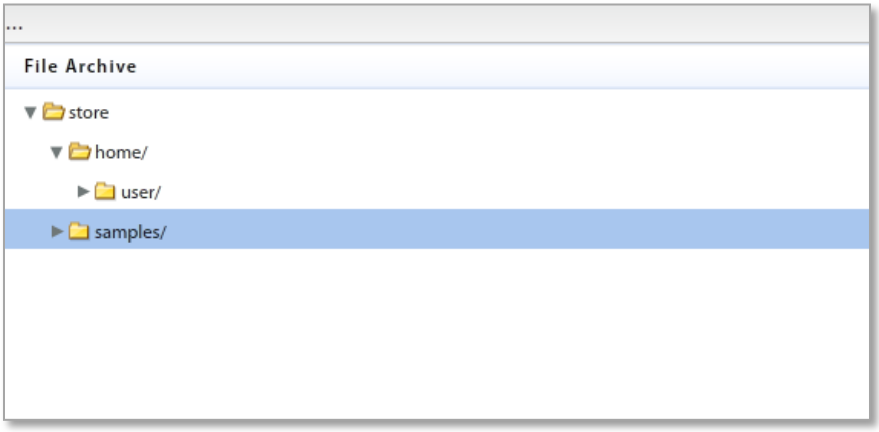
Error Chain Log Grid

File Archive

The File Archive is a display of the file list sent up from the device when the *Archive files on device* policy rule is enabled. When the rule is enabled, the device periodically sends a list of all folders and files stored on the device and the SD card, to the server. Administrators can view the list here.

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

Select ***File Archive*** from the left panel of the *User Profile*.



Client Certificates

Client Certificates provides a method for you to deploy client authentication certificates to user devices. A certificate can be uploaded to the *ZENworks Mobile Management* server from the dashboard 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 by 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.

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.

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.

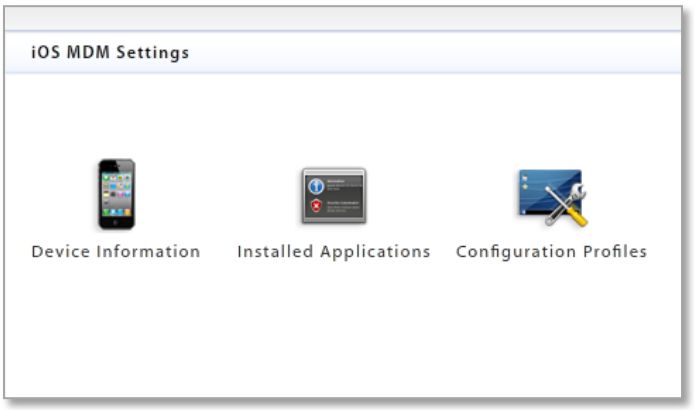
To upload a certificate file:

1. Select ***Client Certificates*** from the left panel of the *User Profile*.
2. Select the ***Upload*** button to browse and select the certificate file.
3. Highlight the certificate and select the ***Use This Certificate*** check box.
4. If the certificate is protected by a password, enter the ***Password*** and confirm it.

Certificate Formats Supported on Various Device Platforms		
	.cer	**.pfx / .p12**
Android	OS 2.1 update 1	
	OS 2.2	OS 2.2
	OS 2.3	OS 2.3
	OS 2.3.4	OS 2.3.4
BlackBerry (with *NotifySync*)	OS 4.5	
	OS 4.6	
	OS 5.0	
	OS 6.0	OS 6.0
	OS 7.0	OS 7.0
iOS	iOS 4.1	iOS 4.1
	iOS 4.3.5	iOS 4.3.5
	iOS 5	iOS 5
Symbian	OS 9.1	OS 9.1
	OS 9.2	OS 9.2
Windows Mobile	OS 6.1 Standard	OS 6.1 Standard
	OS 6.1 Professional	OS 6.1 Professional
	OS 6.5 Professional	OS 6.5 Professional

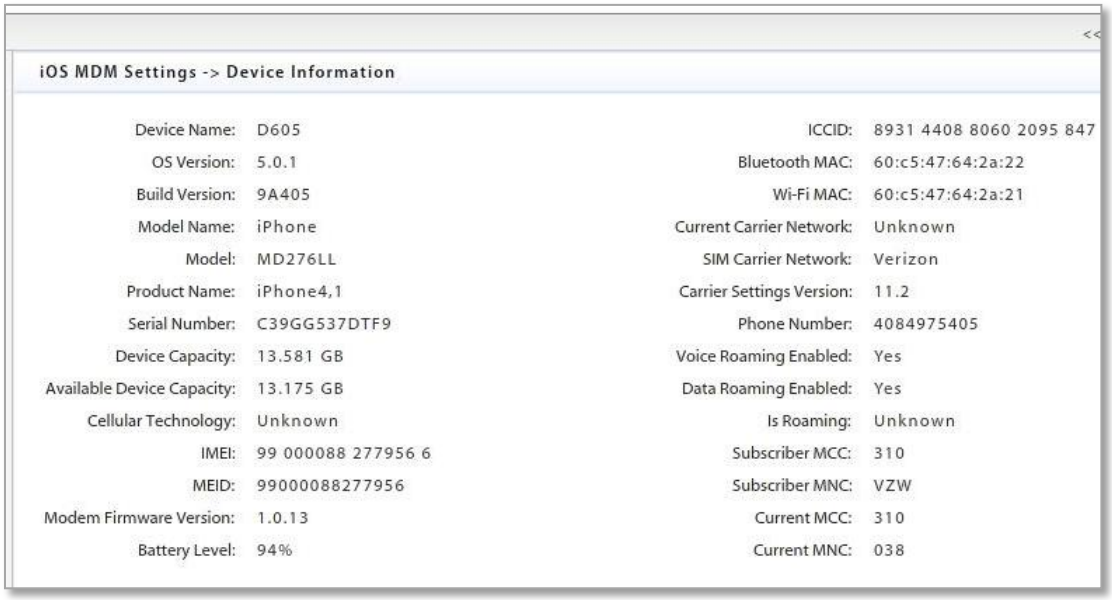
iOS MDM Settings

Select ***iOS MDM Settings*** from the left panel of the *User Profile*.

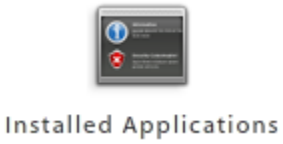


Device Information

Select the **Device Information** icon to view device and network statistics for the iOS device.



Installed Applications



Select the Installed Applications icon to view a list of applications installed on the user's device and to manage mobile apps for iOS 5 users.

The *Installed Apps* grid is updated when the device uploads a list of all applications on the device.

The grid is only updated if the *Record Installed Applications* policy rule is enabled on the policy suite with which the user is associated.

The *Managed Apps* grid is only available for iOS 5 user. It lists the mobile apps available to an iOS 5 user as determined by the *Mobile App Permissions* and allows the administrator to manage (install, uninstall, etc.) the apps listed here.

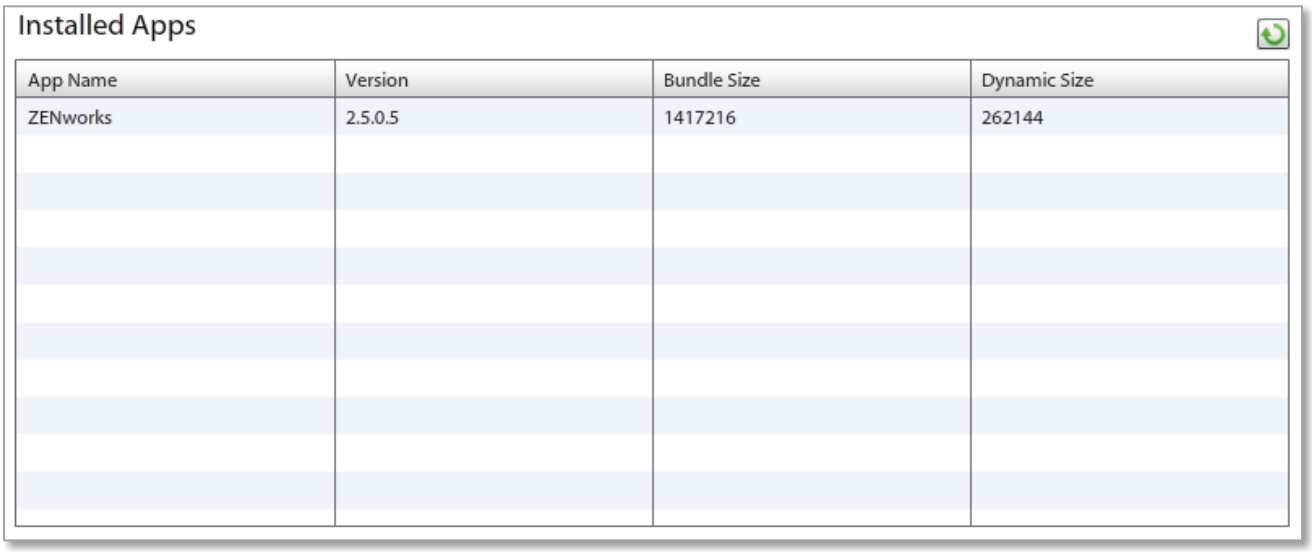
Ability to manage the user's apps here requires that the *Manage Mobile Apps* policy rule be enabled on the policy suite with which the user is associated.

Policies That Control Installed Applications

The ***Record Installed Applications*** and ***Manage Mobile Apps*** policy rules are located in the ***iOS Device: iOS MDM*** category of each policy suite.

The Installed Apps Grid

The *Installed Apps* grid lists all non-system applications that have been installed on an iOS 4 or iOS 5 device. The list is only updated if the policy suite with which the user is associated has the *Record Installed Application* policy enabled.



