NotifyMDM
Mobile Device Management

NotifyMDM Server Release Notes

Table of Contents

NotifyMDM Server Release Notes

The *NotifyMDM* server is a component of Notify Technologies MDM system that serves as a management and policy enforcement platform for mobile devices.

NotifyMDM was designed to enable Administrators to keep device users up-to-date with company security policies and management features, ensuring confidentiality and integrity of wirelessly transmitted corporate information. This is accomplished by communicating with the NotifyMDM device applications and also by using the ActiveSync protocol.

This document provides a history of releases including dates, known issues, and notes for the NotifyMDM administrator.

Revision History

Date	Author	Description of Changes
2018.5.2	Tom Walker	3.11.4 Release
2017.11.6	Tom Walker	3.11.3 Release
2017.8.20	Tom Walker	3.11.2 Release
2017.15.1	Tom Walker	3.11.1 Release
2017.15.1	Tom Walker	3.11.0 Release
2016.9.25	Tom Walker	3.10.4 Release
2016.9.19	Tom Walker	3.10.3 Release
2016.9.12	Tom Walker	3.10.3 Release
2016.9.12	Tom Walker	3.10.2 Release
2016.5.16	Tom Walker	3.10.1 Release
2016.5.16	Tom Walker	3.10.0 Release
2015.08.31	Anthony Costello	3.9.2 Release
2015.07.29	Anthony Costello	3.9.1 Release
2015.07.08	Anthony Costello	3.9.0 Release
2015.04.13	Anthony Costello	3.8.1 Release
2015.03.09	Anthony Costello	3.8.0 Release
2015.03.09	Anthony Costello	3.7.2 Release
2014.11.10	Anthony Costello	3.7.1 Release
2014.10.06	Anthony Costello	3.7.0 Release
2014.6.16	Anthony Costello	3.6.3 Release
2014.5.27	Anthony Costello	3.6.2 Release
2014.4.28	Anthony Costello	3.6.1 Release
2014.4.07	Anthony Costello	3.6.0 Release

2014.2.13	Anthony Costello	3.5.2 Release
2014.2.10	Anthony Costello	3.5.1 Release
2014.1.13	Anthony Costello	3.5.0 Release
2013.12.9	Anthony Costello	3.4.1 Release
2013.12.2	Anthony Costello	3.4.0 Release
2013.09.26	Anthony Costello	Added Known Issue: - Hands-off enrollment issue with iOS 7 devices. [11889]
2013.09.19	Anthony Costello	3.3.2 Release
2013.09.16	Anthony Costello	3.3.1 Release
2013.09.03	Anthony Costello	3.3.0 Release
2013.08.29	Anthony Costello	3.2.1 Release
2013.08.19	Anthony Costello	3.2.0 Release
2013.08.05	Anthony Costello	3.1.1 Release
2013.07.29	Anthony Costello	3.1.0 Release

Revision History

2013.07.08	Anthony Costello	3.0.0 Release
2013.07.08	Anthony Costello	2.8.5 Release
2013.06.25	Anthony Costello	2.8.4 Release
2013.06.10	Anthony Costello	2.8.3 Release
2013.04.22	Thomas Burkett	2.8.2 Release
2013.04.22	Anthony Costello	2.8.1 Release
2013.04.08	Anthony Costello	2.8.0 Release
2013.02.25	Anthony Costello	2.7.1 Release
2013.02.19	Anthony Costello	2.7.0 Release
2012.12.10	Anthony Costello	2.6.1 Release
2012.10.29	Anthony Costello	2.6.0 Release

2012.08.13	Anthony Costello	2.5.5 Release
2012.07.23	Anthony Costello	2.5.4 Release
2012.07.23	Anthony Costello	2.5.3 Release
2012.07.16	Anthony Costello	2.5.2 Release
2012.04.13	Thomas Burkett	2.3.0 Release
2012.03.28	Matt Zimmerman	2.2.0 Release
2012.03.13	Matt Zimmerman	2.1.1 Release
2012.03.08	Matt Zimmerman	2.1.0 Release Added Known Issue - Clearing violation [8049] - Locking the main configuration profile [7783] - Instances when you have to reload your configuration profiles [7649]
2012.02.09	Jodie Grazier	2.0.1 Release
2012.02.09	Jodie Grazier	2.0.0 Release Added Known Issue: - Dashboard initial load [7548] - Multiple tabs connected to same Dashboard [7583]
2012.01.25	Jodie Grazier	1.9.3 Release Update link in Known Issues – Kerio
2012.01.06	Jodie Grazier	NotifyMDM for iOS v1.9.2 release. Corrects issue 7364.

