Compliance Manager

ZENworks® Mobile Management 2.9.x

May 2014

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

Requirements

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 the Windows operating system

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.

Location of the Compliance Manager

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

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.

Compliance Manager

The **Compliance Manager** gives an administrator the ability to restrict access to ActiveSync and *ZENworks Mobile Management* resources based on a device's state of compliance. Restrictions can be imposed based on:

- Compliance with a configurable set of criteria (*Access Restrictions*)
- Individual user names (*Access Restrictions*)
- Individual devices, designated by phone number or device UID (*Access Restrictions*)
- Specific device types, models, or OS versions (*Device Platform Restrictions*)

Each time a device synchronizes it sends its statistics, which the server compares against the restriction criteria. Devices are restricted when they are found to be non-compliant with one or more of the restrictions or specifications.

Non-Compliant Devices Can Be Restricted From:

- ActiveSync connections
- *ZENworks Mobile Management* corporate resources
    - File Share
    - Managed Apps
- iOS corporate resources
    - Access Point Name
    - CalDAV Server
    - CardDAV Server
    - Exchange Servers
    - LDAP Servers
    - Mail Servers
    - Provisioning Profiles
    - Subscribed Calendars
    - VPNs
    - Web Clips
    - Wi-Fi Networks
- Android corporate resources: Wi-Fi Networks and VPNs

Non-Compliant Devices Are Not Restricted From:

- *ZENworks Mobile Management* Server connections
- Certain ActiveSync traffic, such as policy suite updates and wipe commands

When a device is found to be non-compliant, it is permitted to connect with the *ZENworks Mobile Management* server, even though it is restricted from some or all of the resources listed above. In this way, the server continues to gather statistics from the device and can release the device from restrictions when it becomes compliant.

In most cases, the server automatically removes the restriction from a device that has returned to a compliant state. Certain restriction breaches, however, require an administrator to release the device by using one of the ***Clear*** options on the *Users* grid: **Clear ActiveSync Authorization Failures, Clear ZENworks Authorization Failures,** or **Clear SIM Card Removed or Changed Violation.**

Alert Settings

Alerts notify administrators of issues and events in the *ZENworks Mobile Management* system through the *View Alerts* grid on the dashboard (*Activity Monitor*) and can be configured to alert administrators via email or SMS messages. The system does not send alerts unless they are enabled. All alert settings are disabled by default.

Even if you are not using the Compliance Manager Access Restrictions or Device Platform Restrictions, you may want to enable some of the Non-Access Restriction Based Alerts and Event Based Alerts.

In addition to reporting device access restriction and device restriction violations, *Alert Settings* can monitor device resource levels and connectivity, as well as administrator or user initiated events.

Four Categories of Alert Settings

Access Restriction Based Alerts are associated with the *Access Restrictions*. There is a corresponding setting for every Access Restriction.

Non-Access Restriction Based Alerts are associated with *Device Platform Restrictions*, device resource levels, or organization-wide connectivity.

Event Based Alerts are associated with incidents initiated by administrators or users. Alerts can be set for when devices are cleared, wiped, or locked; when password recovery attempts are made; or when new devices enroll via hands-off provisioning.

System Alerts are associated system level alerts. An alert can be set to notify administrators when the Apple Push Notification service certificate approaches its expiration date.

See also Managing Alert Settings.

See Appendix B: Alert Settings for descriptions of the alerts.

Access Restrictions

Use the Access Restrictions to set the criteria which devices must meet to access the server. Single users or devices (designated by phone number or device UID) can also be restricted.

The resources you restrict for non-compliant devices can be set globally (identical restrictions for all Access Restrictions) or for individual devices or users.

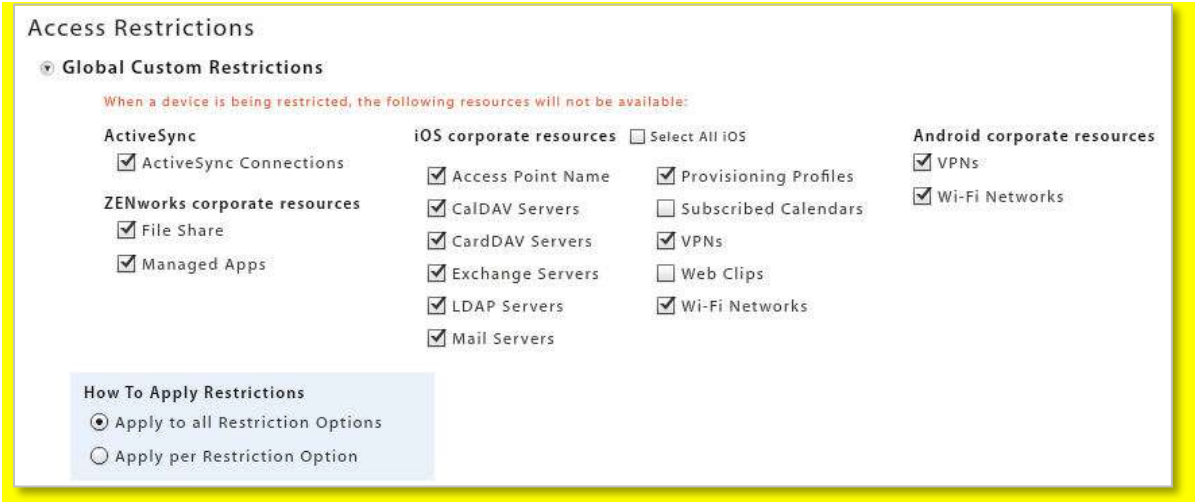
Select *Access Restrictions* from the left panel of the Compliance Manager page.

Setting Global Restrictions or Defining Individual Restriction Option

The restrictions for non-compliance with *Access Restrictions* can be set globally (identical restrictions for all Access Restrictions) or Individual restriction.

Select ***Global Custom Restrictions***.