The Managed Apps Grid

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

If the user's policy suite also has the *Manage Mobile Apps* policy enabled, an administrator can use the option buttons below the grid to install, reinstall, or uninstall an app on the user's device. Administrators can also remove an invalid Redemption Code for a Volume Purchase Program (VPP) app.

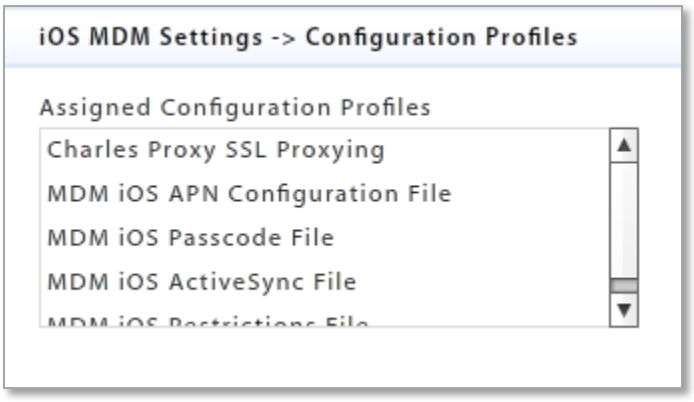
A managed app is one that has been installed on the device through MDM by either the user, an administrator, or by a forced push of the application. Applications that are not installed through MDM or those already existing on the device before the app was made available through MDM cannot be managed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

Using the Information in the Managed Apps Grid

Status	The most common status messages include: • *Managed* – Indicates that the app is installed on the device • *Not Installed via MDM* – Indicates that the app is available through *ZENworks Mobile Management*, but is not required and has not been installed by *ZENworks*. • *Managed, but Uninstalled* – Indicates an app that is not installed; possibly because it was removed by the user or is not required. Other status messages give additional information about apps on the device.
Rejection Reason	If the app is not installed, look here to see if installation of the app was attempted and why it was rejected.
Remove with MDM	Whether this app is removed, along with its data, if the MDM profile is removed.
Prevent Backup	Whether the user is prevented from backing up this app via iTunes.
Redemption Code	The redemption code associated with a Volume Purchase Program (VPP) app.
Timestamp	Last update of the app's status.

Configuration Profiles

Select the **Configuration Profiles** icon to view the assigned configuration profiles on the user's device. The device periodically sends a list of all profiles assigned to the device. Administrators can view the list here.

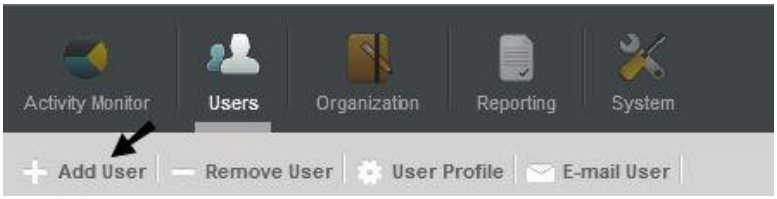


Adding / Removing / Disabling Users

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).

Users imported in a batch are assigned the same policy suite, device connection schedule, ActiveSync server (if defined), LDAP server (if defined), and carrier (if desired).

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 detail 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.

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:

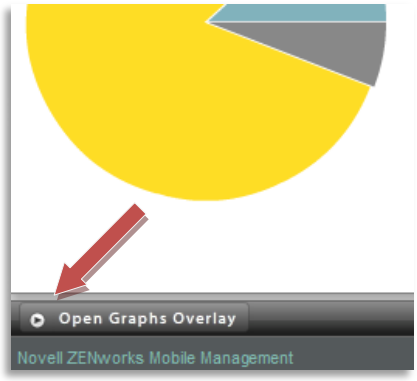
Active/Inactive Devices	Pie chart showing the percentage of active devices versus disabled devices.
Device Activation/De-Activation History	Bar chart showing the number of devices activated and deactivated in the past seven days.
Devices by AS Authorization Failure	Pie chart showing the percentage of devices passing invalid credentials for the ActiveSync accounts of known users to the server.
Devices by AS Version	Pie chart showing the percentage of devices operating with various ActiveSync protocol versions.
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 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 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 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 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 ZENworks App Language	Pie chart showing the percentage of devices by their language setting.
Devices by ZENworks App Version	Pie chart showing the percentage of devices by the version of the *ZENworks Mobile Management* app installed.
Devices by ZENworks Authorization Failure	Pie chart showing the percentage of devices passing invalid credentials for the *ZENworks Mobile Management* accounts of known users to the server.
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 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 Policy	Pie chart showing the percentage of devices operating under each policy suite.
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.

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.

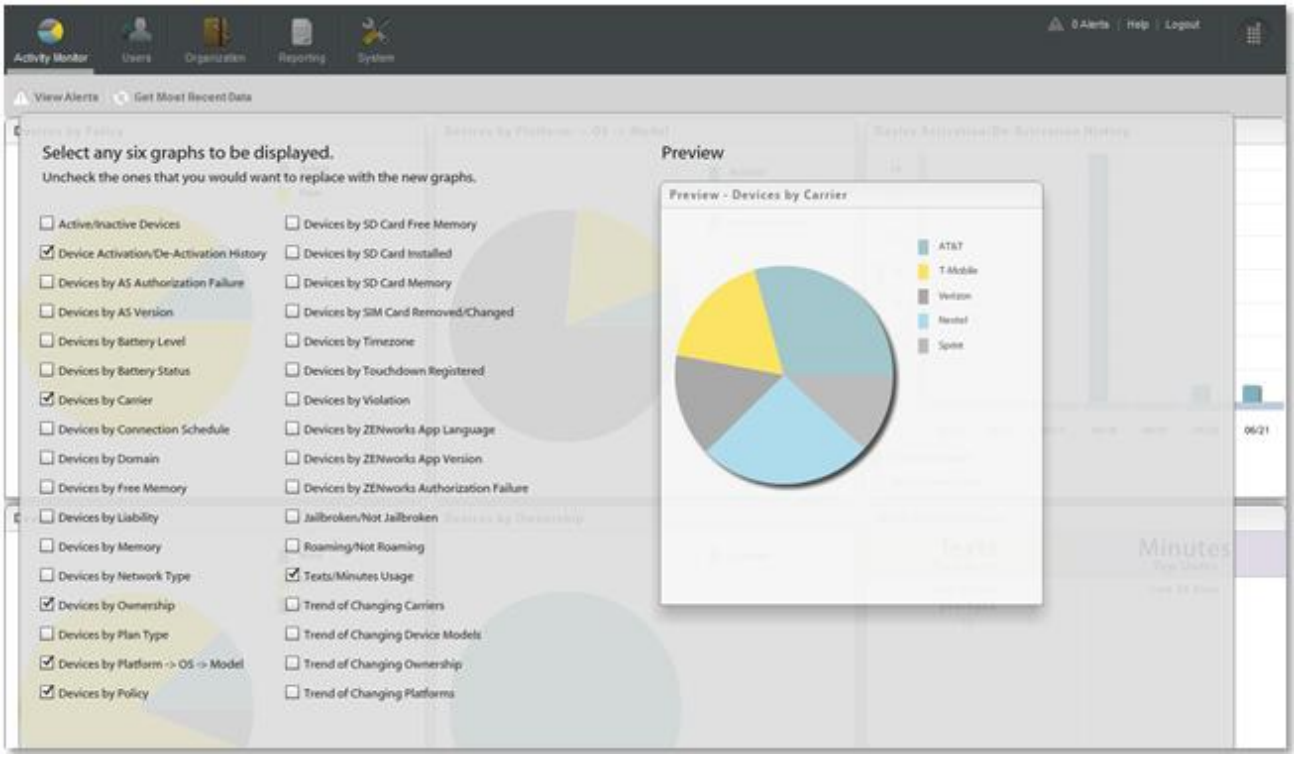
Select Graphs. Click the *Open Graphs Overlay* button at the bottom left corner of the Activity Monitor screen. Select the six graphs you want to display on the grid.