Revision History

2011.12.29	Jodie Grazier	1.9.2 Release
2011.12.06	Jodie Grazier	1.9.1 Release
2011.12.06	Jodie Grazier	1.9.0 Release
2011.11.16	Jodie Grazier	Added Known Issues: - Issues with searching in the dashboard - ActiveSync URL containing slashes [6711] - Redirects not handled correctly [6965]
2011.10.07	Jodie Grazier	1.8.4 Release
2011.09.23	Jodie Grazier	1.8.3 Release

2011.09.20	Jodie Grazier	1.8.2 Release
2011.09.01	Jodie Grazier	1.8.1 Release
2011.08.09	Jodie Grazier	1.8.0 Release Added Known Issue: - Permissions required to run Update Manager application [5197]
2011.07.12	Jodie Grazier	1.7.0 Release Added Known Issues: - Changing organization name [5445] - Short device connection schedules [5381] - Clear Passcode action [5194] - Synchronization of Current Carrier Network [5136]
2011.07.08	Jodie Grazier	Added Known Issues: - MS KB2509553 [5563] - TouchDown and Hands-Off registration [5636]
2011.06.21	Jodie Grazier	1.6.0 Release
2011.05.23	Jodie Grazier	1.5.1 Release
2011.04.19	Jodie Grazier	Added Known Issues and subcategorized the section.
2011.04.04	Jodie Grazier	1.5.0 Release

Installation Information

Date: 07/08/2015

Product: NotifyMDM Server

Requirements

This is a brief summary of the requirements; see the Installation Guide for the full set of requirements.

- Windows Server 2012 R2 / 2012 / 2008 R2 SP1 / 2008 with SP2 / 2003 R2 x64 / 2003 **Note:** Windows Server 2003 is no longer supported after NotifyMDM 3.8.0. - Including Microsoft IIS
  - Apply all Windows Server updates
- Microsoft SQL Server 2014, 2012, 2008 R2 SP1 (Standard Edition), 2008 R2 (Standard Edition), 2008 SP3 (Standard Edition), 2008 SP1 (Standard Edition) Microsoft SQL 2008 Web Edition OR Microsoft SQL Express 2008 (Supported for product evaluations; Not recommended for production)
- An SMTP Server

Version Support Policy

Last Updated: 2016.5.16

Server Software. Notify Technology Corporation provides support for the current *NotifyMDM* production version and one (1) previously released production version. In addition, periodic hotfix enhancements may be provided for the most recent release of the current production version. Production versions that are two (2) releases behind the current Generally Available release are considered by Notify Technology Corporation to have reached their "end of life" and are no longer supported.

NotifyMDM 3.10.1 is the most current production version. Versions 3.9.1, 3.9.0, 3.8.1, and 3.8.0 are also currently supported. Versions older than 3.8.0 have reached end-of-life status.

Device Application Software. The current production version of *NotifyMDM* server software (3.10.1) supports device application software versions 3.7.0 and higher.

Installation Package

Name	Version
smailpp.dll	2.4.0.21
ntc_mdm_AdminAuthenticator.dll	3.9.0
ntc_mdm_AdminRoles.dll	3.9.0
ntc_mdm_AirProxy.dll	3.9.0
ntc_mdm_AirSyncParser.dll	3.9.0
ntc_mdm_APN.dll	3.9.0
ntc_mdm_AutoEmailChecker.dll	3.9.0
ntc_mdm_BaseQueryOffloader.dll	3.9.0
ntc_mdm_CommandBase.dll	3.9.0