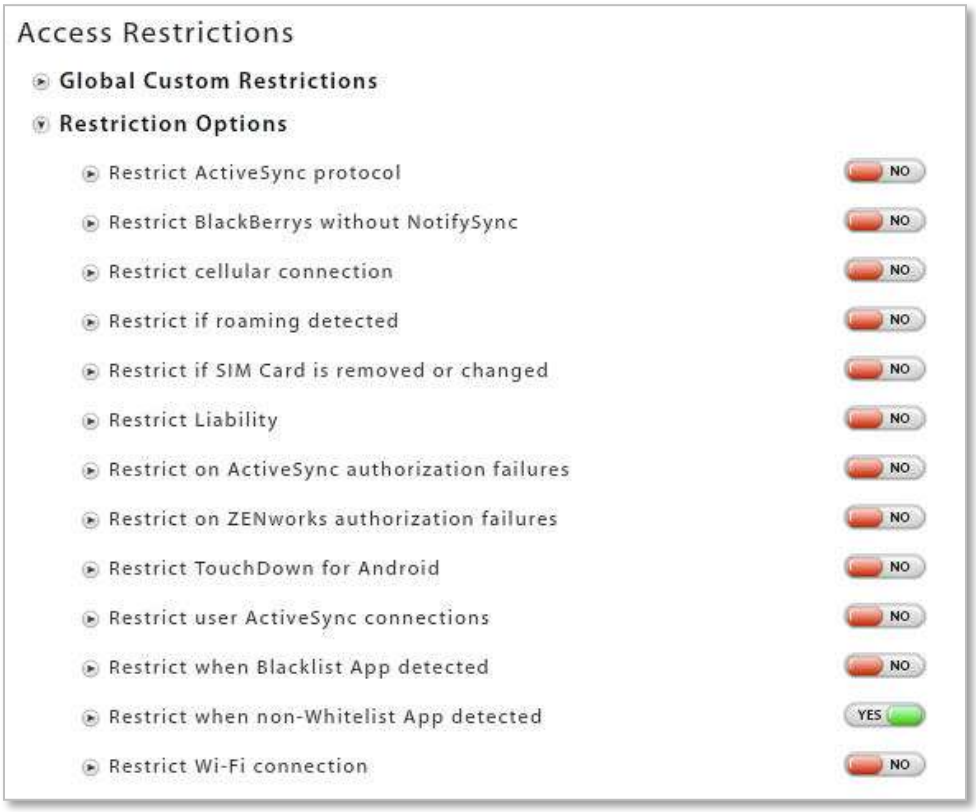
- To set global restrictions, select ***Apply to all Restriction Options***, then select the resources you want to restrict.
- To configure settings for each restriction option, select ***Apply per Restriction Option***, then select the resources you want to restrict within each restriction option.



Configuring the Access Restrictions

1. Select ***Restriction Options***.
2. Click the slider to enable (YES) or disable (NO) each restriction.
3. Click the ***Save Changes*** button.

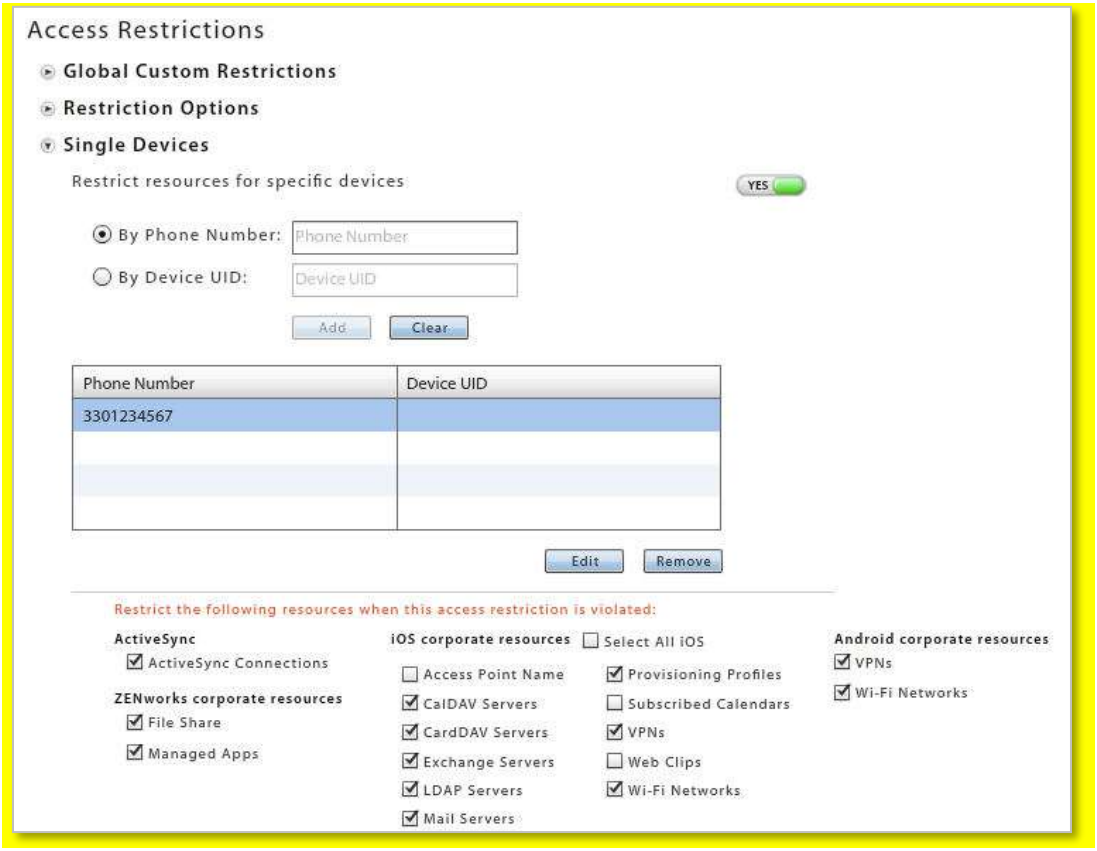
See Appendix A: Access Restrictions for descriptions of each restriction.



Restricting Single Devices

You can restrict devices that are already enrolled or devices that are not yet enrolled.

