NotifyMDM
Mobile Device Management

Configuration Guide: Compliance Manager

This guide provides information on . . .

. . . Configuring compliance Access Restrictions for an Organization

. . . Configuring the Alert Settings that trigger for non-compliant devices

. . . Placing a device on a connectivity watch list

Link to other configuration guides for information on . . .

. . . Organization Configuration and Management

. . . Adding Users and Enrolling Devices

Table of Contents

Accessing the Dashboard

Access the Dashboard

NotifyMDM dashboard requirements:

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

In your web browser, enter the server address of the *NotifyMDM* server followed by ***/dashboard***

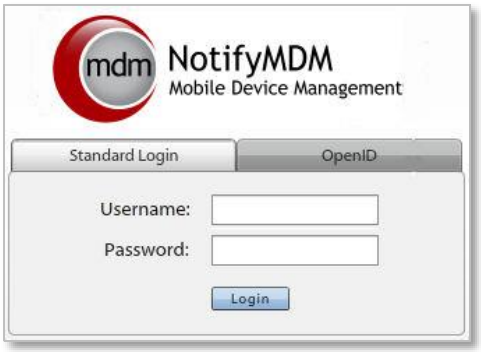
Example: https://company.mdm.server/dashboard

On-Demand users enter: https://ondemand.notifymdm.com/dashboard

Standard Login

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

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



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

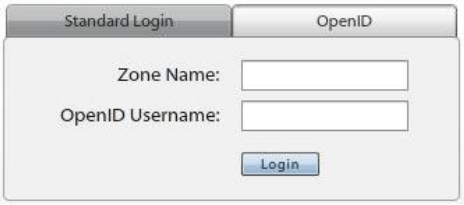
OpenID Login

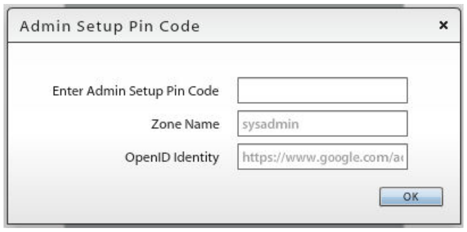
Use your OpenID credentials to log in.

1. At the *NotifyMDM* login screen, enter the **Zone Name**, an easy to remember name *NotifyMDM* uses to redirect you to the OpenID provider portal. If your provider requires it, enter your **OpenID Username** as well.
2. At the provider site, enter your OpenID credentials.

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

   Zone Name and new PIN codes are emailed to you from the *NotifyMDM* server.





Zone Name: sysadmin

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

Location of the Compliance Manager

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

Compliance Manager

Compliance Manager gives an administrator the ability to restrict access to ActiveSync and/or *NotifyMDM* 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 administrator set restrictions or specifications.

Non-Compliant Devices Can Be Restricted From:

- ActiveSync connections
- *NotifyMDM* corporate resources
    - File Share
    - Managed Apps
    - Network Access
- 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:

- *NotifyMDM* Server connections
- Select ActiveSync traffic, such as policy suite updates and wipe commands

When a device is found non-compliant, it is permitted to connect with the *NotifyMDM* 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 once it becomes compliant.

In most cases, the server automatically removes the restriction from a device that has returned to a compliant state. Several restriction breaches, however, require an administrator to release the device using one of the ***Clear*** options on the *Smart Devices and Users* grid:

- Clear ActiveSync Authorization Failures,
- Clear NotifyMDM Authorization Failures
- Clear Data Usage Statistics Reset by User Violation
- Clear SIM Card Removed or Changed Violation

Alert Settings

Alerts notify administrators of issues and events in the *NotifyMDM* system through the *View Alerts* grid on the dashboard (*Activity Monitor and Alerts*) and can be configured to alert administrators via email or SMS message. The system will 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.

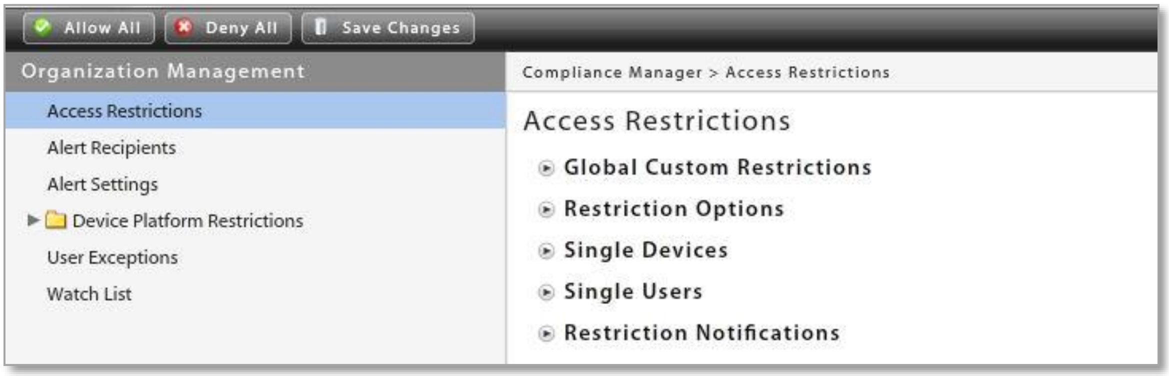
See Appendix B: Alert Settings for descriptions of the alerts.

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 be restricted as well.

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

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

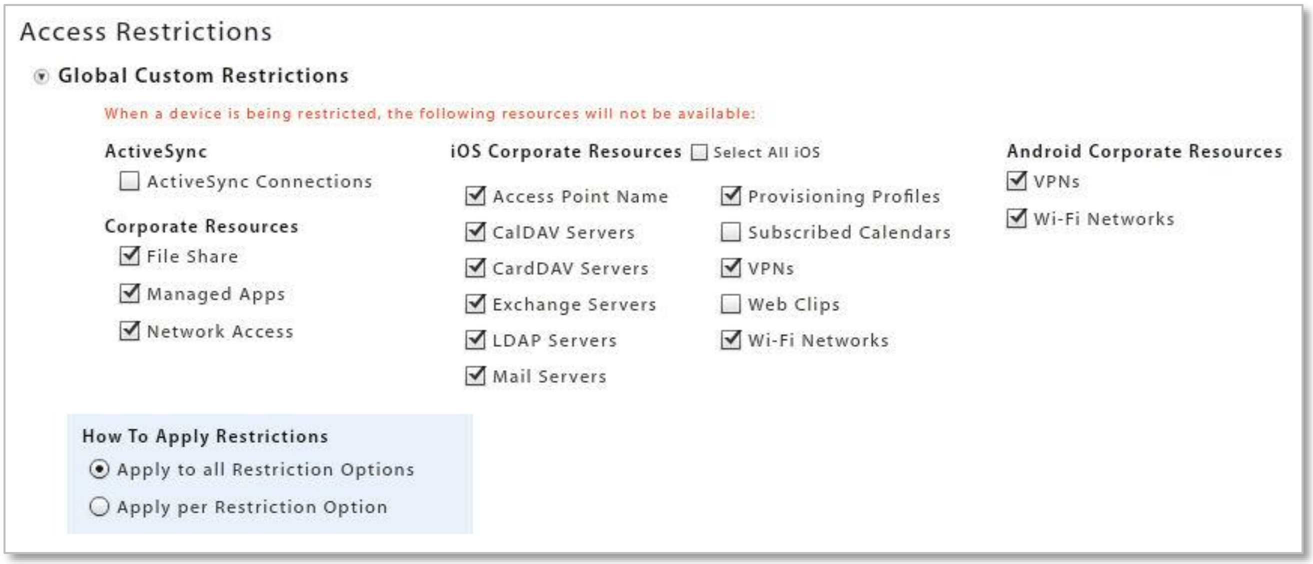


Set Global Restrictions or Define per Restriction Option

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

Select **Global Custom Restrictions**.