ntc_mdm_ConfigFileReader.dll	3.9.0
ntc_mdm_CriticalLogger.dll	3.9.0
ntc_mdm_DatabaseInterface.dll	3.9.0
ntc_mdm_DatabaseLogger.dll	3.9.0
ntc_mdm_DatabaseLoggerWrapper.dll	3.9.0
ntc_mdm_DatabaseTaskScheduler.dll	3.9.0
ntc_mdm_HTTPInterface.dll	3.9.0
ntc_mdm_IOSMDMParser.dll	3.9.0
ntc_mdm_IOSMDMSync.dll	3.9.0
ntc_mdm_ISAPIRedirectFilter.dll	3.9.0
ntc_mdm_Jobs.dll	3.9.0
ntc_mdm_Licensing.dll	3.9.0
ntc_mdm_MailComposer.dll	3.9.0
ntc_mdm_MDMParser.dll	3.9.0
ntc_mdm_MDMSocket.dll	3.9.0
ntc_mdm_MDMSync.dll	3.9.0
ntc_mdm_SMTP.dll	3.9.0
ntc_mdm_WBXMLParser.dll	3.9.0

Known Issues

NotifyMDM Server

1. The NotifyMDM installation package should be downloaded on the system to which it will be installed. If the package is downloaded to a different system and then transferred over a network to the NotifyMDM system, the installation may produce popup warnings about 'Unknown Publisher'.
2. The NotifyMDM product is not currently localized. Using non-English text in the dashboard may result in unexpected display of the text. [2037]
3. If the web component of the NotifyMDM server must be moved to a different server or install directory, special steps must be taken with the MDM.ini file. Please contact Technical Support for more information. [1434]
4. Because of the following issue, it is recommended that Windows security update KB2509553 not be installed on a Windows Server 2003 x64 box where NotifyMDM will be installed. If the Windows security update KB2509553 is installed on a Windows Server 2003 x64 box, the NotifyMDM SQL Database install will not work properly. [5563]
5. An initially long load time can be experienced upon the first visit to the Dashboard. You will also experience this upon clearing your browser cache as the Dashboard reloads the entire Flash file. [7548]
6. When logged into the Dashboard on multiple tabs within a browser, logging out on one tab will cause a session error on the other tabs connected to that server. [7583]

7. ActiveSync server address URLs that contain a slash are not handled properly. This has been observed with Lotus Traveler and with Google Apps Premier. This has been corrected in NotifyMDM v1.9.0. [6711]
8. Redirects are not handled properly, specifically for the ActiveSync server address URL. A possible workaround is to put the redirect address in as the ActiveSync server address. [6965]
9. The organization name should NOT be changed, in particular if the iOS APNs certificate is being used. If the organization name is changed, policy changes and Selective Wipes could fail. [5445]
10. Some aspects of the searching capabilities are not currently working. In the User Profile:
    a. Searching for text in an SMS/MMS does not return results [2875]
    b. Searching for an SMS/MMS or phone record by phone number must match the record exactly. For example, if the record contains a country code, the search criteria must also include the country code. [3722 / 3365]
    c. Searching Group Email
        i. When searching the Subject, the text must match exactly in order to return results [5212] ii. When searching the Body, no results are returned. [3294]