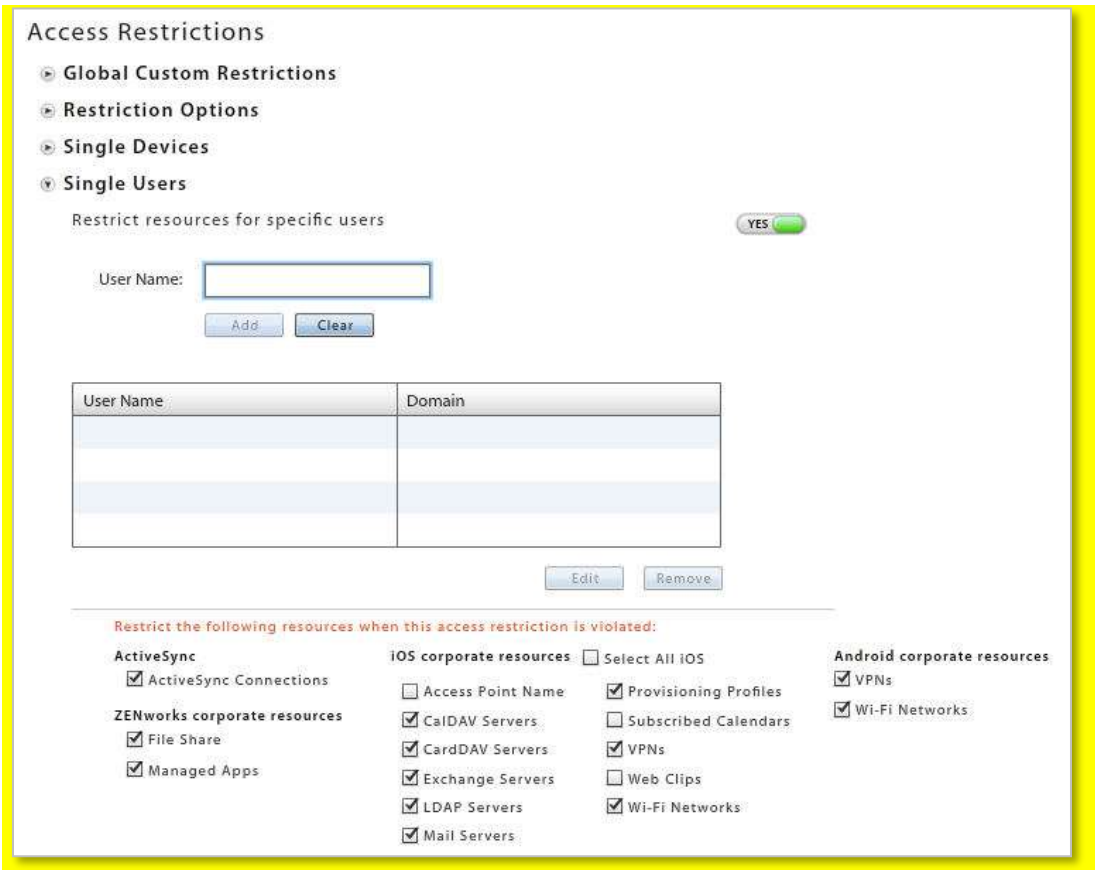
1. Select ***Single Devices***.
2. Click the slider to enable (YES) or disable (NO) the restriction.
3. Select ***By Phone Number*** or ***By Device UID*** and enter the number that identifies the device.
4. Click the ***Add*** button.
5. If you are specifying the restricted resources for this device, select the appropriate boxes. If restricted resources have been assigned globally, this area is dimmed.



Restricting Single Users

You can restrict users that are already enrolled or users that are not yet enrolled.

1. Select ***Single Users***.
2. Click the slider to enable (YES) or disable (NO) the restriction.
3. Enter the ***User Name*** or enter the ***Domain\User Name*** (required if there are users in different domains who have the same user name).
4. Click the ***Add*** button.
5. If you are specifying the restricted resources for this device, select the appropriate boxes. If restricted resources have been assigned globally, this area is dimmed.



Device Platform Restrictions

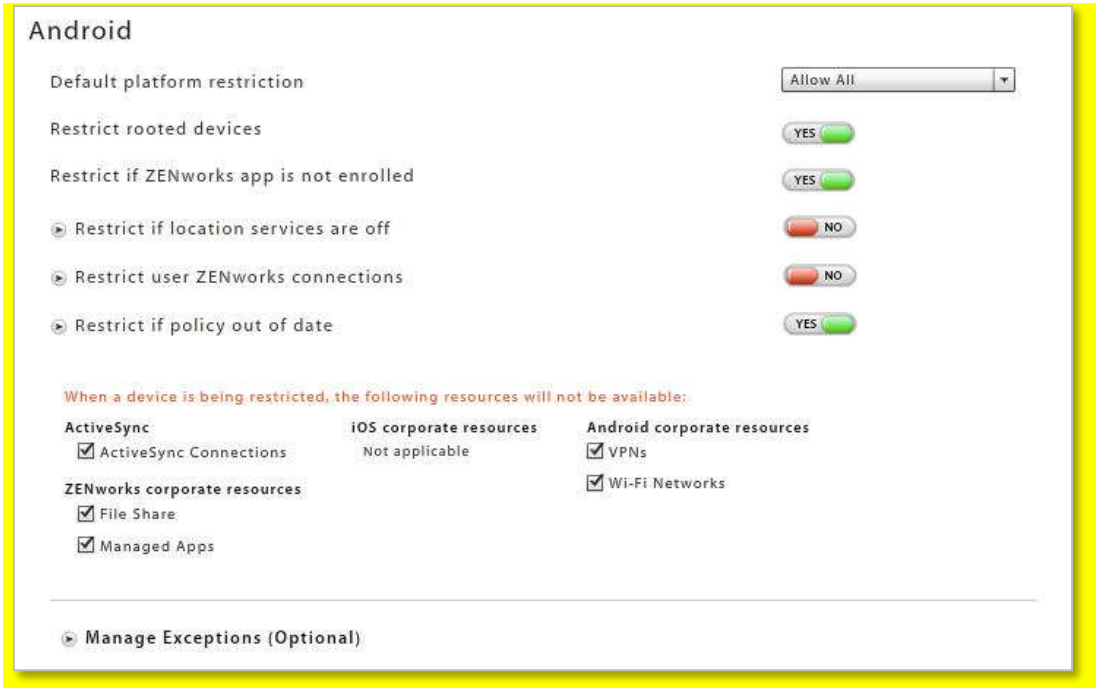
Defining Restrictions

Use Device Platform Restrictions to specify the types of devices that may access the server.

- Devices can be specified by manufacturer, model, operating system (OS) version, and carrier.
- Devices can be restricted under any of the following conditions:
  - The *ZENworks Mobile Management* app is not enrolled
  - The location is not updated
  - *ZENworks Mobile Management* connections are not occurring
  - The policy suite is out-of-date
- Android and iOS devices can be restricted if they are rooted or jailbroken.
- iOS devices can be restricted based on passcode and configuration profile compliance.

The resources you restrict for non-compliant devices can be selected per device platform.

1. Select ***Device Platform Restrictions*** from the left panel of the Compliance Manager page.
2. Select a device platform.
3. Choose to ***Allow All*** or ***Restrict All*** devices of this platform type or allow ***Supported Devices Only***.
4. Click the slider to enable (YES) or disable (NO) the restriction associated with this device platform
5. Select the appropriate boxes to specify the restricted resources for devices of this platform type that violate a restriction rule.
6. Click ***Manage Exceptions*** to define exceptions to the allowed or restricted devices.