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



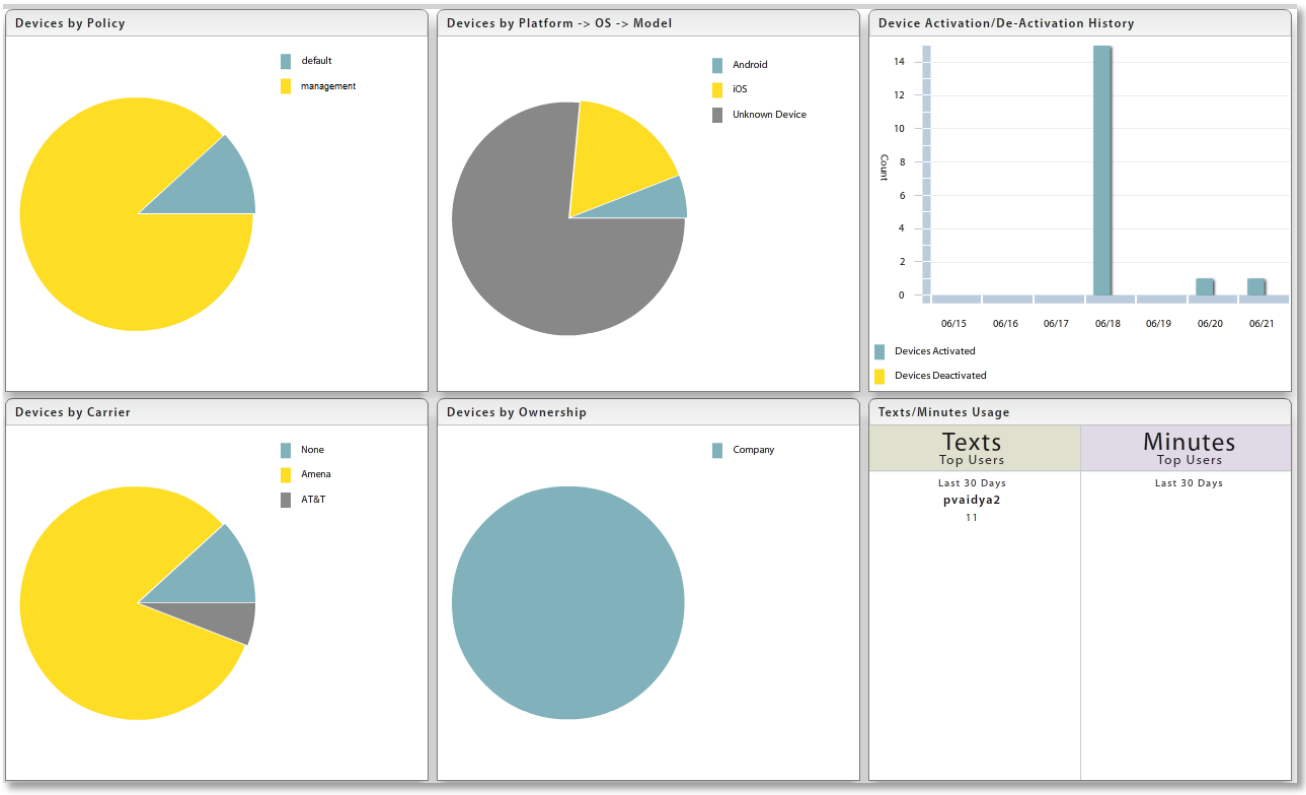
When selecting the graphs, a preview screen appears in a panel to the right. The information in the chart preview is sample data.

The Activity Monitor grid always displays six graphs. If fewer are chosen, a warning appears indicating that the most recently deselected graphs will display along with your choices. If you attempt to exit the Overlay screen with more than six graphs selected, a pop-up message reminds you to deselect one or more of the previously selected graphs.

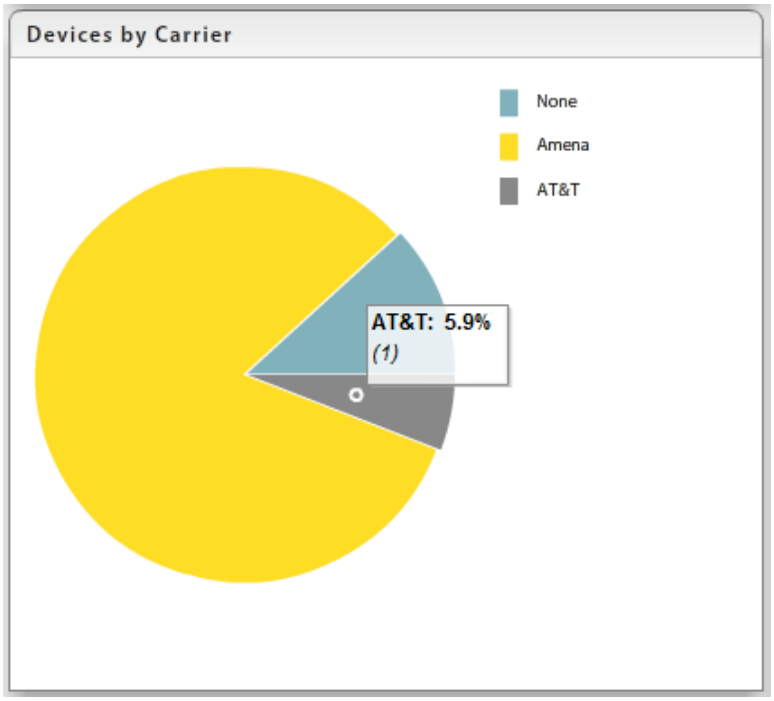


Click the *Close Graphs Overlay* button when your selections are complete.

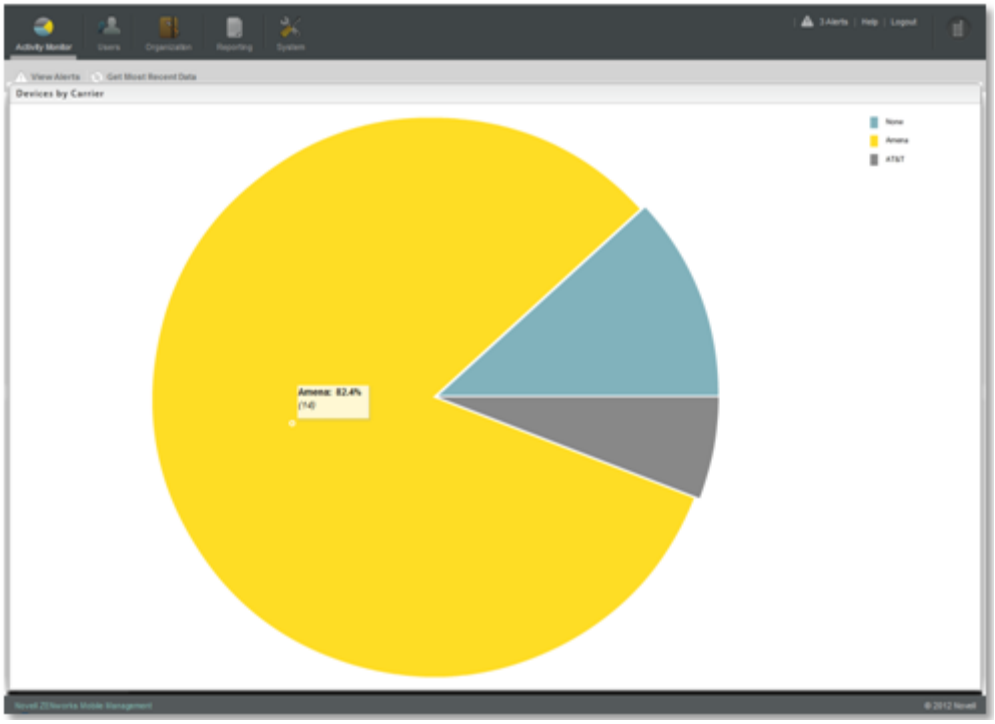
Rearrange Panels. You can rearrange the panels in the view by selecting a block and dragging it and dropping it where you prefer.



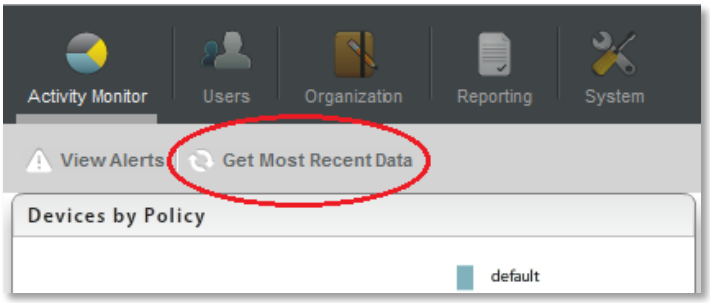
View Details. You can see detail of the statistics by hovering over a section of a graph or chart.



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.

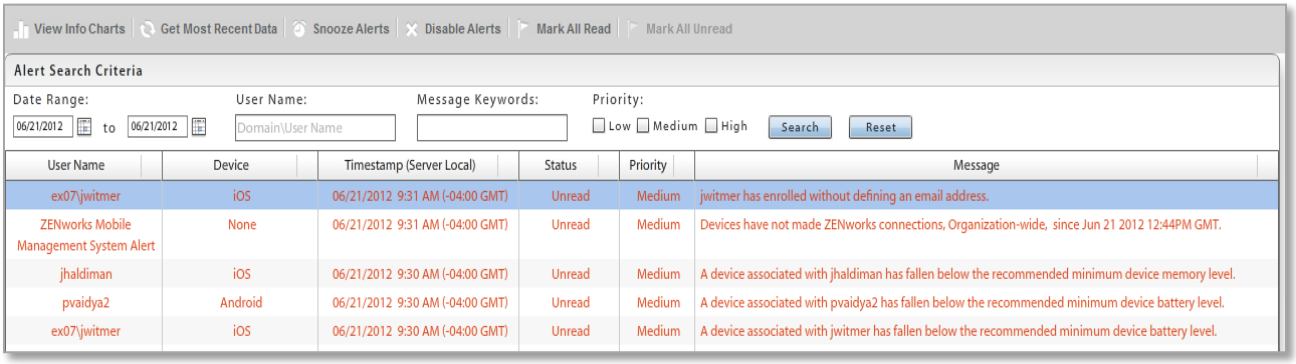


Refresh the View. You can refresh the Activity Monitor view with the most recent data by selecting *Get Most Recent Data* in the gray option bar.

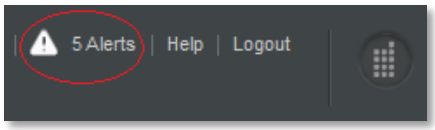


Flip to the *View Alerts* Grid. You can flip the Activity Monitor view to a table of alerts listed by user. Select ***View Alerts*** in the option bar. Select ***View Info Charts*** to return to the Activity Monitor view.

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.