    In NotifyMDM v1.9.0, the searches that are not working correctly have been disabled.
11. If an iOS device is actively displaying the 'Enter Passcode' screen while the Clear Passcode is issued, the Clear Passcode does not take effect until the screen is turned off and back on again. [5194]
12. When using the iOS APNs certificate, the Current Carrier Network is not being returned properly by the device. [5136]
13. The Windows administrator user logged in when running the Update Manager application must have a login with UAC in "silent mode". The default administrator account for a server will run this way. If "silent mode" is not enabled for a given administrator, they will not be able to apply updates. [5197]
14. The configuration profile of an iOS device enrolled as a secondary or tertiary device in a single user account will be modeled after the primary device. Therefore, iOS users should continue to use the multiple device enrollment method used for NotifyMDM version 1.9.1 or less (i.e. use of aliases) until NotifyMDM for iOS app version 1.9.2 is installed on the device. [7364]
15. Clearing a violation on a single device will clear the violation on all devices for that user. [8049]
16. When setting Administrator Role permissions in the dashboard, when the user who is logged in and applying the permission to the role that they are using, the user must log out and log back in for the new role permissions to take effect. [8633]
17. A recent or currently restricted admin has the ability to view cached pages within the dashboard after their Administrator Role has been restricted from viewing the information. [8639]
18. When exporting logs, only the records that have currently loaded within the data grid are exported. To get all of the data, a user would have to repeatedly scroll to the bottom of the data grid in order to export all desired records. [8709]
19. When exporting reports, the user must expand all data within the grid to ensure all the data that is in the report is exported. [8744]
20. When "Allow Profile Removal" is set to 'Never' under the iOS Settings of the policy and the APN certificate has been disabled, after enrolling an iOS device, the user will not be able to remove the MDM iOS Mobile Configuration Profile. [8754]
21. When installing the NotifyMDM server and a local path is already present for the default web site, the local path is not overwritten for the new installation of the Web component. [8796]
22. Running a database task manually does not generate an entry in the Database Task Scheduler log. [8819]
23. Depending on the settings within the particular .swf file that is being uploaded as a plug-in, it's possible for the dashboard to take on the scaling options of the plug-in itself rather than retain its own. This can occur with the upload of the .swf file and not by using a URL. [8850]
24. When using server side Autodiscover, there it is a possible for an infinite loop of Autodiscovering to occur if the Autodiscover server is the NMDM server. [9615]
25. After running the 2.6.0 update, all of the pre-existing location times become for the Server Local Time will show the time of when the update was performed. [9694]
26. When adding a user through LDAP whose policy settings are via a group or folder, when the user is removed from the LDAP server, the user remains on the NotifyMDM server, as it should, but keeps it's settings from the group or folder. [10518]

27. Currently, Groups that do not contain a member attribute can be imported via LDAP into the dashboard. When using a group without a member attribute, it will not work properly and return an error about an invalid username or password. [10812, 10829]
28. The administrator alert message sent when a “Stop Managing Device” command has been issued reads, “The Enrollment has been reset for <username>.” In an upcoming version, this will be corrected with a message that properly describes the event. [11330]
29. If users have enrolled via SAML and the SAML server is subsequently disabled, users will be unable to retrieve managed apps since accessing managed apps still requires the entry of the SAML user and password.
30. **Web Clusters**
    a. In order to support cookies working across multiple physical web servers, we will be supporting saving sessions on a central machine using memcached. (Please see our Web Cluster setup guide for more information regarding memcached setup.)
    b. NOTIFYMDM server upgrades may overwrite the php.ini changes done for memchached. Administrators will want to be aware of this and adjust accordingly after upgrading.
    c. For plugins and custom logos to function reliably, files for the following two directories must be placed on all web servers and the install paths must match.
        i. <install path>web\dashboard\images\CustomLogos
        ii. <install path>web\dashboard\plugins\
    d. If you have configured a web cluster on your system (supported in v3.7.0+), subsequent upgrades of NOTIFYMDM must be done on each server in the cluster. It is recommended that servers are updated one at a time and that you allow each update to complete before beginning an update on another server in the cluster.
    e. If you have configured a web cluster on your system (supported in v3.7.0+) and are running or would like to run in a Linked Server environment with NLES, both the MDM.ini and UserConfig.ini files need updated and must match across each web server in the cluster. IIS must be restarted on each web server after changes are made.
31. When adding multiple users to a local group, moving in excess of 600 users from the “Available” column to the “Assigned” column causes a timeout before the transfer can complete. Thus, the administrator is unable to update the group. Moving 600 or less users at a time does not cause the issue.

Android Devices

1. When NotifyMDM is interfacing to an ActiveSync server that is set to not allow nonprovisionable devices, some Android devices may not be able to register. This has been experienced with devices running OS 2.2.1 (but not HTC Sense devices), however this may apply to other devices. [1957]
2. Hands-off registration should not be used for Android devices with TouchDown. When using handsoff registration, initiating TouchDown registration through NMDM app does not work properly. [5636]
3. Android devices may fail to download attached files which are 33 MB or larger. This seems to be a device limitation and an error message stating “Unable to display file due to insufficient memory” is expected behavior. [10788]
4. The “Allow sharing clipboard between applications” policy does not work on Samsung tablets.
5. When using Samsung KNOX™ Device on a Galaxy S5, we have seen an issue with adding an app in kiosk mode where the app shortcut is not created when that app is already being managed on the NotifyMDM server.
6. The Samsung Galaxy Tab 3 does not adhere to the KNOX™ Device HTTP Proxy Browser policy.
7. The Samsung KNOX™ Device policy “Allow installation of non-trusted apps” currently allows the installation of any app regardless of what the slider is set to in the Dashboard. This is an issue that needs addressed in the KNOX™ Device API by Samsung.
8. The serial number displayed on an Android device may not necessarily match the serial number that it returns to the NotifyMDM server. Thus, what is displayed on the device may not match what is displayed in the NotifyMDM Dashboard.
9. **Samsung KNOX™**