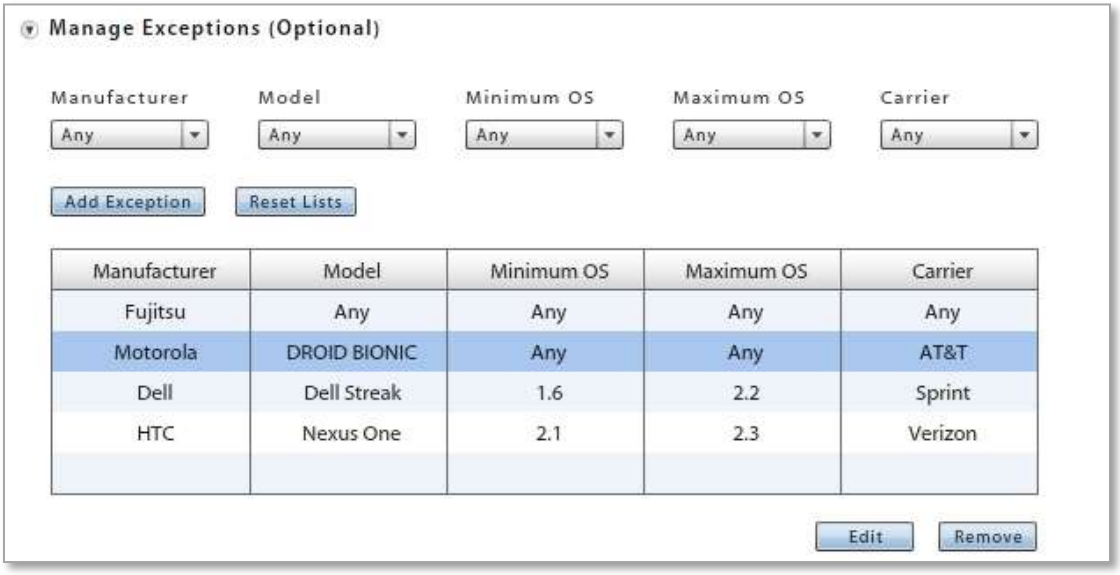


Managing Exceptions

You can define exceptions to the Device Platform Restrictions:

If you ***Allow All*** devices in the platform or allow ***Supported Devices Only***, exceptions can define one or more devices of that type that you will not allow. If you ***Restrict All*** devices in the platform, exceptions can define one or more devices of that type that you will allow.

1. Select ***Manage Exceptions*** on the Compliance Manager page.
2. Choose the ***Manufacturer***, ***Model***, ***Minimum*** / ***Maximum OS***, and ***Carrier*** for the device exception.
3. Click the ***Add Exception*** button.



Restriction Notifications

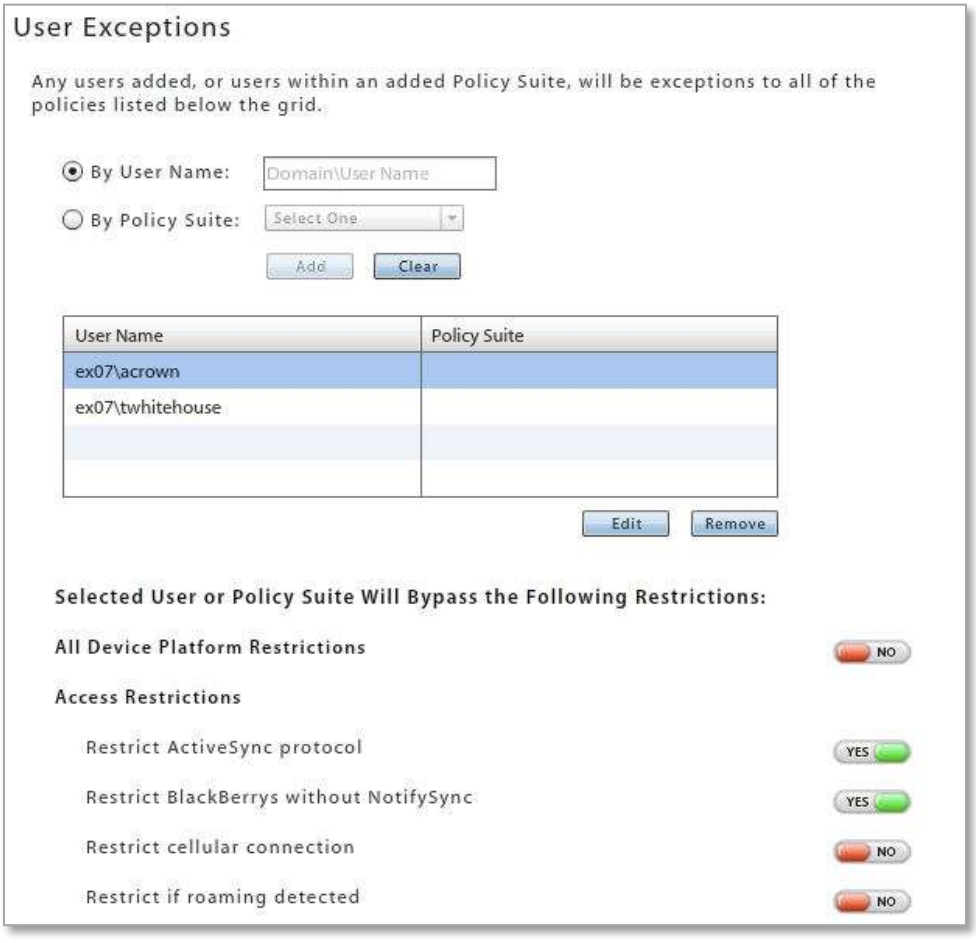
You have the option of sending an email notification to the user whose device is in violation of one of the *Access Restrictions* or *Device Platform Restrictions*.

1. Select ***Restriction Notifications*** from the left panel on the Compliance Manager page.
2. Select ***Access Restrictions*** or ***Device Platform Restrictions***.
3. Select ***Restriction Notifications*** and click the slider so that it reads **YES** to enable this option.
4. Compose or edit the subject and body of the email that is sent to the users who are in violation of one of the Access Restrictions or Device Platform Restrictions.
5. Click the ***Save Changes*** button.