Reporting

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

The reports are as follows:

Device Reports

- **Devices by Liability**
- **Devices by Network Type**
- **Device by OS Version and Model**
- **Device by OS Version and Platform**
- **Devices by Platform**
- **Devices by Platform and Model**
- **Devices by Policy Suite**
- **Data Usage by DeviceSAKey**

User Reports

- **Users by Carrier**
- **Users by Ownership**

Compliance Reports

- **Access Restriction Violations**
- **Device Platform Restrictions by User**
- **Exceptions by User**
- **Resource Restrictions by User**
- **User by Exceptions**

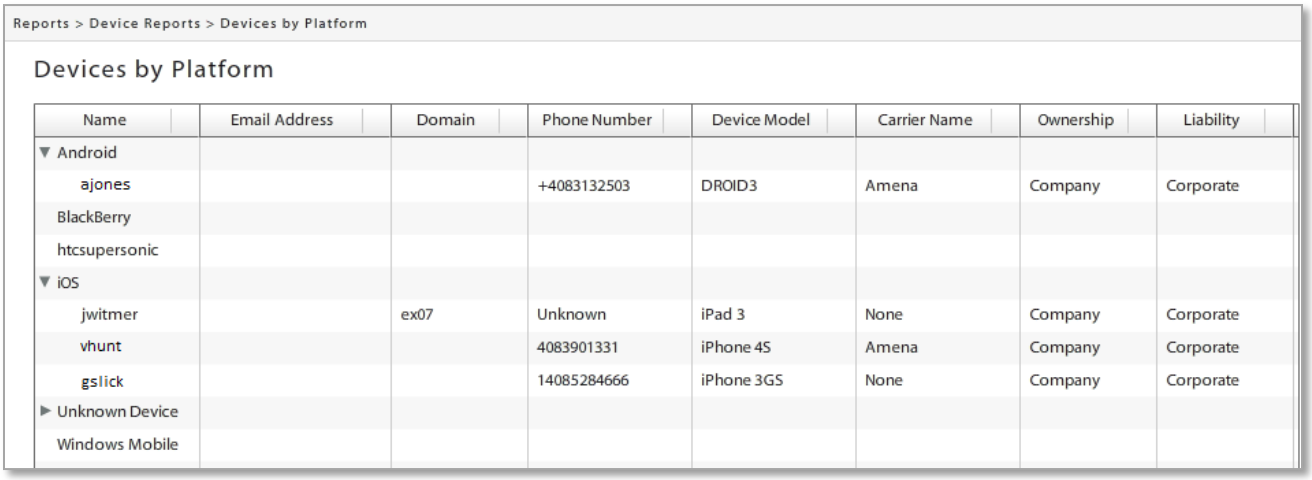
Administrative Roles Reports

- **Organization Administrators**
- **Organization Roles**
- **System Administrators**
- **System Roles**

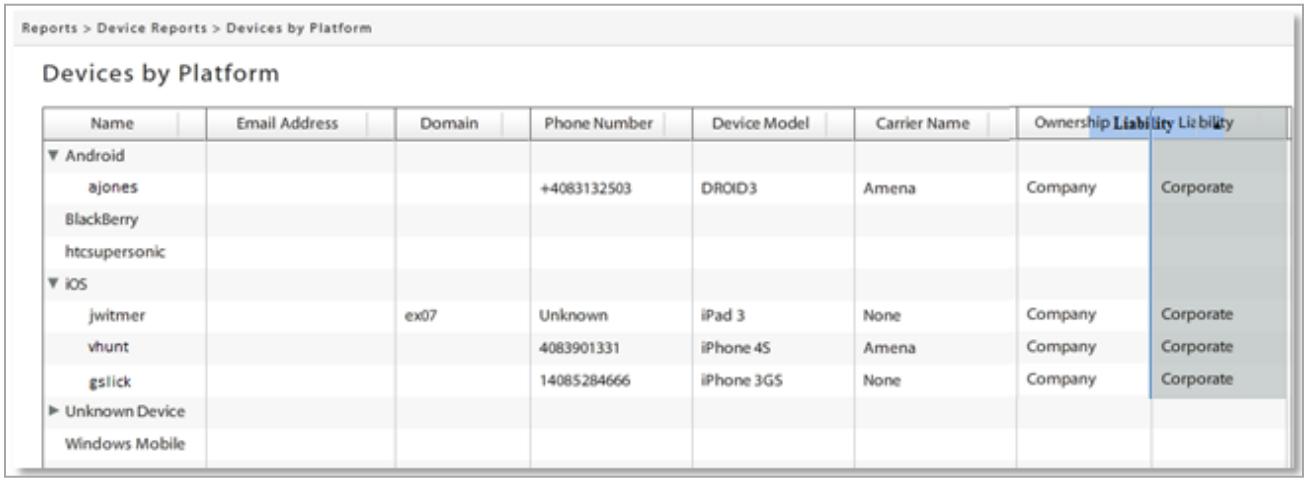
Using the Reports

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.



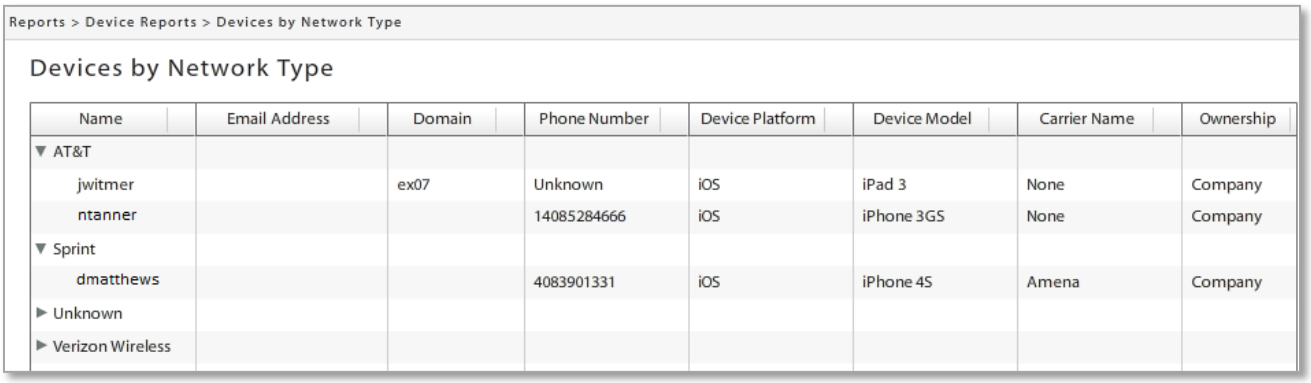
Export Report Data. Export data from the report to a comma separated values (CSV) or Excel (XLS) file. Choose the ***Export Format***, then click the ***Export Report*** button to save the current report to a file.

Sample Reports

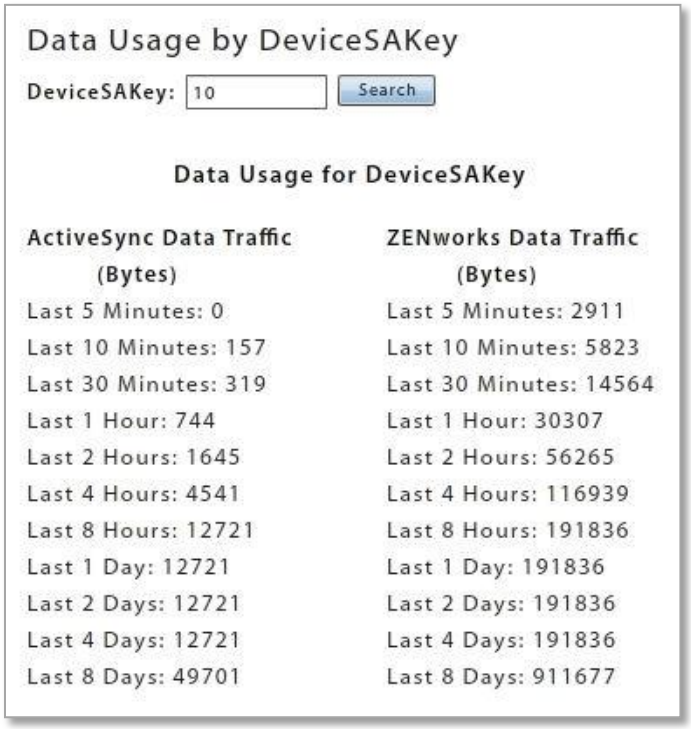
Sample Device/User Reports

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



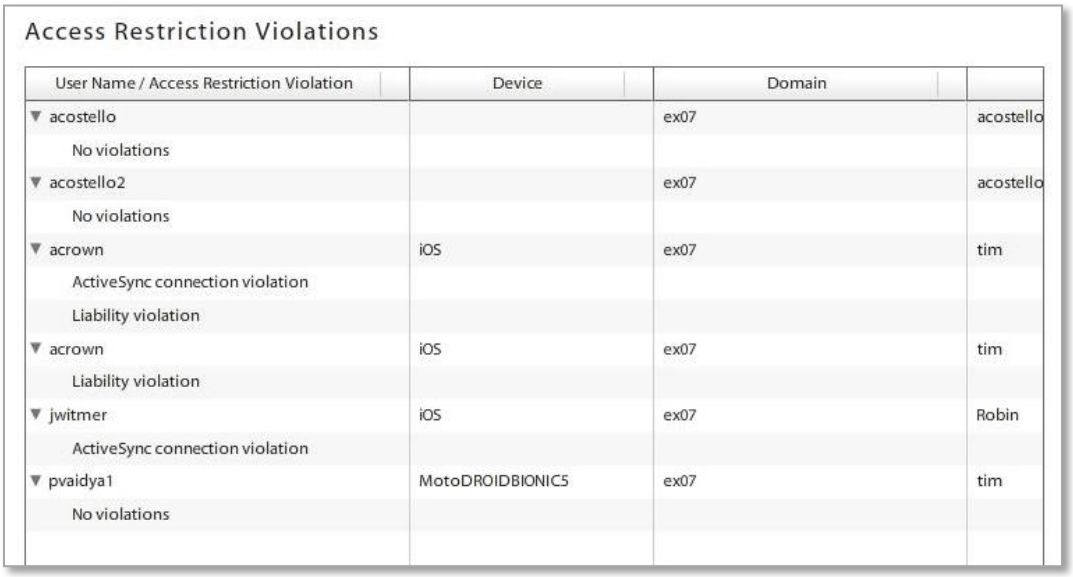
Name	Email Address	Domain	Phone Number	Device Platform	Device Model	Carrier Name	Ownership
▼ AT&T							
jwitmer		ex07	Unknown	iOS	iPad 3	None	Company
ntanner			14085284666	iOS	iPhone 3GS	None	Company
▼ Sprint							
dmatthews			4083901331	iOS	iPhone 4S	Amena	Company
▶ Unknown							
▶ Verizon Wireless							