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



Access Restrictions

Global Custom Restrictions

When a device is being restricted, the following resources will not be available:

ActiveSync
- ☐ ActiveSync Connections

Corporate Resources
- ☑ File Share
- ☑ Managed Apps
- ☑ Network Access

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

Android Corporate Resources
- ☑ VPNs
- ☑ Wi-Fi Networks

How To Apply Restrictions
- ● Apply to all Restriction Options
- ○ Apply per Restriction Option

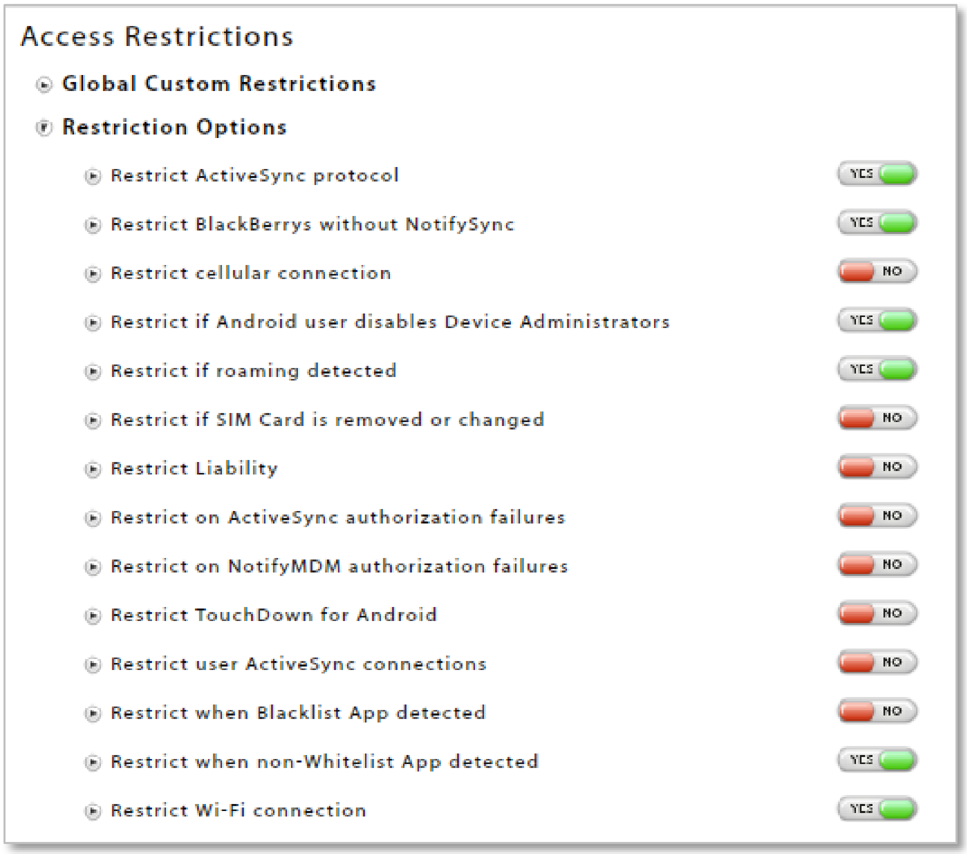
Configure the Access Restrictions

Select **Access Restrictions**.

Click the slider to enable (YES) or disable (NO) each restriction.

Click the **Save Changes** button.