User Exceptions

After *Access Restrictions* and *Device Platform Restrictions* are configured, you might want to designate user exceptions to the configurations. When you create an exception, you are essentially creating an alternate set of criteria for an individual user or users that are governed by a specific policy suite.

1. Select ***User Exceptions*** from the left panel of the ***Compliance Manager*** page.
2. Select ***By User Name*** or ***By Policy Suite***. Enter a user name or select a policy suite from the drop-down list.
3. Click the ***Add*** button.
4. Select the user or policy suite for which you are creating exceptions.
    - For exceptions to Access Restrictions, adjust the slider for each access restriction to enable (YES) or disable (NO) the restriction.
    - For exceptions to Device Platform Restrictions, adjust the slider for ***All Device Platform Restrictions*** to enable (YES) or disable (NO) the restriction. You can also define exceptions per device platform within the Device Platform Restrictions.
5. Click the ***Save Changes*** button.



Managing Alert Settings

Alert Recipients

Use ***Alert Recipients*** to create a list of administrators who can be notified of a violation by email or SMS. When configuring the ***Alert Settings***, you will choose from this list, who you wish to notify.

If an alert setting has been enabled for an access restriction, a device platform restrictions, or event, an alert appears on the View Alerts page of the Activity Monitor section. However, when configuring the Alert Settings, you may designate administrators who should also be notified by email or SMS of a violation. Email or SMS notifications to administrators can be sent for any of the Alert Settings.

1. Select ***Alert Recipients*** from the left-hand panel of the ***Compliance Manager*** page.
2. Click the ***Add Alert Recipient*** button.
3. Enter the ***Display Name*** and ***E-mail Address*** of the recipient.
4. If you want the recipient to receive SMS notifications, provide the ***Carrier*** and ***Phone Number*** of the device to which it should be sent. See a list of supported carriers.
5. Click the ***Finish*** button.

Alert Settings

Alerts notify administrators of issues and events in the *ZENworks Mobile Management* system. They are reported on the Activity Monitor page of the dashboard in the *View Alerts* grid and can be configured to alert administrators via email or SMS message. Alerts can be rated with a high, medium, or low priority.

Some alerts report violations of:

- Access restrictions
- Device platform restrictions

Some alerts monitor:

- Device resource levels and connectivity
- Administrator or user initiated events
- System level events

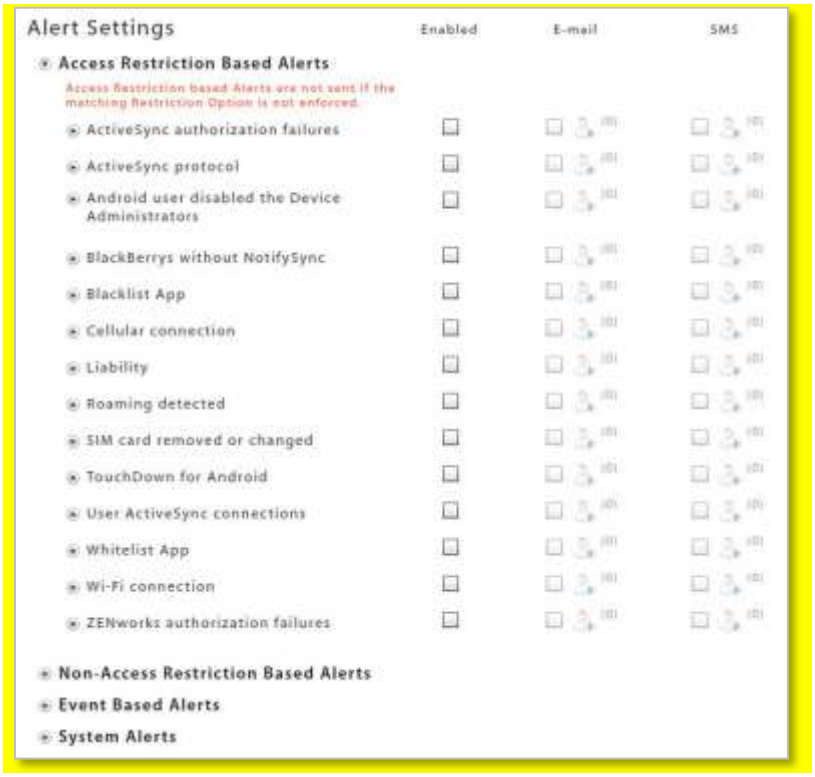
Four Categories of Alert Settings

Access Restriction Based Alerts are associated with the Access Restrictions. There is a corresponding setting for every Access Restriction.

Non-Access Restriction Based Alerts are associated with Device Platform Restrictions, device resource levels, or organization-wide connectivity.

Event Based Alerts are associated with incidents initiated by administrators or users. Alerts can be set for when devices are cleared, wiped, or locked; when password recovery attempts are made; or when new devices enroll via hands-off provisioning.

System Alerts are associated system level alerts. An alert can be set to notify administrators when the Apple Push Notification service certificate approaches its expiration date.



Alert Setting Parameters

Report Every (Minutes)

For all alerts, except those in the event based category, you set Report Every (Minutes). An alert is issued when a violation is initially detected and repeats the alert at the interval you set for as long as the violation continues. The default interval is 60 minutes.

Priority

You set an alert Priority for every alert setting to rate its level of importance. Choose from a *High*, *Medium*, or *Low* priority. The default priority for every alert is *Medium*. On the View Alerts grid, you can sort or search by priority. If you change the priority of an alert setting, the priority of all existing alerts of that type is changed.

Non-Access Restriction Based Alerts

Several of the *Non-Access Restriction Based Alerts* have additional parameters that govern when the alert is triggered. See Appendix B: Alert Settings for details.

Enable the Alert Settings

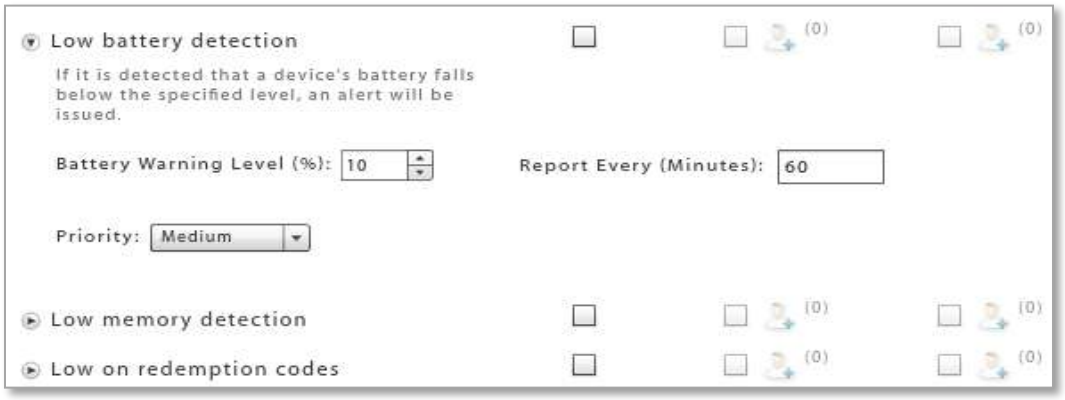
The system does not send alerts unless they are enabled. All alert settings are disabled by default.