a. When the “Require encryption on the SD card” policy via KNOX™ Device is enforced, the device will not prompt the user to encrypt the SD card until a reboot of the device is performed.
b. The Samsung KNOX™ Device “Allow NFC” policy setting is supported with KNOX™ 2.0 and greater.
c. With a Samsung device that supports KNOX™ Workspace, the “Allow Camera” setting in Device Control will control the device camera both inside and outside the Workspace container.
d. Samsung KNOX™ Workspace and App Wrapping
    i. KNOX™ 1.0
        1. Unwrapped apps install outside of the container.
        2. Wrapped apps install inside of the container
    ii. KNOX™ 2.0
        1. Enterprise apps (wrapped or not) install inside of the container.
        2. Play store apps (links) install outside of the container.
e. On Android KNOX™ 2.0 device that have been assigned a policy that enforces the creation of a KNOX™ container, not all password policy changes will result in prompting the user to change the container password. Changes to policies other than “Minimum password length” or “Minimum number of complex characters” will not prompt the user to update the password.
f. The following behavior has been seen on the Galaxy Tab S 8.4/10.5 and Galaxy Note 10.1 when GCM is enabled where if a selective wipe is issued and the device is inside the Workspace container, the selective wipe can be delayed (anywhere from 10-20 minutes) from wiping the device.
g. BlackList/Whitelist of apps enforced via KNOX™ Device controls the entire device. Blacklist/Whitelist of apps enforced via KNOX™ Workspace only controls the container.
h. When the KNOX™ workspace container is created, it automatically installs some apps into it (Container Agent, Personal Home, Phone, Setup Wizard and Verifier). These apps are considered to be installed by the user with all package names starting with “com.sec.knox.” If you have whitelist active and have alerts, compliance restrictions or both enabled, you will get restricted and/or alerted. **To avoid being restricted, you must put ‘knox’ in the whitelist.**

10. The serial number displayed on an Android device may not necessarily match the serial number that it returns to the NotifyMDM server. Thus, what is displayed on the device may not match what is displayed in the NotifyMDM Dashboard.
11. **Note:** With the Certificate Management feature added in NotifyMDM 3.8.0, it is not recommended to be used for Android Devices at this time as certificates cannot be removed from the device via a Selective Wipe. To remove certificates, a Full Wipe of the device is required.

iOS Devices

1. The **Allow YouTube** policy setting only controls the iOS YouTube app, it does not control access to YouTube via the browser on the device. [3808]
2. Some Corporate Resources for iOS Devices allow a password to be specified when they are assigned to users. If a password is not set, the user will be prompted for the password each time the configuration profile is loaded. [3938]
3. If Require Minimum Password Length is enabled on the NotifyMDM server and set to a value greater than 4, it still looks as if the Simple Passcode option on the device can be enabled (which would allow a simple 4 character password). However, the Minimum Password Length will enforce the set length requirement even when a user has enabled the Simple Passcode option on the device. [2197]
4. Although the **Allow Data Roaming** can be set to NO in NotifyMDM and enforced correctly on the device, the value is still editable in the device’s setting. If the value is edited by the user, the setting will be changed back to OFF after the next sync cycle. [6701]
5. If the user is in the Mail application when a policy change is synchronized, the Mail app may display an error “The connection to the server failed.”. Exiting the Mail app and re-entering will correct the issue. [4693]