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



Access Restrictions

Global Custom Restrictions

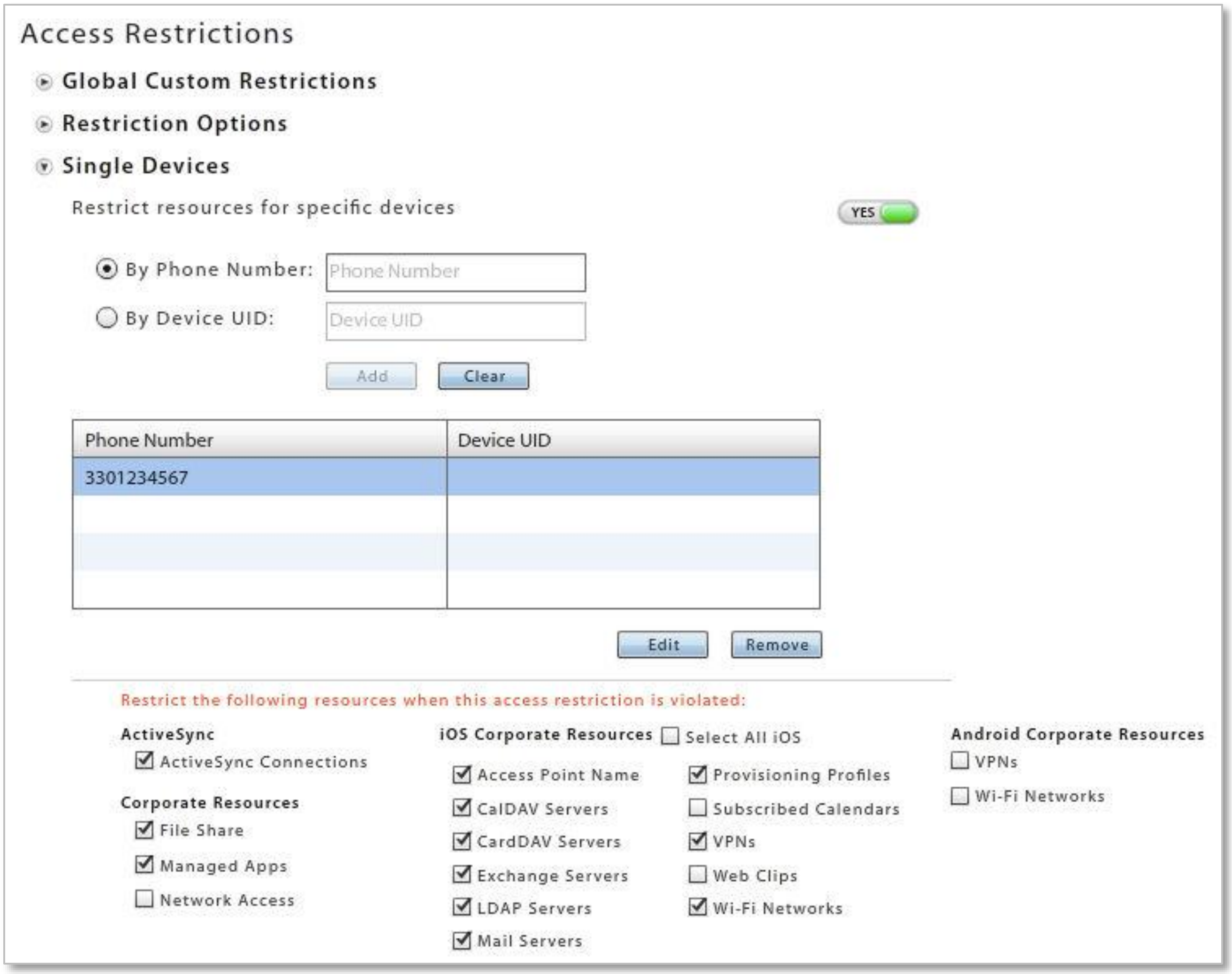
Restriction Options

Restrict ActiveSync protocol	YES
Restrict BlackBerrys without NotifySync	YES
Restrict cellular connection	NO
Restrict if Android user disables Device Administrators	YES
Restrict if roaming detected	YES
Restrict if SIM Card is removed or changed	NO
Restrict Liability	NO
Restrict on ActiveSync authorization failures	NO
Restrict on NotifyMDM authorization failures	NO
Restrict TouchDown for Android	NO
Restrict user ActiveSync connections	NO
Restrict when Blacklist App detected	NO
Restrict when non-Whitelist App detected	YES
Restrict Wi-Fi connection	YES

Restrict Single Devices

You may 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 which identifies the device.
4. Click the **Add** button.
5. If you are specifying the restricted resources for this device, check the appropriate boxes. If restricted resources have been assigned globally, this area will be gray.



Access Restrictions

- Global Custom Restrictions
- Restriction Options
- Single Devices

Restrict resources for specific devices: YES

● By Phone Number: Phone Number

○ By Device UID: Device UID

Phone Number	Device UID
3301234567	

Restrict the following resources when this access restriction is violated:

ActiveSync
- ☑ ActiveSync Connections

Corporate Resources
- ☑ File Share
- ☑ Managed Apps
- □ Network Access

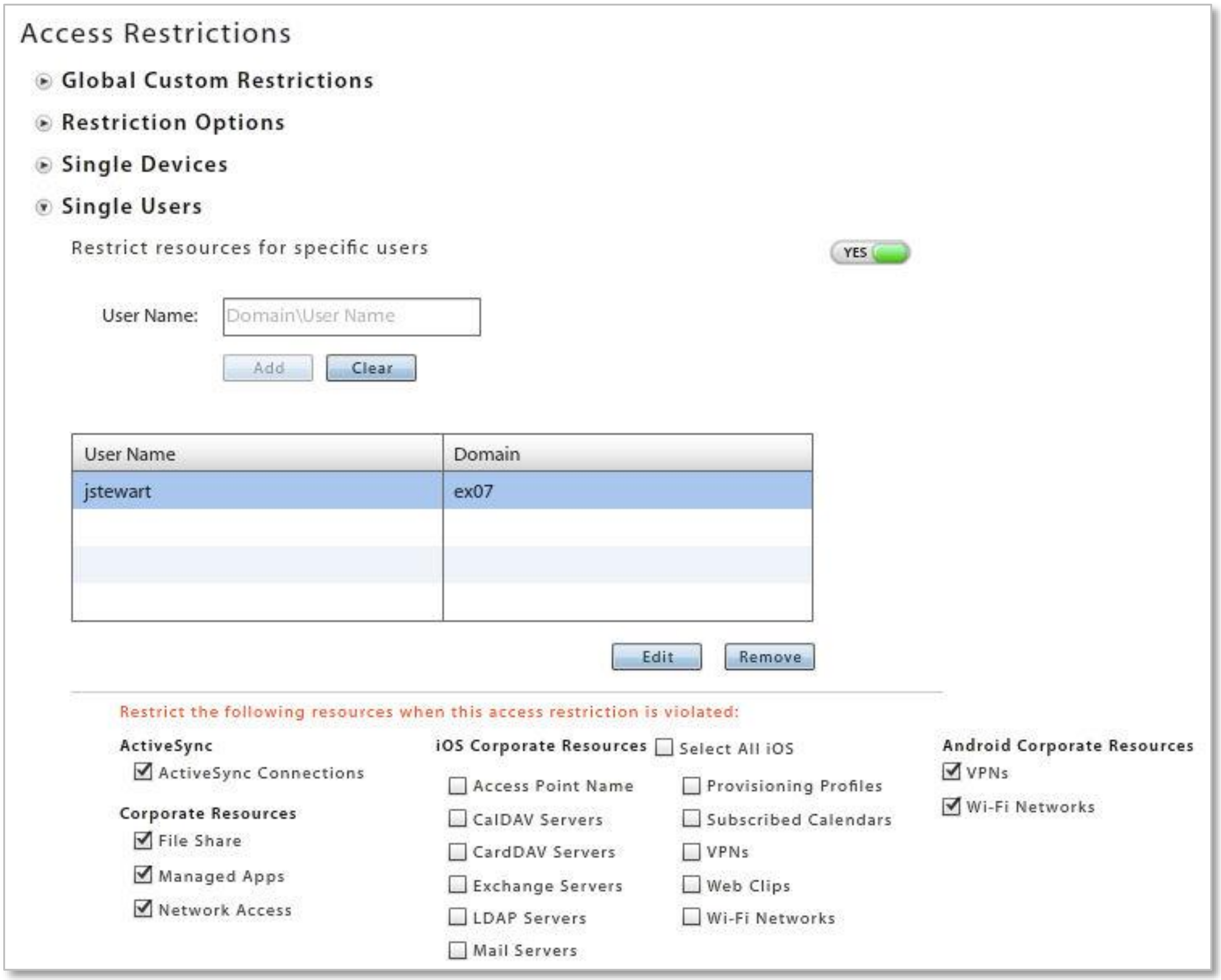
iOS Corporate Resources □ Select All iOS
- ☑ Access Point Name
- ☑ CalDAV Servers
- ☑ CardDAV Servers
- ☑ Exchange Servers
- ☑ LDAP Servers
- ☑ Mail Servers
- ☑ Provisioning Profiles
- □ Subscribed Calendars
- ☑ VPNs
- □ Web Clips
- ☑ Wi-Fi Networks

Android Corporate Resources
- □ VPNs
- □ Wi-Fi Networks

Restrict Single Users

You may 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 of the same user name, on different domains).
4. Click the **Add** button.
5. If you are specifying the restricted resources for this device, check the appropriate boxes. If restricted resources have been assigned globally, this area will be gray.