Sample Compliance Report

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

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



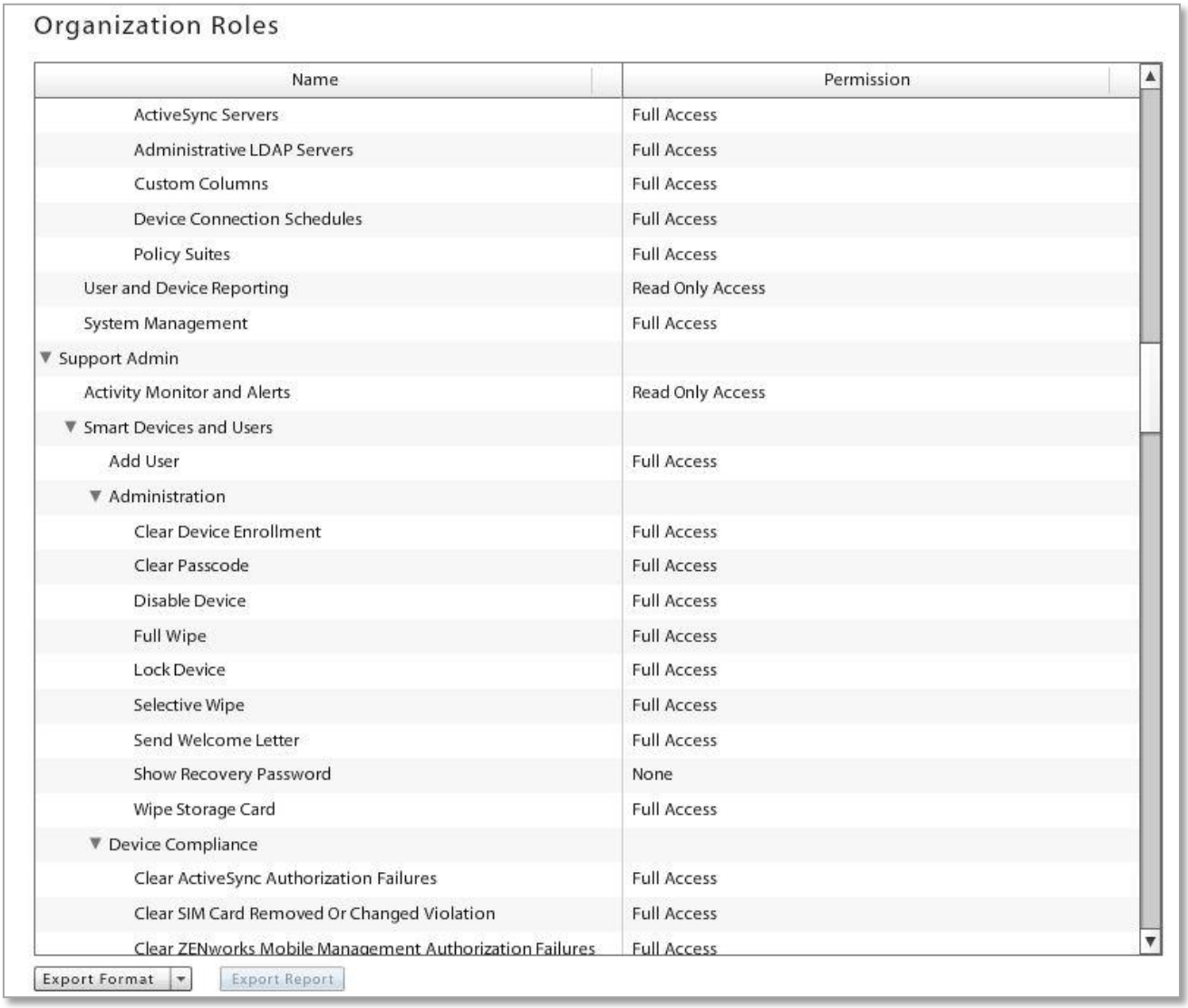
Access Restriction Violations

User Name / Access Restriction Violation	Device	Domain	
▼ acostello		ex07	acostello
No violations			
▼ acostello2		ex07	acostello
No violations			
▼ acrown	iOS	ex07	tim
ActiveSync connection violation			
Liability violation			
▼ acrown	iOS	ex07	tim
Liability violation			
▼ jwitmer	iOS	ex07	Robin
ActiveSync connection violation			
▼ pvaidya1	MotoDROIDBIONIC5	ex07	tim
No violations			

Sample Administrative Roles Report

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

- Administrator Name
- Administrative Role Name
- Permissions



Managing Corporate Resources

Corporate Resources refers to the servers and networks to which users have access, such as LDAP and mail servers or Wi-Fi and VPN networks.

Use this group of tools to define credentials for the server and network resources. Then use the resources in the ***Users*** view to associate **iOS device users** with a server or network and configure user account settings to push out to devices.

Assignments in the User Profile panel

*When servers and networks are defined, select a user from the **Users** grid. Then use the assignment options in the **User Profile** view to associate iOS device users with a server, network, or service.*

Server and Network Configurations

You can define the following servers and networks:

Server or Network	Description
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.
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.
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.
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.
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.
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.
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.
VPNs	Define your VPN networks. Then associate a user with the VPN network and define the wireless network credentials to push out to the user's device. Current Functionality: IPSec (Cisco protocol)
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.

Distinguishing between Resource LDAP Servers and Administrative LDAP Servers

LDAP servers defined here are for the purpose of configuring LDAP settings to make available to iOS device users. When users synchronize the settings, the device is automatically enabled for accessing corporate directory information.

Administrative LDAP servers defined under *User Account Settings* are for the purpose of adding users in batches, importing user information into custom column fields, and authenticating administrators via an LDAP server.

Server Credentials

The credentials for each server and network are defined by using a wizard:

Mail Servers

-Email Server Type

-Account Name

-Server Address

-Server Port

-Use SSL

-Account Type

-IMAP Path Prefix

-Authentication Type

Exchange Servers

-Exchange Server Name

-Exchange Server Address

-Exchange Port

-Use SSL

-Use S/MIME (iOS 5+)

LDAP Servers

-LDAP Display Name

-LDAP Server Address

-LDAP Port

-Use SSL

CalDAV Servers

-Display Name

-Server Address

-Server Port

-Use SSL

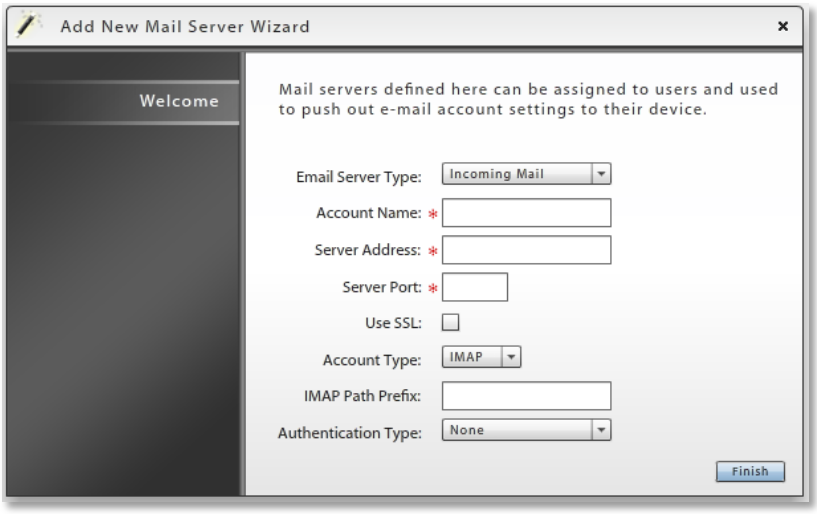
CardDAV Servers

-Display Name

-Server Address

-Server Port

-Use SSL



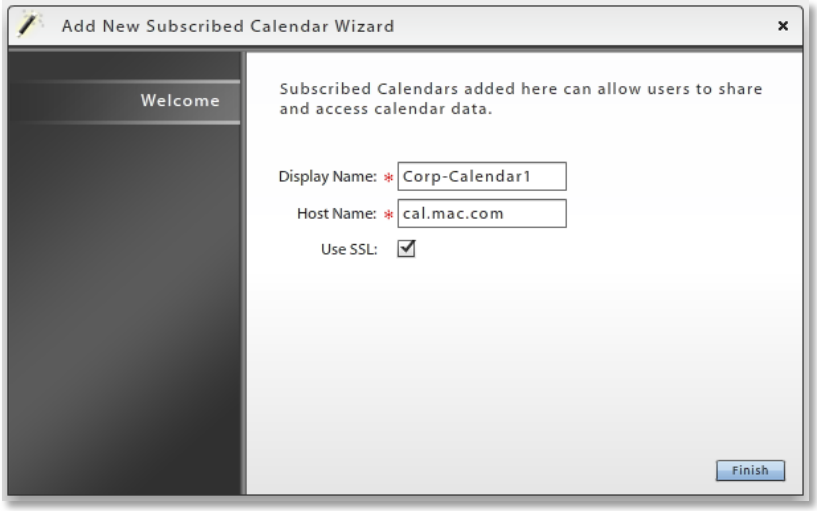
Sample Add New Server Wizard

Subscribed Calendars

-Display Name

-Host Name

-Use SSL



Add New Subscribed Calendar Wizard

Network Credentials

Wi-Fi Networks

-Network Name

-SSID

-Auto Join (iOS 5+)

-Hidden Network

-Security Type

-Password

-Password Per Connection

-Accepted EAP Types

-EAP-FAST

-Allow Trust Exceptions

-Inner Identity

VPNs

-Display Name

-Remote Address

-Group Name

-Shared Secret

-Proxy Type

-Proxy Address

-Proxy Port

-Proxy Username

-Proxy Password

Sample Add New Network Wizard

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 ***Client Certificates***.