6. When setting the **Accept cookies** policy to a value other than “Never”, the value will be exposed as an option on the device, but not automatically selected. [3840]
7. When changing the **Maximum grace period** Security Settings for a policy suite to the value of 240, the corresponding setting is not reflected on the devices for that policy suite. [5911]
8. When working with managed Enterprise apps, if the .ipa file will be hosted on the NotifyMDM server, the app should be generated with the NotifyMDM server address in the .plist.
9. When working with managed Enterprise apps, if the files will be hosted somewhere other than the NotifyMDM server, the host server will need MIME types configured for .plist and .ipa. Instructions can be found here: http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html
10. When using advanced Apple MDM API, the main configuration profile cannot be locked or password protected on the device. [7783]
11. Systems where iOS users are interfacing with a Novell GroupWise DataSync server must use DataSync Update 4 (Mobility 1.2.4) to fully utilize the hands-off enrollment functionality. Users need to enroll using their entire email address in lieu of their username if they are enrolling by the hands-off method. Similar processes must be followed to use hands-off enrollment when users interface with Exchange 2003 or any other mail server running ActiveSync 2.5 protocol. A user’s username and the string of characters to the left of the @ sign in their email address must be the same.
12. ActiveSync does not support having mail moved from another account into its inbox natively, so the “Allow Move” option does not directly affect them. This option can also prevent Forwards/Replies from another email address. [9588]
13. When using Web Clips, whenever the profile is removed from the device, the icon on the home screen will become blank. This icon will still have the designated name and will open to a blank white screen. [11038]
14. If iOS 7 device users are not associated with an LDAP server, from which an email address can be obtained, they will need to enroll using their entire email address in lieu of their username if they are enrolling by the hands-off method. This is a known issue associated with iOS 7. Users of iOS devices with OS versions less than 7.0, can enroll using either a username or full email address. [11889]
15. Apple’s Volume Purchasing Program (VPP) is only supported for iOS devices running 7.0.3 and later.
16. Device Enrollment Program (DEP) tokens should not be shared across Organizations on a NotifyMDM server.
17. If the “Allow user to change restrictions” policy under iOS Devices > Supervised Mode is set to *Yes*, a user can enable/disable restrictions from the device. If the policy is subsequently set to *No*, a user can still disable restrictions, but cannot enable any of them.
18. APN Notifications
    a. There are two ways that the notification can be received on the device.
        i. When the app is running in the background, the notification is received in the notification center.
        ii. When the app is running in the foreground, the notification is received as an alert.
    b. All characters on a notification can be completely seen when the device is turned for landscape view.
    c. With iOS 8, after tapping to open a notification from within the Notification center, the notification will automatically clear.
19. Single Sign On (SSO) is supported for iOS versions 7.0 or higher, however, various iOS bugs can prevent the SSO payload from being installed on certain versions.
20. When the Enterprise version of the NotifyMDM app is pushed to the device (via the Push NotifyMDM to iOS Devices feature), the application will not open if the ActiveSync account has not been set up on the device. If the ActiveSync password is entered before or after receiving the application - it will open correctly.

Windows Devices

1. Support for Windows 8.1/10 as of NotifyMDM server version 3.9.1.
2. Windows 8.1
    - Tablets are not properly enrolling because nothing is being returned to uniquely identify the device.
    - Phones – Federated enrollment may not work on every device. Enrollment currently fails on the Nokia Lumias 635 and 830.
    - The “Handsfree Only” option for Allow Bluetooth is not supported. If selected, the option will function the same as ‘Allowed.’
        i. When MDM is set to proxy ActiveSync, devices won’t sync mail and an error message appears on the device.
        ii. When proxy ActiveSync is not enabled and an Exchange user’s policy has Bluetooth set to Handsfree Only, an error message appears and Bluebooth is allowed on the device.
3. Windows 10
    - Encryption is not supported in Windows 10 Desktop.
    - Remote lock is not supported in Windows 10 Desktop.
    - Devices – Remote lock does work, but the device changes the PIN. The end user can retrieve the PIN through the Desktop User Self-Administration portal.
    - Issues were seen with a device adhering to a Device Connection Schedule
        i. When the device goes to sleep, it will not sync.
        ii. While awake, the device will sync in a manner that is not consistent with the assigned sync schedule. The same behavior was seen with a Windows 10 VM.