Restrict resources for specific users YES

User Name: Domain\User Name

User Name	Domain
jstewart	ex07

Restrict the following resources when this access restriction is violated:

ActiveSync
☑ ActiveSync Connections

Corporate Resources
☑ File Share
☑ Managed Apps
☑ Network Access

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

Android Corporate Resources
☑ VPNs
☑ Wi-Fi Networks

Device Platform Restrictions

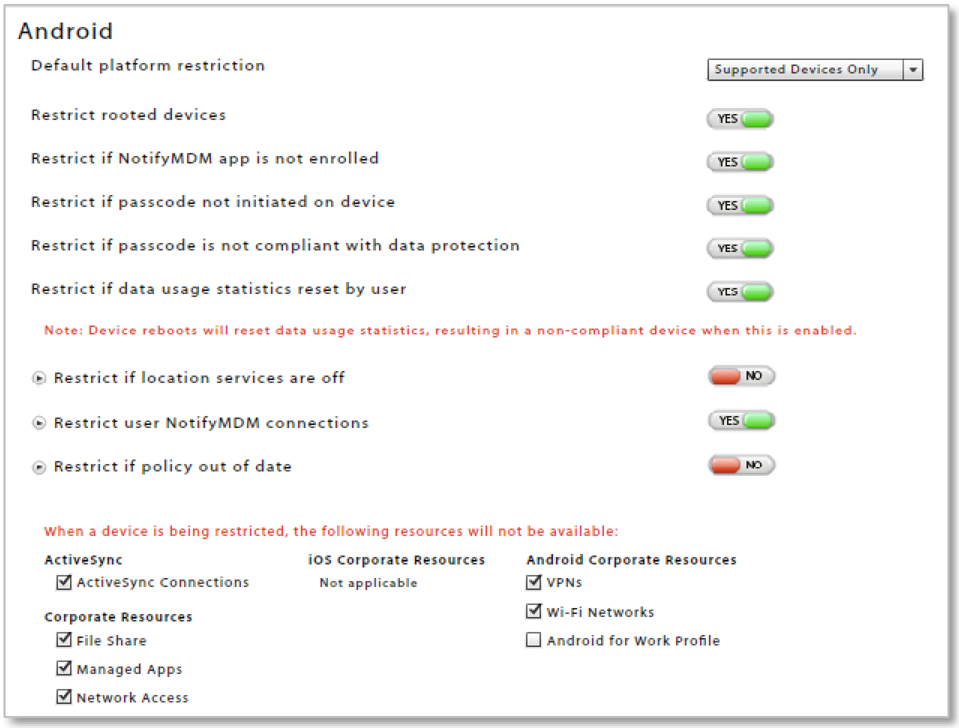
Define Restrictions

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 if the:
  - NotifyMDM App is not enrolled
  - Location is not updated
  - NotifyMDM connections are not occurring
  - Policy Suite is out of date
- Android and iOS devices can be restricted if they are rooted or jailbroken.
- iOS devices interfacing with a server that employs Apple's advanced MDM API 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-hand 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. Check 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.



Android

Default platform restriction: Supported Devices Only

Restrict rooted devices: YES

Restrict if NotifyMDM app is not enrolled: YES

Restrict if passcode not initiated on device: YES

Restrict if passcode is not compliant with data protection: YES

Restrict if data usage statistics reset by user: YES

Note: Device reboots will reset data usage statistics, resulting in a non-compliant device when this is enabled.

Restrict if location services are off: NO

Restrict user NotifyMDM connections: YES

Restrict if policy out of date: NO

When a device is being restricted, the following resources will not be available:

ActiveSync
☑ ActiveSync Connections

Corporate Resources
☑ File Share
☑ Managed Apps
☑ Network Access

iOS Corporate Resources
Not applicable

Android Corporate Resources
☑ VPNs
☑ Wi-Fi Networks
☐ Android for Work Profile

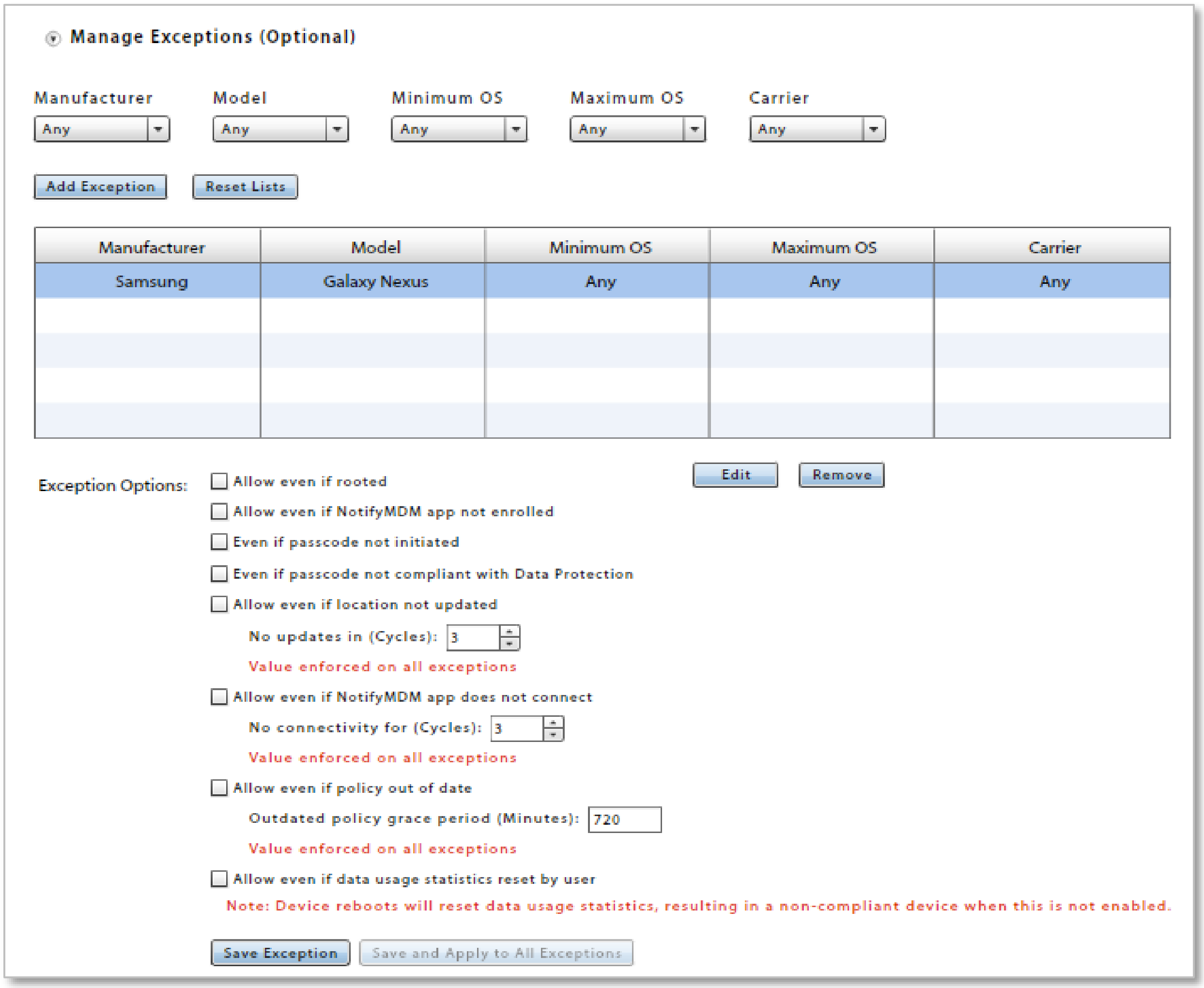
Manage Exceptions

Exceptions for *Device Platform Restrictions* can be used in two ways.

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. Choose the **Manufacturer**, **Model**, **Minimum** / **Maximum OS**, and/or **Carrier** for the device exception.
2. Click the **Add Exception** button.
3. If you are restricting all devices, but adding an exception, select any **Exception Options** you want to apply.
4. Click **Save Exceptions**.