Even if you are not using the Compliance Manager's *Access Restrictions* or *Device Platform Restrictions*, you may want to enable some of the ***Non-Access Restriction Based Alerts*** and ***Event Based Alerts***.

See Appendix B: Alert Settings for descriptions of the alerts.

1. Select ***Alert Settings*** from the left panel of the ***Compliance Manager*** page.
2. Select the box in the Enabled column next to each of the alerts you want the system to issue. When a violation of an enabled setting is detected, the alert is issued and displayed in the ***View Alerts*** grid.

   Access Restriction Based Alerts are not sent unless the matching ***Access Restriction*** is enforced.
3. Click the expansion button next to the setting to define the ***Report Every*** interval, the ***Priority***, and any other parameters associated with the alert.



4. Select the box in the ***E-mail*** column or the ***SMS*** column next to the alert if you want to send an email or SMS notification to an administrator when violations are detected. Choose a recipient from the list.
   - If you are adding a recipient for the first time, the Manage Alert Recipients Wizard pops up.
   - Click the recipient icon  to edit the list of recipients.

Connectivity Watch List

The watch list provides the administrator with a way to monitor individual users for connectivity issues.

You can add users to the watch list who have not synchronized with the ActiveSync server or have not synchronized the device's *ZENworks Mobile Management* application. You can also select a policy suite to watch, which monitors the connectivity of every user associated with a specific policy suite.

The watch list alert setting must be enabled in order to receive alerts about users on the watch list.

1. Select ***Watch List*** from the left panel of the ***Compliance Manager*** page.
2. In ***Alert Settings,*** select ***Non-Access Restriction Based Alerts*** to enable ***Watch List***.

Note***:*** Devices in Direct Push mode, whose timeout intervals can vary in length, may not return results as consistently as devices in Scheduled Push mode. They may need to be on the watch list longer before results are reported.

1. Select ***Watch List*** from the left panel of the ***Compliance Manager*** page.
2. Click the ***Add Watch List Entry*** button.
3. Enter a ***User Name*** in the format Domain\User Name or select a policy suite from the drop-down list.
4. In ***ActiveSync Timeout***, select the length of time to monitor the user's ActiveSync connections. If the user does not connect within this time, an alert is issued.

   Choose from 1-60 Minutes, 1-24 Hours, or 1-60 Days.
5. In ***iOS APN Timeout***, select the number of APN connection cycles to monitor. If the user does not synchronize through Apple's Advanced MDM API within this defined number of cycles, an alert is issued.

   Choose from 1-5, 10, 15, or 20 cycles.
6. In ***ZENworks Timeout***, select the number of *ZENworks* connection cycles to monitor. If the user does not connect within this defined number of cycles, an alert is issued.

   Choose from 1-5, 10, 15, or 20 cycles.
7. Click the ***Finish*** button to add the user.

Appendix A: Access Restrictions and Device Platform Restrictions

For information regarding the functionality of compliance restrictions across device platforms, please see the *Compliance Manager* section in the Device Platform Functionality matrix.

	Restriction imposed when...	Configurable Options	Restricted Device is granted access when…
Access Restriction			
Restrict on 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.	Failed login attempt limit (# of attempts):	An Administrator permits access via the Clear ActiveSync Authorization Failures button.
Restrict ActiveSync protocol	A device cannot support sufficient ActiveSync policies because of ActiveSync version support limitations with the device or server.	Minimum AS version:	---
Restrict cellular connection	A device is using a cellular network connection and is in violation of the enabled Restrict Cellular Connection access restriction. Only detected for BlackBerry devices currently using a non-WiFi preferred network setting for *ZENworks Mobile Management*	---	The device changes its state.

	connection.		
Restrict if Android user disables Device Administrators	An Android user has not granted device administrator privileges to the *ZENworks Mobile Management* app.	---	. . . the user enables Device Administration on the device
Restrict Liability	A device enrolls with a liability status specifically restricted by the Restrict Liability access restriction.	Type: (Corporate/Individual)	The liability status is corrected by an administrator
Restrict on 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.	Failed login attempt limit (# of attempts):	An Administrator permits access via the ***Clear ZENworks Authorization Failures*** button.
Restrict BlackBerrys without GO!NotifySync	A BlackBerry device that does not have the *GO!NotifySync* application has enrolled. Devices that have a version of *GO!NotifySync* without the *MDM* component also trigger this restriction.	---	The device is re-enrolled with *GO!NotifySync*
Restrict if roaming detected	A device is roaming and is in violation of the Restrict if Roaming Detected access restriction.	---	The device is no longer in a roaming state
Restrict if SIM Card removed or changed	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.	---	An Administrator permits access via the ***Clear SIM Card Removed or Changed Violation*** button.
Restrict TouchDown for Android	TouchDown is required and either an Android device does not have the TouchDown application or the TouchDown version does not meet the minimum requirement.	Devices with TouchDown versions in disallowed range (Max. and Min.) OR Devices without TouchDown and those with TouchDown versions Outside Desired Range disallowed range (Max. and Min.)	The TouchDown version is updated OR A compliant version of the TouchDown app is installed on the device
Restrict user ActiveSync connections	A device's Last ActiveSync Sync time stamp has not updated within the set interval.	No connectivity for (Minutes):	ActiveSync synchronization resumes