Kerio

1. When users interfacing with a Kerio mail server register to NotifyMDM, a 500 error is returned to the device and the registration does not complete. Kerio considers a command used for validating NotifyMDM traffic to be from an unsupported device. The issue can be circumvented by following the instructions outlined in the Kerio knowledge base article noted below: http://kb.kerio.com/article.php?id=224 [3035]

Version History

Version 3.11.4

Description: Update
Date: 2018.5.2

Bug Fixes

1. Fixed an issue where VPP apps that are out of licenses would not hold up the process for remaining VPP apps.
2. Fixed an issue where Organization Administrators cannot be created with email address that has an apostrophe (') symbol.
3. Fixed an issue where Updating iOS WiFi resources configured with Automatic Proxy settings removes the proxy server address.
4. Fixed an issue where Add Geofence form does not reset when closing the dialog.
5. Fixed an issue where the "RemoveProfile" iOS command was trying to remove ManagedDomains information when ManagedDomains were disabled.

Changes/New Features

1. Added support for Location based Policy assignments using Geofences.

Version 3.11.3

Description: Update
Date: 2017.11.6

Bug Fixes

1. Fixed issue where iOS 11 Devices getting stuck on Device Information command.
2. Miscellaneous fixes and performance related improvements.

Version 3.11.2

Description: Update
Date: 2017.08.20

Bug Fixes

3. Corrected an issue where the Quota Reset Day of the Month not resetting the data usage on the device.
4. Corrected an issue where snoozing alerts causes the dashboard to reload.
5. Corrected an issue where VPP invitation is not sent automatically when enrolling DEP devices.
6. Corrected an issue for iOS 10.3.2 not allowing the changed state of an installed app from unmanaged to managed.
7. Corrected an issue for iOS Device Model is not reflected properly for app-less devices

Changes/New Features

8. Added an Alert for license seats dropping below a set threshold.
9. Enhancement to assign Access Point Names to Local Groups.
10. Removed BlackBerry Apps from Organization Management.
11. Improve Compliance Alerts loading times.
12. Enhancement to assign Access Point Name credentials at the resource level instead of user level

Version 3.11.1

Description: Update
Date: 2017.01.15

Bug Fixes

13. Fixed issue where LDAP folders fail to display after a periodic update
14. Fixed issue where Data Plans in the Device Grid displaying 'NaN' for values over 1000

Version 3.11.0

Description: Update
Date: 2017.01.15

Bug Fixes

1. Fixed issue where notifications and alerts for Data Plans not working.
2. Fixed issue where Data plans in the device panel displays too many decimal places.
3. Fixed issue where Certificate Templates cannot be created on ZMM servers that do not have the CA installed on a Domain Controller.
4. Fixed issue where installing recommended apps through VPP is not working for all users.
6. Fixed issue when removing an Organization in System Administration was failing.

Changes/New Features

1. VPP invitations are sent automatically for iOS 9 and above devices.
2. Added new section in Organization Management to create Geofences.
3. Added new alert in the Compliance Manager Alerts page to trigger an alert when a device enters/exits a geofence.

Version 3.10.4

Description: Update
Date: 2016.09.19

Changes/New Features

1. Added support for Apple iOS 10.

Version 3.10.3

Description: Update
Date: 2016.09.12

Bug Fixes

1. Miscellaneous bug fixes and performance related improvements.

Version 3.10.2

Description: Update
Date: 2016.09.12

Changes/New Features

1. Changed behavior - when a device is set up for the first time, the managed app list now populates immediately.
2. Improvement - removed 1000 result limit from PowerShell get-user command.

Bug Fixes

1. Fixed issue where Removing an iOS or Android Wi-Fi Resource assigned to LDAP groups causes dashboard to refresh.
2. Fixed issue where Web enrolled iOS devices show "Unknown" for device name in user profile.
3. Fixed issue where device would report "NOT NOWs" so DEP enrollment completes correctly.
4. Fixed issue when selecting the Save Changes button within System Management->System Administration->Organizations causes numerous fields to disappear or checkboxes to become unchecked.
5. Fixed issue where the MDM app push will fail on DEP device configuration.
6. Fixed issue for Single app mode where app for Android.
7. Fixed issue for Windows devices where security actions will fail to re-send on network errors.
8. Fixed issue where APN (Access Point Name) iOS Corporate Resource incorrectly uses LDAP username instead of global username when new users are added to the LDAP group.
9. Fixed issue where proxy address disappears from the iOS Wi-Fi corporate resource.
10. Fixed issue where commands were getting stuck when saving changes on iOS devices page.
11. Fixed issue where sending notification for iOS does not send the message to the device.
12. Fixed issue where Device Information error on iOS devices having both (GSM and CDMA technologies).