Manage Exceptions (Optional)
Add Exception
Reset Lists
Edit
Remove
Save Exception
Save and Apply to All Exceptions

Manufacturer	Model	Minimum OS	Maximum OS	Carrier
Any	Any	Any	Any	Any

Manufacturer	Model	Minimum OS	Maximum OS	Carrier
Samsung	Galaxy Nexus	Any	Any	Any

Exception Options:

☐ Allow even if rooted

☐ Allow even if NotifyMDM app not enrolled

☐ Even if passcode not initiated

☐ Even if passcode not compliant with Data Protection

☐ Allow even if location not updated

No updates in (Cycles): 3

Value enforced on all exceptions

☐ Allow even if NotifyMDM app does not connect

No connectivity for (Cycles): 3

Value enforced on all exceptions

☐ Allow even if policy out of date

Outdated policy grace period (Minutes): 720

Value enforced on all exceptions

☐ Allow even if data usage statistics reset by user

Note: Device reboots will reset data usage statistics, resulting in a non-compliant device when this is not enabled.

Restriction Notifications

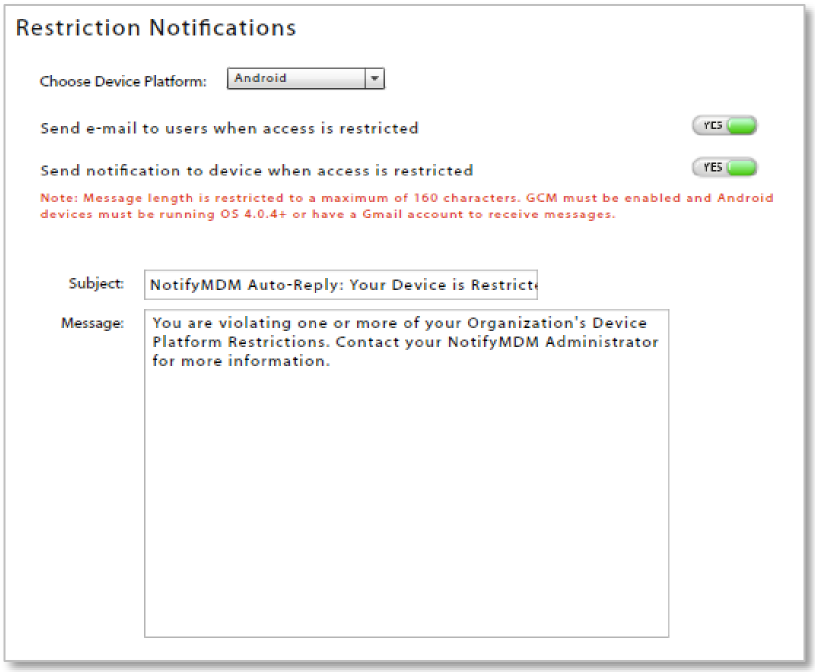
You have the option of sending a message notification pushed via APN/GCM* services and/or an email to users whose device is in violation of one of the *Access Restrictions* or *Device Platform Restrictions*.

*Notification messages apply only to Android and iOS devices.

1. Select **Access Restrictions** or **Device Platform Restrictions**.
2. Select **Restriction Notifications**.
3. Select a device platform from the drop-down list if you are composing a message for a *Device Platform Restriction* violation.
4. Click the slider so that it reads **YES** to enable the send email and/or the send notification option(s).
5. Compose or edit the subject (emails only) and body of the email/notification that will be sent to users in violation of one of the Access Restrictions or Device Platform Restrictions.

   Note: When *Send notification* is enabled, the message length is limited to 160 characters. For Android devices, GCM must be enabled and devices must be running OS 4.0.4+ or have a Gmail account.

6. Click the **Save Changes** button.



Restriction Notifications

Choose Device Platform: Android

Send e-mail to users when access is restricted YES

Send notification to device when access is restricted YES

Note: Message length is restricted to a maximum of 160 characters. GCM must be enabled and Android devices must be running OS 4.0.4+ or have a Gmail account to receive messages.

Subject: NotifyMDM Auto-Reply: Your Device is Restrict

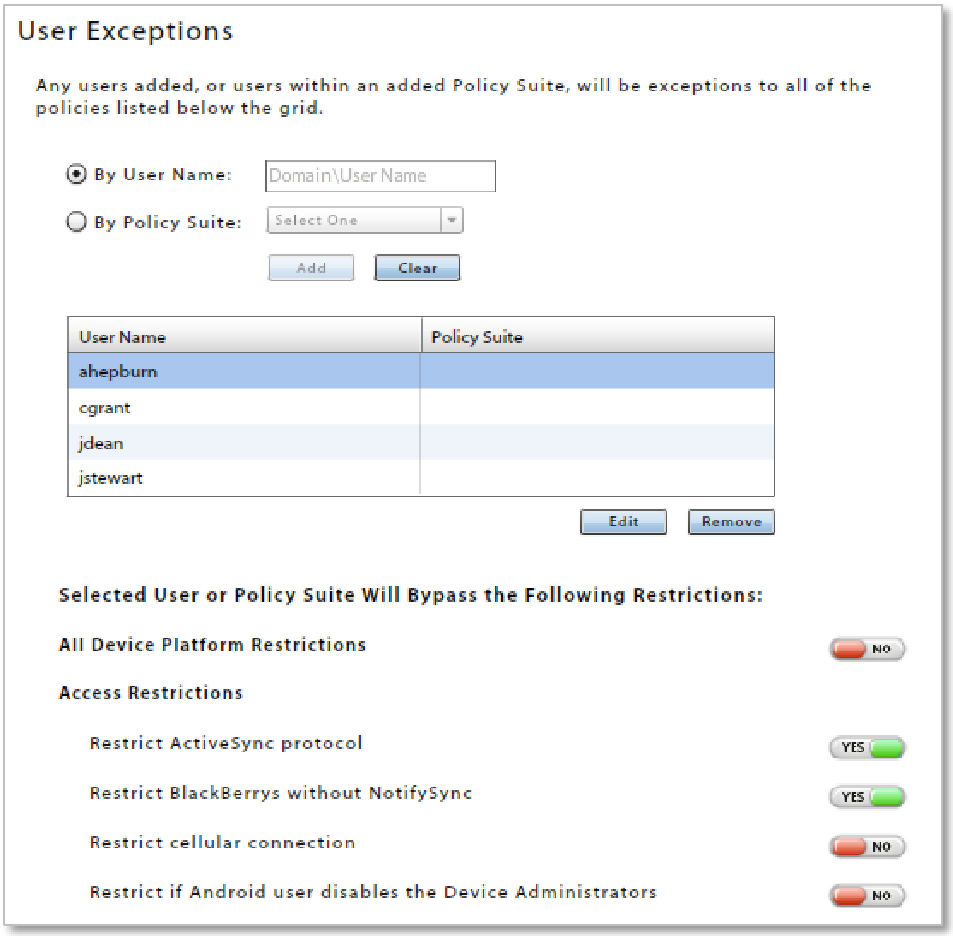
Message: You are violating one or more of your Organization's Device Platform Restrictions. Contact your NotifyMDM Administrator for more information.