Restrict when Blacklist App detected	A device has a blacklisted application installed.	---	The device user uninstalls the blacklisted application
Restrict when non-Whitelist App detected	A device has an application that does not match the whitelist criteria.	---	The device user uninstalls the application that does not match the whitelist criteria
Restrict Wi-Fi connection	A device is using a Wi-Fi connection and is in violation of the enabled Restrict Wi-Fi Connection access restriction. Only detected for BlackBerry devices currently using a WiFi preferred network setting for *ZENworks Mobile Management* connection.	---	The device ceases to use WiFi
Single Devices	A specific device, identified by phone number or UID number, has been denied access.	By Phone Number: By Device UID:	An Administrator permits access
Single Users	A specific user, identified by the User Name, has been denied access.	User Name	An Administrator permits access
Device Platform Restriction			
Restrict if ZENworks app is not enrolled	A device enrolls via the native ActiveSync agent alone and without the *ZENworks Mobile Management* application.		The device is re-enrolled with *ZENworks Mobile Management*
Restrict if location not updated	A device's location has not updated within the defined interval.	No updates in (Cycles):	The device's location updates
Restrict user ZENworks connections	A device's *Last ZENworks Sync* time stamp has not updated within the set interval.	No connectivity for (Cycles):	*ZENworks Mobile Management* synchronization resumes
Restrict if policy out of date	A policy suite has been updated on the server, but a device has not updated within the set grace period.	Outdated policy grace period (Minutes):	The device downloads the most current policy suite updates
Restrict rooted devices	A rooted Android device connects to the server.		An Administrator permits access

Restrict jailbroken devices	A jailbroken iOS device connects to the server.		An Administrator permits access
Restrict if iOS passcode not initiated	The user's policy suite requires a password, but the iOS device does not have a passcode initiated.		The user initiates the use of a passcode on the device
Restrict if iOS passcode is not compliant with requirements	The user's policy suite requires a password, but the iOS device does not have a passcode compliant with the requirements.		The passcode is changed to something that is compliant with requirements
Restrict if iOS passcode is not compliant with data protection	The iOS device does not have a passcode and thus is not compliant with iOS data protection, which enhances the built-in hardware encryption by protecting the hardware encryption keys with the passcode.		The passcode is set
Restrict if unmanaged configuration profile is on device	An iOS device has an unmanaged configuration profile (one other than the APN profile or profiles associated with the APN profile).		The unmanaged configuration profile is removed from the device
Restrict if iOS APN profiles are not enrolled	An iOS device has not loaded the iOS APN configuration profile and has never synchronized through the Apple Advanced MDM API.		iOS APN profiles are enrolled
Restrict if no iOS APN connectivity	A device's Last iOS APN Sync time stamp has not updated within the set interval.	No updates in (Cycles):	iOS APN connections resume

Appendix B: Alert Settings

For information regarding the functionality of alert settings across device platforms, see the Compliance Manager section in the Device Platform Functionality matrix.

Alert	Alert is issued when:	Alert Setting Parameters
Access Restriction Based Alert		
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.	---
ActiveSync protocol	A device cannot support sufficient ActiveSync policies, because of ActiveSync version support limitations with the device or server.	---
Android user disabled the Device Administrators	An Android user has not granted device administrator privileges to the *ZENworks Mobile Management* app.	---
BlackBerrys without GO!NotifySync	A BlackBerry device that does not have the *GO!NotifySync* application has enrolled.	---
Blacklist App	A device is blocked because it has a blacklisted application installed.	---
Cellular connection	A device is using a cellular network connection and is in violation of the enabled *Restrict Cellular Connection* access restriction. Can only be detected for BlackBerry devices currently using a non-WiFi preferred network setting for *ZENworks Mobile Management* connection.	---
Liability	A device enrolls with a liability status specifically restricted by the *Restrict Liability* access restriction.	---
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.	
Roaming detected	A device is roaming and is in violation of the *Restrict if Roaming Detected* access restriction.	---
SIM Card removed or changed	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.	---
TouchDown for Android	TouchDown is required and either an Android device does not have the TouchDown application or the TouchDown version does not meet the minimum requirement.	---
User ActiveSync connections	A device's *Last ActiveSync Sync* time stamp has not updated within the set interval.	---
Whitelist App	A device is blocked because it has as application installed that does not match the Whitelist criteria.	
Wi-Fi connection	A device is using a Wi-Fi connection and is in violation of the enabled *Restrict Wi-Fi Connection* access restriction. Only detected for BlackBerry devices currently using a WiFi preferred network setting for *ZENworks Mobile Management* connection.	---
Non-Access Restriction Based Alerts		
Android rooted device	A rooted Android device connects to the *ZENworks Mobile Management* server.	---
iOS jailbroken	A jailbroken iOS device connects to the *ZENworks Mobile Management* server.	---
iOS APN profiles not enrolled	An iOS device has not loaded the iOS APN configuration profile and has never synchronized through the Apple Advanced MDM API.	
iOS APN connectivity	A device's *Last iOS APN Sync* time stamp has not updated within the set interval.	
iOS passcode not initiated	The user's policy suite requires a password, but the iOS device does not have a passcode initiated.	---
iOS passcode not compliant with	The user's policy suite requires a password, but the iOS	---

requirements	device does not have a passcode compliant with the requirements.	
iOS passcode not compliant with data protection	The user's Policy Suite requires a password and device encryption, but the iOS device does not have a passcode and does not have encryption set.	---
iOS unmanaged configuration profile	An iOS device has an unmanaged configuration profile (other than the APN profile or profiles associated with the APN profile).	---
Location not updated	A device's location has not updated within the defined interval.	---
Low battery detection	A device's battery level has fallen below a specified warning level. Defaults to 10%.	**Battery Warning Level (%)**
Low memory detection	A device's memory level has fallen below the greater of the two specified levels. Defaults to 15 MB or 10%.	**Memory Warning Level (MB) -** For devices with a memory capacity less than 100 MB, warning occurs if available memory falls below the specified megabytes. **Memory Warning Level (%) -** For devices with a memory capacity greater than 100 MB, a warning occurs if the available memory falls below the specified percentage.
Low on redemption codes	The number of redemption codes (for iOS devices installing an app obtained through the Apple Volume Purchase Program) available on the server has fallen below a specified amount. Defaults to 5 codes remaining.	**Codes Remaining**
ZENworks app is not enrolled	A device of any platform type connects to the server via ActiveSync and does not have the *ZENworks Mobile Management* application enrolled.	---
Organization-wide ActiveSync connectivity	The *Last ActiveSync Sync* time stamp has not updated for any users within the set interval. Default is 720 minutes.	**No Connectivity for (minutes)**
Organization-wide ZENworks connectivity	The *Last ZENworks Sync* time stamp has not updated for any users within the set interval. Default is 3 cycles.	**No Connectivity for (cycles)** - Number of Device Connection Schedule cycles.