SCEP Servers and the ZENworks Mobile Management System

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

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

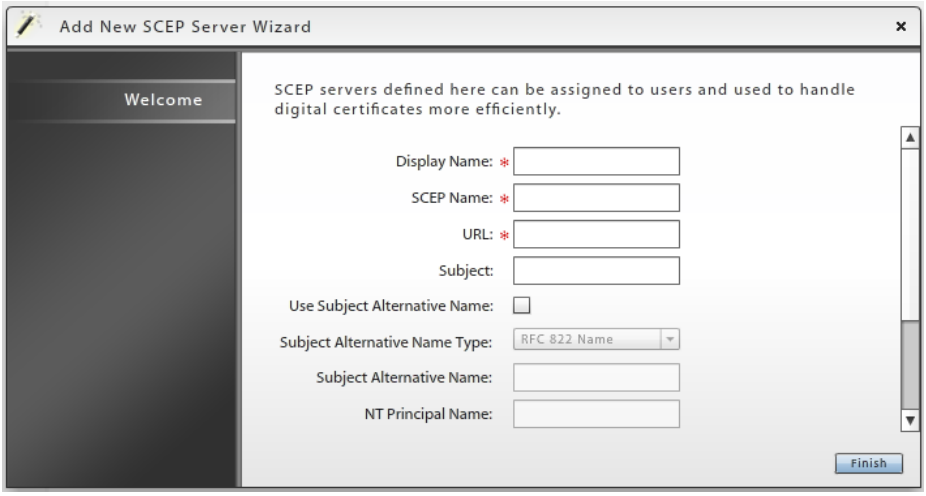
The initial configuration profile that the user accepts contains the address of the SCEP server. The device connects with both the *ZENworks Mobile Management* and SCEP servers to complete several configuration steps:

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

Define a SCEP Server

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

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



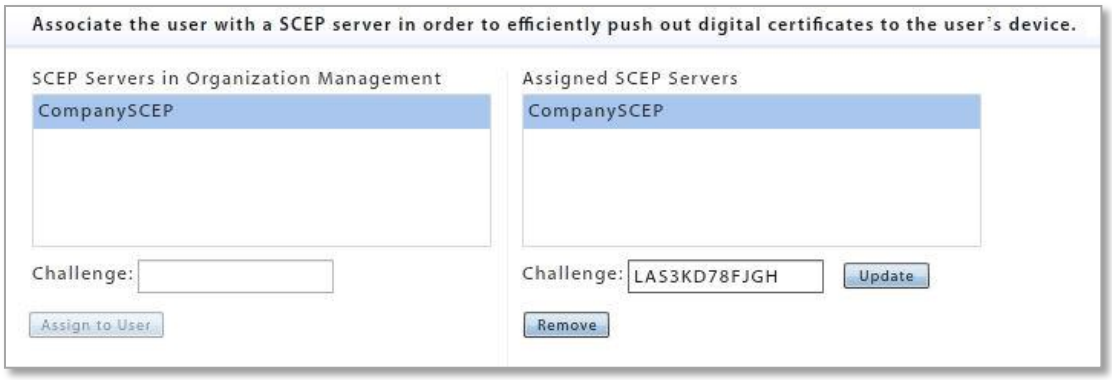
Now, you can use the ***Smart User and Devices*** view on the dashboard to assign a SCEP server to users.

Associating a User with a SCEP Server

From the dashboard, select the ***Smart Users and Devices*** view and select a user to view his or her profile. Select ***Assign SCEP Server*** from the left panel. Select a SCEP server for the user from the table.

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.

Click the ***Assign to User*** button.



Organization Control

Organization Control settings are located in the *Organization* view. They consist of a variety of options that give you the ability to maintain organization configurations or communicate information to users.

Options for Communicating Information
(documented in this guide)

- Group E-mailing
- File Share
- Mobile Apps

Configuration Options
(see *Configuration Guides*)

- Compliance Manager
- SMTP Server

Group E-mailing

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

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

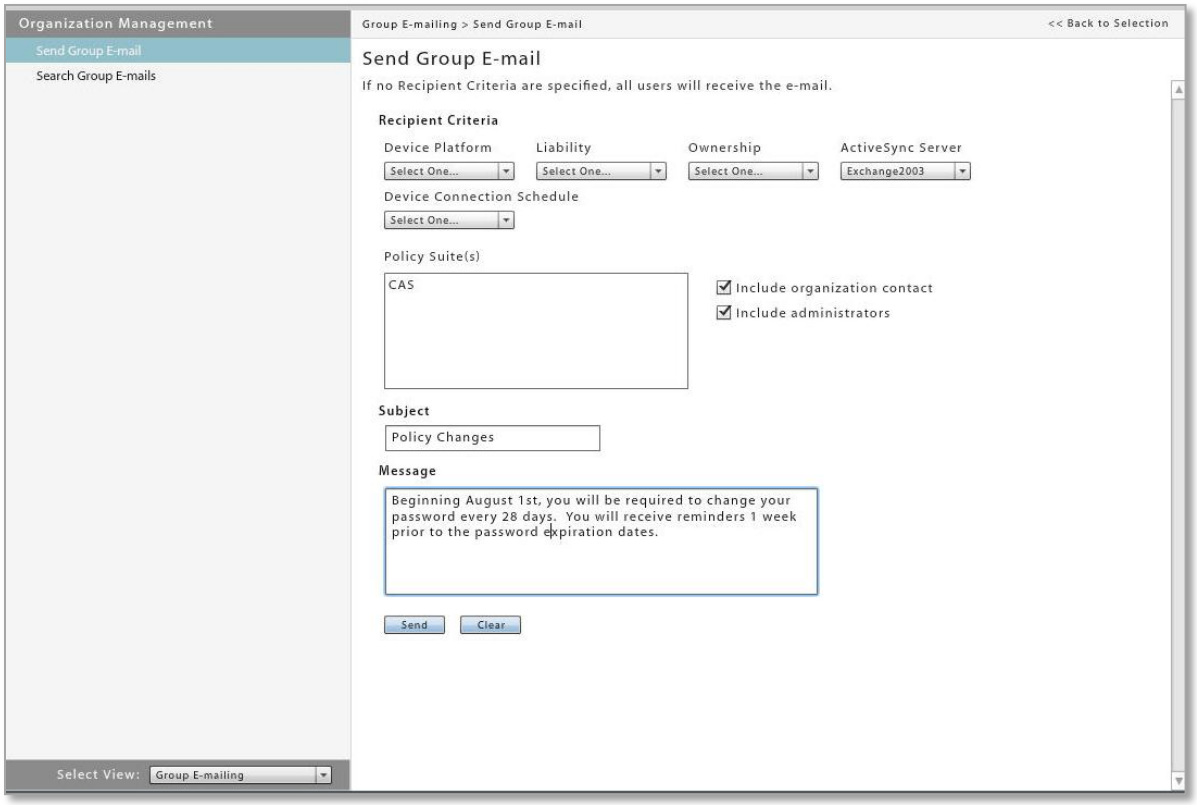
Send Group E-mail

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

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

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

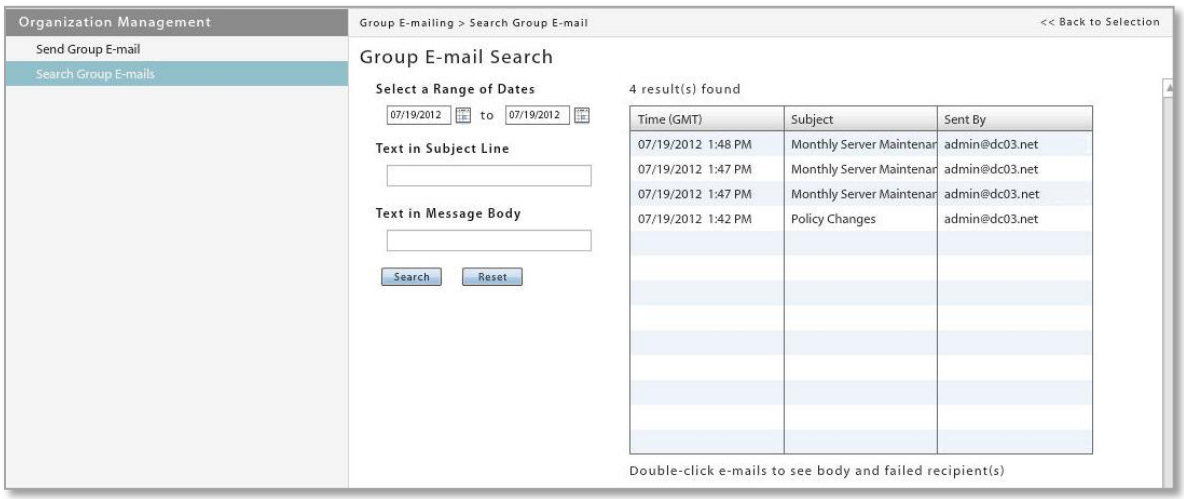
To send a group email, select ***Organization*** > ***Group E-mailing*** > ***Send Group E-mail***



Search Group E-mail

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

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



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 device with the *NotifySync* application.