User Exceptions

Select **User Exceptions** from the left-hand panel of the **Compliance Manager** page.

Once *Access Restrictions* and *Device Platform Restrictions* are configured, you may wish 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 **By User Name** or **By Policy Suite**. Enter a user name or select a policy suite from the drop-down list.
2. Click the **Add** button.
3. Highlight 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.
4. Click the **Save Changes** button.



User Exceptions

Any users added, or users within an added Policy Suite, will be exceptions to all of the policies listed below the grid.

● By User Name: Domain\User Name

○ By Policy Suite: Select One

User Name	Policy Suite
ahepburn	
cgrant	
jdean	
jstewart	

Selected User or Policy Suite Will Bypass the Following Restrictions:

All Device Platform Restrictions — NO

Access Restrictions

Restrict ActiveSync protocol — YES

Restrict BlackBerrys without NotifySync — YES

Restrict cellular connection — NO

Restrict if Android user disables the Device Administrators — NO

Managing Alert Settings

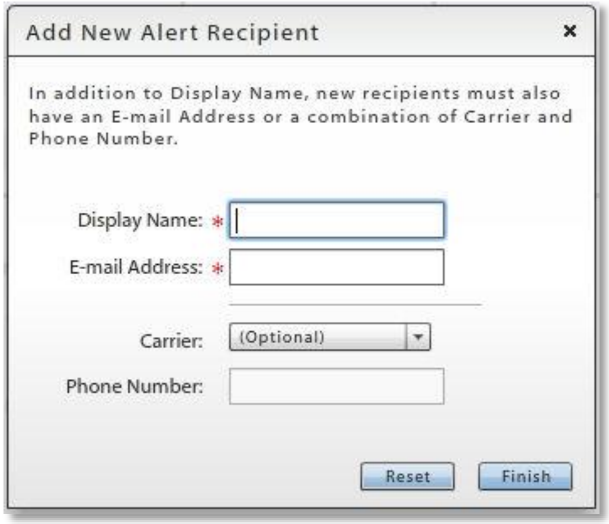
Alert Recipients

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 and Alerts** 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**.

Please note that if you intend to have a notifications sent as an **SMS**, you must supply the recipient's **Carrier** and **Phone Number** when you add them to the list.

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 wish the recipient to receive SMS notifications, you must 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.



Add New Alert Recipient

In addition to Display Name, new recipients must also have an E-mail Address or a combination of Carrier and Phone Number.

Alert Settings

Alerts notify administrators of issues and events in the *NotifyMDM* system. They are reported on the *Activity Monitor and Alerts* page of the dashboard in the *View Alerts* grid and can be configured to alert administrators via email or SMS message as well. 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

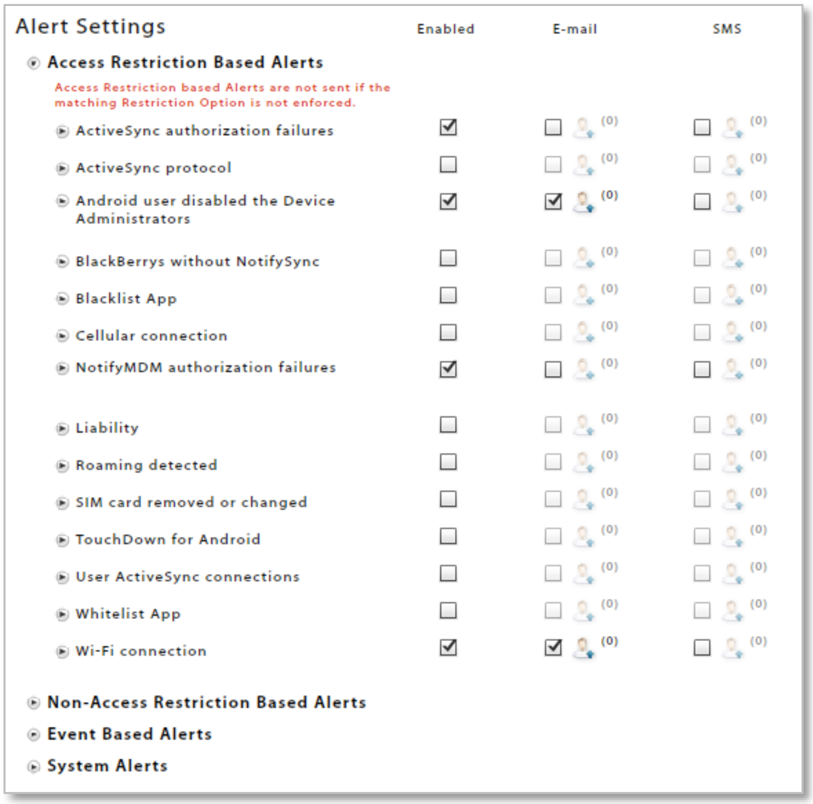
Four Categories of Alert Settings

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 Settings	Enabled	E-mail	SMS
Access Restriction Based Alerts			
Access Restriction based Alerts are not sent if the matching Restriction Option is not enforced.			
ActiveSync authorization failures	☑	☐ (0)	☐ (0)
ActiveSync protocol	☐	☐ (0)	☐ (0)
Android user disabled the Device Administrators	☑	☑ (0)	☐ (0)
BlackBerrys without NotifySync	☐	☐ (0)	☐ (0)
Blacklist App	☐	☐ (0)	☐ (0)
Cellular connection	☐	☐ (0)	☐ (0)
NotifyMDM authorization failures	☑	☐ (0)	☐ (0)
Liability	☐	☐ (0)	☐ (0)
Roaming detected	☐	☐ (0)	☐ (0)
SIM card removed or changed	☐	☐ (0)	☐ (0)
TouchDown for Android	☐	☐ (0)	☐ (0)
User ActiveSync connections	☐	☐ (0)	☐ (0)
Whitelist App	☐	☐ (0)	☐ (0)
Wi-Fi connection	☑	☑ (0)	☐ (0)
Non-Access Restriction Based Alerts			
Event Based Alerts			
System Alerts			

Alert Setting Parameters

Report Every (Minutes)

For all alerts, except those in the event based category, you will 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

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 will be 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

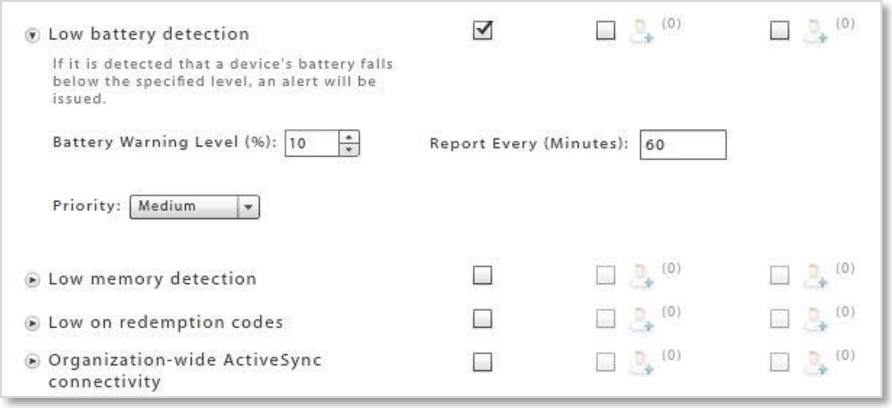
The system will not send alerts unless they are enabled. All alert settings are disabled by default.