Policy out of date	A policy suite has been updated on the server, but a device has not updated within the set grace period.	---
Watch List	A user or policy suite on the Watch List grid has exceeded the time for which he/she/it was being monitored.	---
User's e-mail not set	A user's email address has not been set. *Because a user's email address cannot always be determined during hands-off provisioning, this alerts the administrator that an email address for the user should be manually set.*	---
User ZENworks connections	A device's *Last ZENworks Sync* time stamp has not updated within the set interval.	---
Event Based Alerts		
ActiveSync Account Already Enrolled	An iOS profile included an ActiveSync payload that could not be installed because an identical ActiveSync account was already enrolled.	---
Reset for Enrollment	An administrator has issued a Clear Device Enrollment command from the dashboard to a device.	---
Clear passcode issued by Admin	An administrator has issued a Clear Passcode command from the dashboard to an iOS device.	---
Full wipe issued by Admin	An administrator has issued a Full Wipe command from the dashboard to a device.	---
Full wipe issued by user	A user has issued a Full Wipe command from the User Self Administration Portal to a device.	---
Lock device issued by Admin	An administrator has issued a Lock Device command from the dashboard to a device.	---
Lock device issued by user	A user has issued a Lock Device command from the User Self Administration Portal to a device.	---
New Hands-Off Provisioned device	Any time a new device uses hands-off enrollment to connect to the system.	---
New Hands-Off Provisioned user	Any time a new user uses hands-off enrollment to connect to the system.	---
Recovery password requested by device	A user requests a temporary recovery password form a device's locked screen.	---

Recovery Password viewed by Admin	An administrator has attempted to view a temporary recovery password issued for a user from the dashboard.	---
Recovery Password viewed by user	A user has attempted to view a temporary recovery password from the User Self Administration Portal. (This does not detect when the recovery password has been viewed through Outlook Web Access.)	---
Restricted device attempts to connect	A restricted device tries to access ActiveSync, File Share, or Managed Apps when these resources have been blocked.	---
Stop managing device issued by Admin	An administrator has issued a Selective Wipe command from the dashboard to a device.	---
Stop managing device issued by user	A user has issued a Selective Wipe command from the User Self Administration Portal to a device.	---
TouchDown policy override detection	The system issues a warning if it detects that a user has overridden the TouchDown settings governed by *ZENworks Mobile Management.*	---
User restricted	A user becomes restricted for any reason.	---
Wipe storage card	An administrator has issued a Wipe Storage Card command from the dashboard to a device.	---
System Alerts		
Apple Push Notification (APNs) Certificate Expiration	The APNs certificate approaches its expiration date. Default settings are to issue the reminder 30 days prior to the expiration and repeat it every day.	Reminder prior to expiration (Days)

Appendix C: Compliance Parameters Maintained by Novell, Inc.

Novell, Inc. maintains a *ZENworks Mobile Management* database. The database contains information/parameters for the *ZENworks Mobile Management* Compliance Manager. These parameters define the devices and device characteristics that *ZENworks Mobile Management* supports and provide *ZENworks Mobile Management* administrative users with sets and subsets of information through which they can restrict access to the *ZENworks Mobile Management* server.

Information maintained in this database includes:

- Supported Device Carriers
- Supported Device ActiveSync protocol versions
- Supported TouchDown Versions
- Supported Device Platforms
- Supported Device Manufacturers
- Supported Device Models
- Supported Device OS Versions

New entries are not added to these tables until they are first certified through a quality control process. The quality control process also determines when versions and models reach a point where they are no longer compatible and are removed from the tables.

Information from this database automatically synchronizes to the *ZENworks Mobile Management* server once every 24 hours. Administrators can initiate an update of this information by using the *Check For Updates* option

on the *Update Management* page of the dashboard. (***System*** > ***System Administration*** > ***Update Management*** > ***Manager*** > click the ***Check For Updates*** button.)

Table	Description	In the Dashboard
Device Carriers	A list of device carriers and their corresponding SMS gateways. *ZENworks Mobile Management* is currently limited to one SMS gateway per carrier. A carrier is required for SMS messages sent from *ZENworks Mobile Management* to administrators or users.	A drop-down list is available in Compliance Manager: Alert Recipients, Add Users (Manually), Edit Users, and Add/Edit Organization Administrators
ActiveSync Versions	A list of ActiveSync device protocol versions that *ZENworks Mobile Management* supports. New ActiveSync protocol versions are certified through Novell, Inc.'s quality control process before they are added to this list.	A drop-down list is available in Compliance Manager: Access Restrictions
TouchDown Versions	A list of TouchDown versions that *ZENworks Mobile Management* supports. Versions are added to this list when NitroDesk officially releases a new version to the Android Marketplace and it has been certified through Novell, Inc.'s quality control process.	A drop-down list is available in Compliance Manager: Access Restrictions
ActiveSync Device Type Lookup	ActiveSync devices might report the device platform through the ActiveSync protocol in a cryptic format. *ZENworks Mobile Management* maps what the device returns to the terms commonly used to identify device platform.	Mapped to *Device Platform*
iOS Model Lookup	iOS devices send their model name in a format that does not always match the name by which the device is commonly known. *ZENworks Mobile Management* maps what the device returns to the corresponding consumer name.	Mapped to *Device Model*
Device Platforms	A list of device platforms that *ZENworks Mobile Management* supports. Ties to the *ActiveSync Device Type Lookup* to determine platform.	Used in Compliance Manager: Device Platform Restrictions.
Device Manufacturers	A list of device manufacturers that *ZENworks Mobile Management* supports. Creates subsets for *Device Platform*.	A drop-down list is available in Compliance Manager: Device Platform Restrictions (Exceptions).
Device Models	A list of device models that *ZENworks Mobile Management* supports. Creates subsets for *Device Manufacturer*. Devices certified through Novell, Inc.'s quality control process are added to this list.	A drop-down list is available in Compliance Manager: Device Platform Restrictions (Exceptions).

Device OS Versions	A list of device operating system versions by platform that *ZENworks Mobile Management* supports. Creates subsets for *Device Models*. Device OS versions certified through Novell, Inc.'s quality control process are added to this list.	A drop-down list is available in Compliance Manager: Device Platform Restrictions (Exceptions).

Adding Non-Certified Devices to the Database

ZENworks Mobile Management incorporates a framework that allows the addition of non-certified devices to the compliance parameter tables. In future *ZENworks Mobile Management* versions, administrators will be able to add devices from the dashboard.

Until that time, database queries can be used to add device manufacturers, models, and operating systems not officially certified by the Novell, Inc. Please contact Novell Technical Support staff for assistance in adding non-certified devices.