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

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

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

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

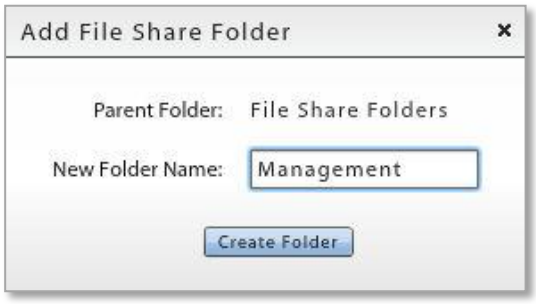
Adding Folders and Files to the Directory

To manage the file directory, select ***Organization*** > ***File Share***

Adding Folders

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

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



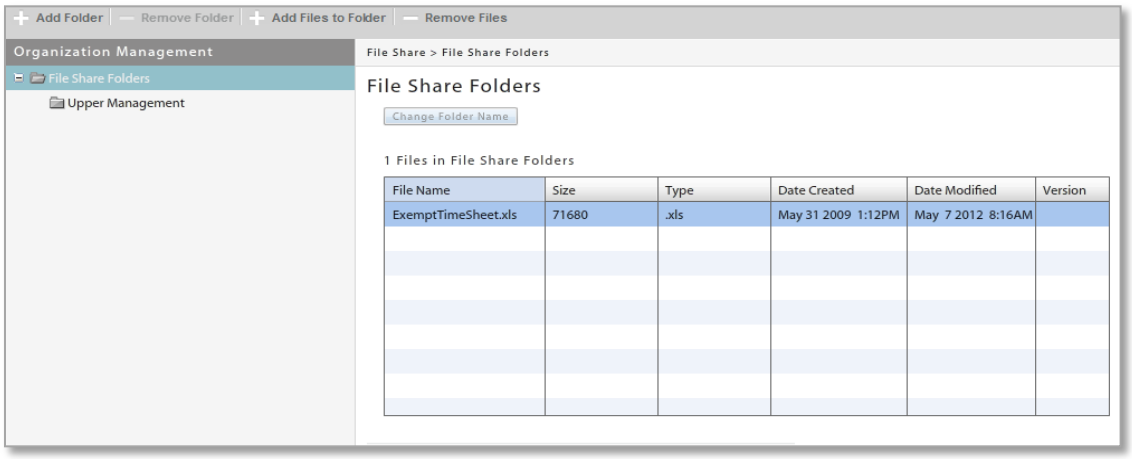
You can edit a folder label by highlighting a folder and clicking the ***Change Folder Name*** button.

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***.

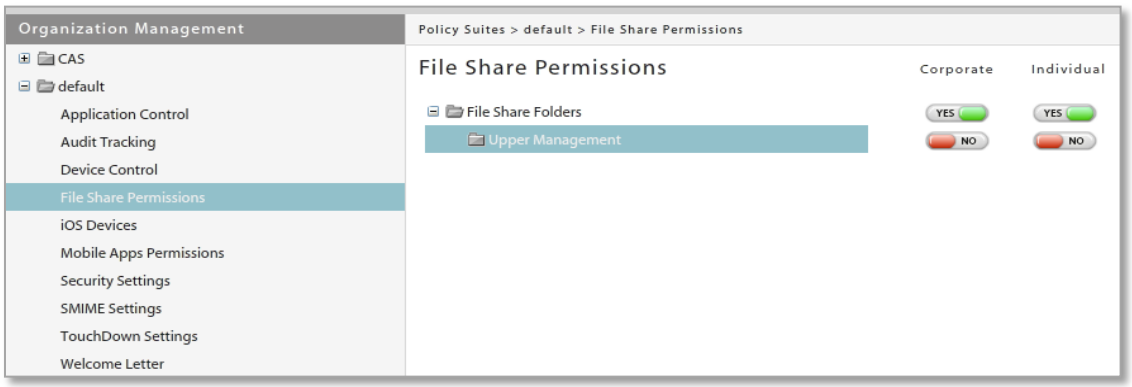
   The *Upload Status* shows the number of files that added successfully.



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

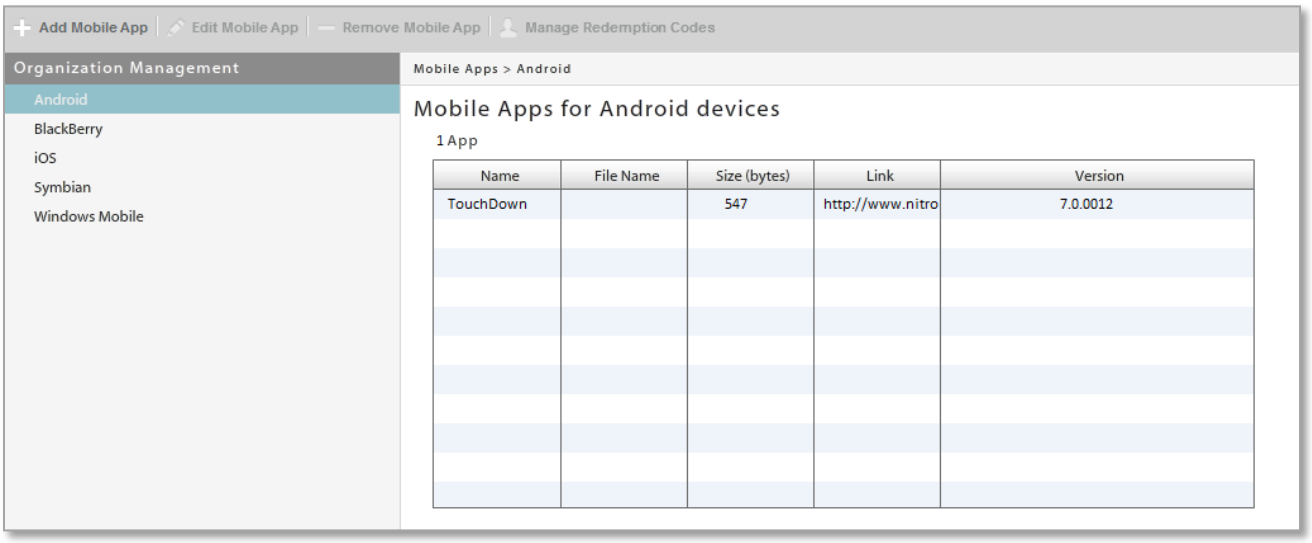


Mobile Apps

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

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

To manage the mobile app list, select ***Organization*** > ***Mobile Apps***



Add a Mobile App

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

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

- For ***BlackBerry*** (with *NotifySync*) and ***iOS 4*** devices, provide application store URLs so that users can link to an application store or download page to obtain the app.
- For ***Android***, ***Symbian S60 3***, and ***Windows Mobile 6*** devices, you can specify an application store URL or you can enter an actual file. If you have synchronized app files to the device, users can open and install them directly from the *ZENworks Mobile Management* app.
- For ***iOS 5*** devices, it is possible to add and manage free App Store apps, Enterprise Apps, and apps that have been prepurchased through the Apple Volume Purchase Program (VPP).

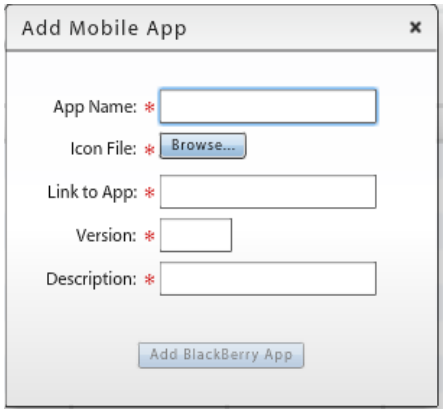
1. Select ***Mobile Apps*** from the ***Organization*** view, then click ***Add Mobile App***.
2. Select the device type to which you will add an app: ***Android***, ***BlackBerry***, ***iOS***, ***Symbian***, or ***Windows Mobile***.
3. Select ***File*** or ***Link*** if you are adding an app for Android, Symbian, or Windows Mobile devices. BlackBerry and iOS default to 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.

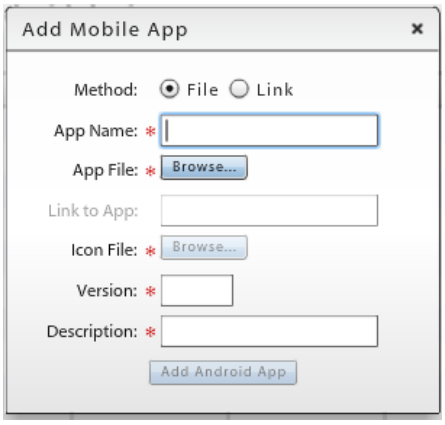
   For *Files*, browse to select a file for the ***App File*** field.