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-hand panel of the **Compliance Manager** page.
2. Check the box in the **Enabled** column beside each of the alerts you want the system to issue. When a violation of an enabled setting is detected, the alert will be issued and displayed in the ***View Alerts*** grid.

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



Low battery detection	☑	□ (0)	□ (0)
Low memory detection	□	□ (0)	□ (0)
Low on redemption codes	□	□ (0)	□ (0)
Organization-wide ActiveSync connectivity	□	□ (0)	□ (0)

If it is detected that a device's battery falls below the specified level, an alert will be issued.

Battery Warning Level (%): 10

Report Every (Minutes): 60

Priority: Medium

4. Check the box in the **E-mail** column or the **SMS** column beside the alert if you wish 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 (1) 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 *NotifyMDM* application. You can also select a Policy Suite to watch, which will monitor 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. In **Alert Settings**, select **Non-Access Restriction Based Alerts** to enable **Watch List**.

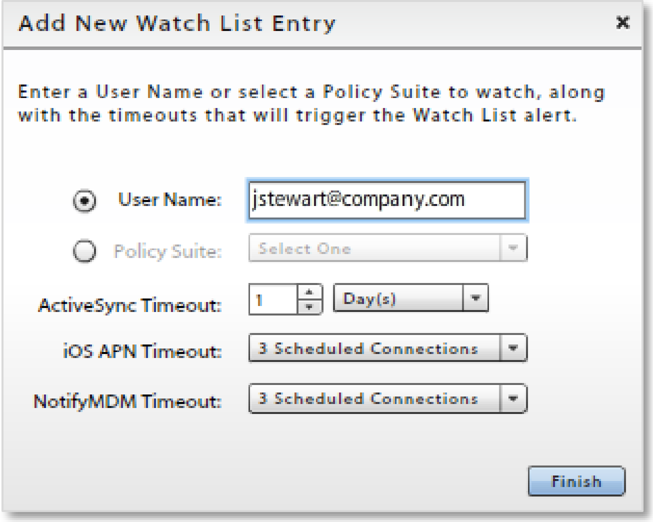
> **Please Note:** Devices in Direct Push mode, whose timeout intervals can vary in length, may not return results as consistently as devices in Scheduled Push mode. They may need to be on the watch list longer before results are reported.

1. Select **Watch List** from the left-hand 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. At **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. At **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. At **NotifyMDM Timeout**, select the number of NotifyMDM 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.



Add New Watch List Entry

Enter a User Name or select a Policy Suite to watch, along with the timeouts that will trigger the Watch List alert.

● User Name: jstewart@company.com

○ Policy Suite: Select One

ActiveSync Timeout: 1 Day(s)

iOS APN Timeout: 3 Scheduled Connections

NotifyMDM Timeout: 3 Scheduled Connections

Appendix A: Access Restrictions & Device Platform Restrictions

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

	Description **Restriction imposed when . . .**	**Configurable Options**	**Restricted Device is granted access when . . .**
Access Restriction			
Restrict ActiveSync protocol	A device cannot support sufficient ActiveSync policies, due to ActiveSync version support limitations with the device or server.	Minimum AS version:	NA
Restrict BlackBerrys without NotifySync	A BlackBerry device that does not have the *NotifySync* application has enrolled. Devices that have the *NotifySync* app, but not the *NotifyMDM* app will also trigger this restriction.	---	. . . the device is re-enrolled with *NotifySync*
Restrict 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	---	. . . the device changes its state

	Description Restriction imposed when . . .	Configurable Options	Restricted Device is granted access when . . .
	NotifyMDM connection.		
Restrict if Android user disables Device Administrators	An Android user has not granted device administrator privileges to the *NotifyMDM* app.	---	. . . the user enables Device Administration on the device
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** option.
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 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*** option.
Restrict on NotifyMDM authorization failures	A device passes invalid credentials for the NotifyMDM 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 NotifyMDM Authorization Failures** option.
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* timestamp has not updated within the	No connectivity for (Minutes):	. . . ActiveSync synchronization resumes

	Description Restriction imposed when . . .	Configurable Options	Restricted Device is granted access when . . .
	set interval.		
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 as 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. Can only be detected for BlackBerry devices currently using a Wi-Fi preferred network setting for NotifyMDM connection.	---	. . . the device ceases to use Wi-Fi
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 User Name, has been denied access.	User Name	. . . an Administrator permits access
Device Platform Restriction			
Restrict if NotifySync app is not enrolled	A BlackBerry device that does not have the *NotifySync* application has enrolled. Devices that have the *NotifySync* app, but not the *NotifyMDM* app will also trigger this restriction.	---	. . . the device is re-enrolled with *NotifySync*
Restrict if NotifyMDM app is not enrolled	A device enrolls via the native ActiveSync agent alone and without the *NotifyMDM* application.		. . . the device is re-enrolled with *NotifyMDM*
Restrict if location services are off	A device's location has not updated within the defined interval.	No updates in (Cycles):	. . . the device's location updates
Restrict user NotifyMDM connections	A device's *Last NotifyMDM Sync* timestamp has not updated within the set interval.	No connectivity for (Cycles):	. . .*NotifyMDM* synchronization resumes
Restrict if policy out of date	A policy suite has been updated on the	Outdated policy grace period	. . . the device downloads the

	Description Restriction imposed when . . .	Configurable Options	Restricted Device is granted access when . . .
	server, but a device has not updated within the set grace period.	(Minutes):	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 passcode not initiated on device	The user's Policy Suite requires a password, but the iOS or Android device does not have a passcode initiated.		. . . the user initiates the use of a passcode on the device
Restrict if passcode is not compliant with requirements	The user's Policy Suite requires a password, but the iOS or Android device does not have a passcode compliant with the requirements.		. . . the passcode is changed to something that is compliant with requirements
Restrict if passcode is not compliant with data protection	The iOS or Android device does not have a passcode and thus is not compliant with "data protection," which enhances the built-in hardware encryption by protecting the hardware encryption keys with the passcode.		. . . the passcode is set
Restrict if data usage statistics reset by user	The user of an Android or iOS device on which the data plan is being tracked, has manually reset the data usage statistics.		. . . an Administrator permits access via the **Clear Data Usage Statistics Reset by User Violation** option; or the end of the billing cycle occurs, the device is removed from the data plan, the device is removed and then added back to the same or a different data plan.
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	An iOS device has not loaded the iOS		. . . iOS APN profiles are

	Description Restriction imposed when . . .	Configurable Options	Restricted Device is granted access when . . .
not enrolled	APN configuration profile and has never synchronized through the Apple Advanced MDM API.		enrolled
Restrict if no iOS APN connectivity	A device's *Last iOS APN Sync* timestamp 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, please see the Device Platform Functionality matrix and reference the *Compliance Manager* section.

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, due to 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 *NotifyMDM* app.	---
BlackBerrys without NotifySync	A BlackBerry device that does not have the *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 NotifyMDM connection.	---
Liability	A device enrolls with a liability status specifically restricted by the *Restrict Liability* access restriction.	---
NotifyMDM authorization failures	A device passes invalid credentials for the *NotifyMDM*	---

Alert	Alert is issued when:	Alert Setting Parameters
	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* timestamp has not updated within the set interval.	---
Whitelist App	A device is blocked because it has an 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. Can only be detected for BlackBerry devices currently using a WiFi preferred network setting for NotifyMDM connection.	---
Non-Access Restriction Based Alerts		
Android rooted device	A rooted Android device connects to the *NotifyMDM* server.	---
Android passcode not initiated	The user's Policy Suite requires a password, but the Android device does not have a passcode initiated.	---
Android passcode not compliant with data protection	The Android device does not have a passcode and thus is not compliant with "data protection," which enhances the built-in hardware encryption by protecting the hardware encryption keys with the passcode.	---
NotifyMDM app is not enrolled	A device of any platform type connects to the server via ActiveSync and does not have the *NotifyMDM* application enrolled.	---

Alert	Alert is issued when:	Alert Setting Parameters
iOS jailbroken	A jailbroken iOS device connects to the *NotifyMDM* 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* timestamp 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 requirements	The user's Policy Suite requires a password, but the iOS 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/or device encryption, but the iOS device does not have a passcode and/or does not have encryption set.	---
iOS unmanaged configuration profile	An iOS device has an unmanaged configuration profile (one 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 application availability	A managed application purchased in bulk is close to its availability limit (download limit or number of available licenses/redemption codes. Alert is generated for any managed app that is: -Low on redemption codes -Low on VPP licenses -Low on Download Limit	**Remaining Application Count**
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

Alert	Alert is issued when:	Alert Setting Parameters
		available memory falls below the specified megabytes. **Memory Warning Level (%) -** For devices with a memory capacity greater than 100 MB, warning occurs if available memory falls below the specified percentage.
Organization-wide ActiveSync connectivity	The *Last ActiveSync Sync* timestamp has not updated for any users within the set interval. Default is 720 minutes.	**No Connectivity for (minutes)**
Organization-wide NotifyMDM connectivity	The *Last NotifyMDM Sync* timestamp 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.	---
User's e-mail not set	A user's email address has not been set. *Since 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 NotifyMDM connections	A device's *Last NotifyMDM Sync* timestamp has not updated within the set interval.	---
Watch List	A user or Policy Suite on the Watch List grid has exceeded the time for which he/she/it was being monitored.	---
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.	---
Clear passcode issued by Admin	An administrator has issued a *Clear Passcode* 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 their device.	---

Alert	Alert is issued when:	Alert Setting Parameters
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 their 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. *(Please note, this does not detect when the recovery password have been viewed through OWA.)*	---
Reset for enrollment	An administrator has issued a *Rest for Enrollment* from the dashboard to a device.	---
Restricted device attempts to connect	A restricted device tries to access ActiveSync or corporate network, File Share, or Managed Apps when these resources have been blocked.	---
Selective wipe issued by Admin	An administrator has issued a *Selective Wipe* command from the dashboard to a device.	---
Selective wipe issued by user	A user has issued a *Selective* command from the User Self Administration Portal to their device.	---
TouchDown policy override detection	The system issues a warning if it detects that a user has overridden the TouchDown settings governed by *NotifyMDM*.	---
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.	---
Reboot issued by Admin	An administrator has issued a Reboot command from the	---

Alert	Alert is issued when:	Alert Setting Parameters
	dashboard to a device. (Samsung KNOX devices only.)	
Power off issued by Admin	An administrator has issued a Power Off command from the dashboard to a device. (Samsung KNOX devices only.)	---
Unblock password entry issued by Admin	From the dashboard, an administrator has unblocked the password entry on a device blocked due to a password policy violation. (Samsung KNOX devices only.)	---
Reboot issued by user	A user has issued a Reboot command from the User Self Administration Portal to a device. (Samsung KNOX devices only.)	---
Power off issued by user	A user has issued a Power Off command from the User Self Administration Portal to a device. (Samsung KNOX devices only.)	---
Unblock password entry issued by user	From the User Self Administration Portal, a user has unblocked the password entry on a device blocked due to a password policy violation. (Samsung KNOX devices only.)	---
Reset to Shared Profile issued by Admin	An administrator has issued the *Reset to Shared Profile* command from the dashboard to a shared device signed in to by an individual user.	---
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 Notify Technology Corporation

Notify Technology Corporation maintains a *NotifyMDM* database in its SAS 70 certified data center. The database contains information/parameters for the *NotifyMDM* Compliance Manager. These parameters define the devices and device characteristics that *NotifyMDM* supports and provide *NotifyMDM* administrative users with sets and subsets of information through which they can restrict access to the *NotifyMDM* 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 Notify Technology Corporation quality control process. Likewise, the quality control process 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 *NotifyMDM* server once every 24 hours, when the server license validation occurs. Administrators can initiate an update of this information, as well, by using the *Validate License* option. **System Administration** > **Organization** > click the **Validate License** button.

Table	Description	In the Dashboard
Device Carriers	A list of device carriers and their corresponding SMS gateways. *NotifyMDM* is currently limited to one SMS gateway per carrier. Carrier is required for SMS messages sent from *NotifyMDM* to administrators or users.	Drop-down lists occur in Compliance Manager: Alert Recipients, Add Users (Manually), Edit Users, and Add/Edit Organization Administrators
ActiveSync Versions	A list of ActiveSync device protocols versions that *NotifyMDM* supports. New ActiveSync protocol versions are certified through Notify Technology's quality control process before they are added to this list.	Drop-down list occurs in Compliance Manager: Access Restrictions
TouchDown Versions	A list of TouchDown versions that *NotifyMDM* supports. Versions are added to this list when NitroDesk officially releases a new version to the Android Marketplace and it has been certified through Notify Technology's quality control process.	Drop-down lists occur in Compliance Manager: Access Restrictions
ActiveSync Device Type Lookup	ActiveSync devices may report device platform through the ActiveSync Protocol in a cryptic format. *NotifyMDM* maps what the device returns to the terms used commercially 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 known commercially. *NotifyMDM* maps what the device returns to the corresponding consumer name.	Mapped to *Device Model*
Device Platforms	A list of device platforms that *NotifyMDM* 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 *NotifyMDM* supports. Creates subsets for *Device Platform*.	Drop-down list occurs in Compliance Manager: Device Platform Restrictions (Exceptions).
Device Models	A list of device models that *NotifyMDM* supports. Creates subsets for *Device Manufacturer*. Devices certified through Notify Technology's quality control process are added to this list.	Drop-down list occurs in Compliance Manager: Device Platform Restrictions (Exceptions).
Device OS Versions	A list of device operating system versions by platform that *NotifyMDM* supports. Creates subsets for *Device Models*.	Drop-down list occurs in Compliance Manager: Device Platform Restrictions (Exceptions).

	Device OS versions certified through Notify Technology's quality control process are added to this list.	

Adding Non-Certified Devices to the Database

NotifyMDM incorporates a framework that will allow the addition of non-certified devices to the compliance parameter tables. In future *NotifyMDM* 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 Notify Technology Corporation. Please contact Notify Technology Corporation Technical Support staff for assistance in adding non-certified devices.