   - For *Android*, select: **.apk** files
   - For *Symbian*, select: **.sis** or **.sisx** files
   - For *Windows Mobile*, select: **.cab** files

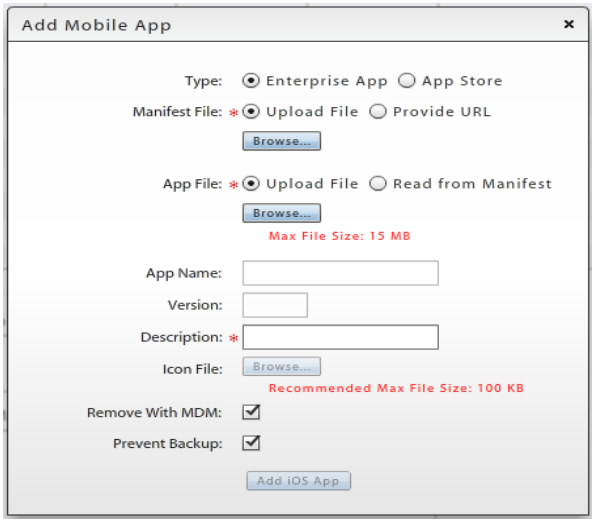
6. For *Links*, browse your image files in the ***Icon File*** field to associate an icon with the application. This also displays on the device.
7. Click the ***Add App*** button.



Add Apps for BlackBerry (w/NotifySync)



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



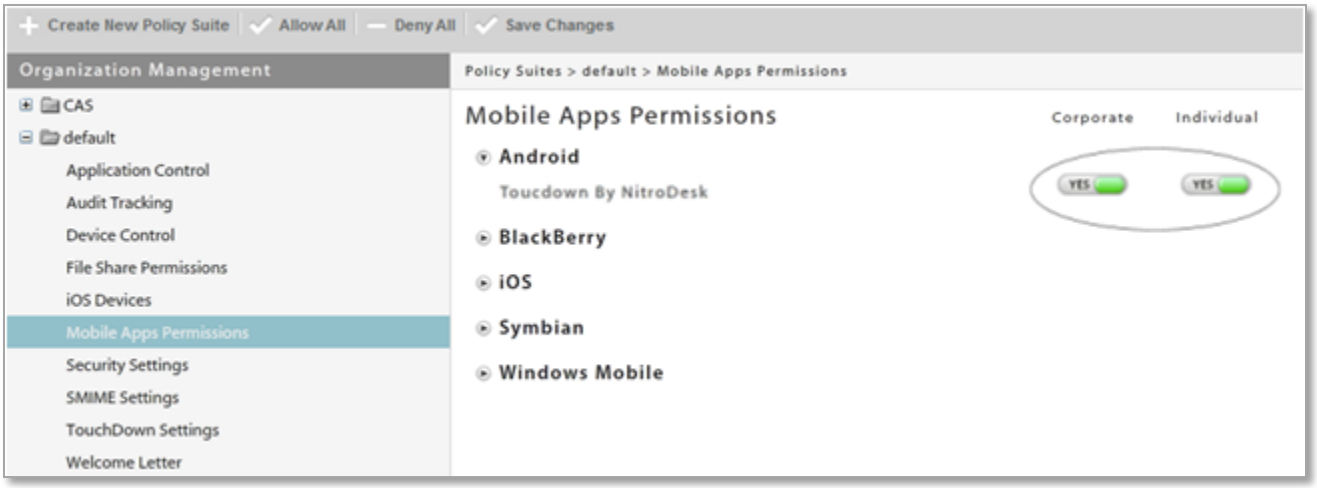
Add Apps for iOS Devices

There is an app list display for each device type. You can select an individual app and edit or remove it by clicking ***Edit Mobile App*** or ***Remove Mobile App***.

Enabling Mobile App Permissions

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

1. Enable the ***Mobile App Permissions*** in the policy suites for each app you have added. From the *ZENworks Mobile Management* dashboard, select ***Organization*** > ***Policy Suites*** > (*select policy suites*) > ***Mobile App Permissions*.**



2. For iOS apps, select ***Organization*** > ***Policy Suites*** > (*select policy suites*) > ***iOS Devices*** > ***Applications***. Then verify that the *Allow application installation* and *Allow iTunes* policies are enabled.

Accessing Mobile Apps on a Device

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

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

Managing Mobile Apps for iOS 5 Devices

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

Management functionality includes:

- Installing/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.

Policy Rules Required for Managing Apps

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

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

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

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

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

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

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

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

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

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

Enabling Force Push for Required Apps

Adding iOS App Store Apps to the List

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

1. Select ***Mobile Apps*** from the ***Organization*** view, then click ***Add Mobile App***.
2. Select the ***iOS*** from the Device Type drop-down list.
3. Choose ***App Store*** as the mobile app ***Type***.
4. Enter a ***Name***, ***Version***, and ***Description*** for the app. What you enter displays on the device.
5. Enter the **App Store URL**.
6. Browse your image files at the ***Icon File*** field and select an icon to associate with the application. This also displays on the device.
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 the user to be able to save the app via iTunes.

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 only available in the United States, and VPP apps are only available through the U.S. App Store.

To add redemption codes:

1. Add the app to the iOS Mobile App list.
2. Select the app, then click ***Manage Redemption Codes***.
3. Select the ***Add Redemption Codes*** tab.
4. Select ***Manual*** or XLS (for XLS, proceed to step 6).if you will enter each code individually.

   If you are entering each code individually, choose Manual.

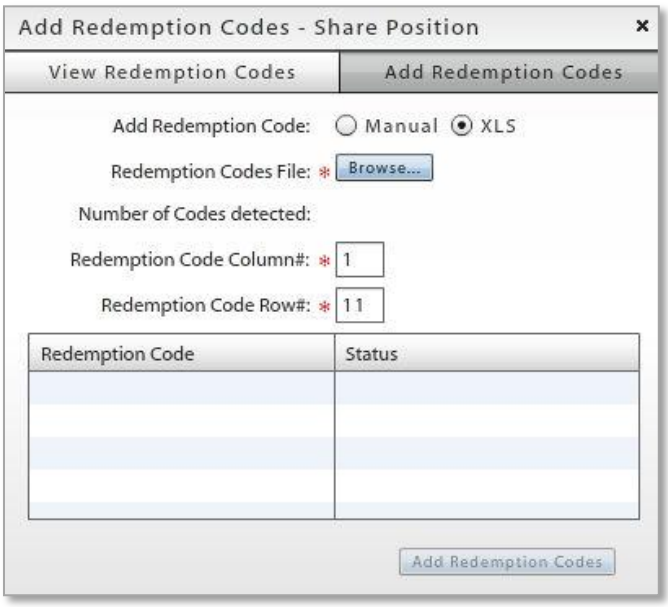
   Enter each code on a new line.
5. Click the ***Add Redemption Codes*** button.

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.

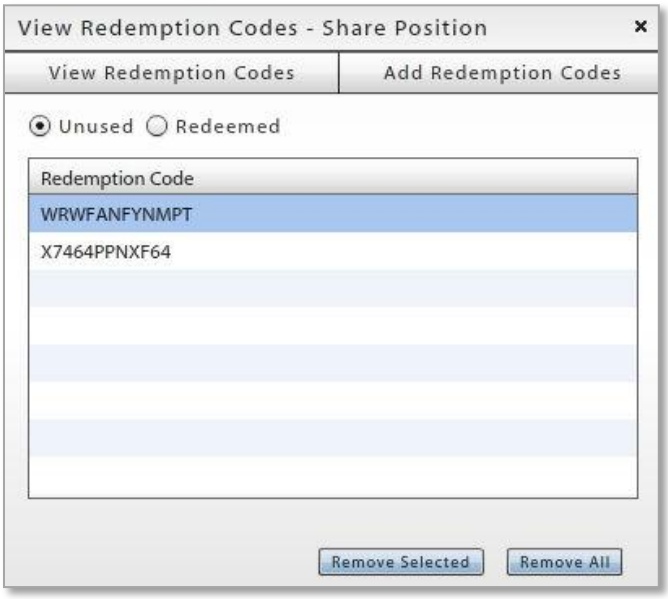
   There are volume purchase details at the top of the spreadsheet. Specify the column and row where the actual redemption codes begin.

7. Click the *Add Redemption Codes* button.



To view or remove redemption codes:

1. Select an app from the iOS Mobile App list, then click ***Manage Redemption Codes***.
2. Select the ***View Redemption Codes*** tab.
3. Choose to view either the ***Unused*** or ***Redeemed*** codes.
4. 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.



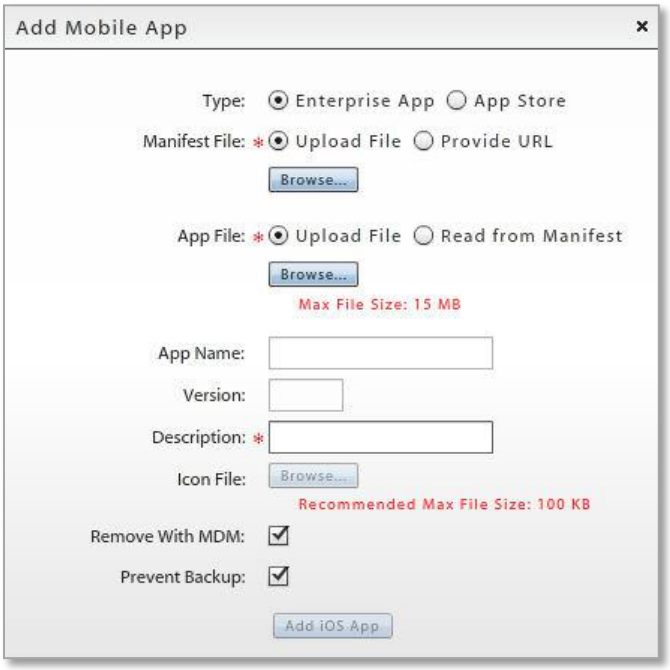
Adding an iOS Enterprise App to the List

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 ***Mobile Apps*** from the ***Organization*** view, then click ***Add Mobile App***.
2. Select the ***iOS*** from the Device Type drop-down list.
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.



Updating Enterprise 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 click ***Update this app for existing users*** to push the upgrade down. Users are prompted to update the app.