Version 3.10.1

Description: Update
Date: 2016.05.16

Bug Fixes

1. Miscellaneous bug fixes and performance related improvements.

Version 3.10.0

Description: Update
Date: 2016.05.16

Changes/New Features

1. Rebranded server from GO!Enterprise MDM to NotifyMDM
    a. Rebranded NotifyMDM Server Dashboard
    b. Rebranded NotifyMDM End User Self Administrator Portal
    c. Rebranded NotifyMDM Mobile Device apps

Bug Fixes

2. Fixed an issue for better error handling when assigning resources.
3. Fixed Managed App issue for iPad enrolled through app-less enrollment.[6379]
4. Fixed issues for Managed not appearing in the Managed App area.[6380]
5. Fixed minor issue for the Apple APN renew Wizard.[6314]
6. Fixed an issue where Generic alerts can cause a Windows device to become unenrolled from the MDM system.[5806]
7. Fixed an issue where manually changing the Sync Schedule from peak to off-peak doesn't change how often the app syncs [4509]
8. Fixed an issue where selecting the Save Changes button within System Administration (under System Management) causes Use GCM and Proxy ActiveSync Traffic by Default options to be disabled.[6408]
9. Fixed an issue where organization Administrator receive “iOS MDM Service Error” when selecting Update Profile.[6399]

Version 3.9.2

Description: Update
Date: 2015.08.31

Changes/New Features

1. Additional Windows 8.1/10 Functionality
    a. Reset PIN
    b. Disable Device
    c. Connection Schedules
    d. ActiveSync configuration of the Native email app
    e. Location Tracking
    f. Allow Bluetooth Discovery
    g. Passport for Work
    h. New Management Policies
    i. Allow VPN Over Cellular Roaming

ii. Allow VPN Over Cellular

i. Added Device Feature Policies
    i. Allow Action Center Notifications
    ii. Allow Toasts
    iii. Allow Microsoft Account Connection
    iv. Allow Windows Store Auto Update
    v. Allow Developer Unlock
    vi. Allow Cortana
    vii. Allow Sync My Settings
    viii. Allow Task Switcher
    ix. Allow Voice Recording
j. New Application Policies
    i. Restrict App to System Volume
k. Added a Windows Phone icon in the Mini Admin.
l. Added Email unlock PIN option for Remote Lock in the Mini Admin.
m. Added the Email Unlock PIN link to the Mini Admin.
n. Added the ability to handle an Ownership value of 'Unknown' that may be returned during enrollment of a Windows device.

2. iOS 8.x/9 Additions
    a. VPP changes
    b. DEP Enrollment Optimizations
    c. Additional Policies
        i. Force Watch Wrist Detection
        ii. Unmanaged Air Drop
        iii. Allow iCloud Photo Library
    d. Additional Supervised Policies
        i. iOS 8.x Policies
            1. Allow Definition Lookup
            2. Allow Predictive Keyboard
            3. Allow Auto Correction
            4. Allow Spell Check ii. iOS 9 Policies
        1. Allow Keyboard Shortcuts
        2. Allow Paired Watch
        3. Allow Passcode Modification
        4. Allow Device Name Modification
        5. Allow Wallpaper Modification
        6. Allow Automatic App Downloads
        7. Allow Enterprise App Trust
    e. Added the ability to change the state of an already installed app from Unmanaged to Managed.
3. Miscellaneous Dashboard Changes
    a. Added the ability to assign Web Clips to Local groups for iOS devices.
    b. Added the ability to assign a VPN to Local groups for iOS devices.
    c. Added the Remove Managed Profile option under Resource Control in Policy Suites.
    d. The Admin Role permission Group E-mailing has been renamed to Group Notifications to match the label under Organization Control.
    e. Added the ability to resize columns on "Assign to Groups/Folders" within Managed Apps. Also added Search capabilities.
4. PHP upgrade to 5.6.12.
5. SAML authentication is now independent from ActiveSync/LDAP authentication. The same domain name can now be entered in the Dashboard for both SAML and ActiveSync/LDAP authentication.
6. UI changes to the Android and iOS Managed Apps page for handling Pending and Installed states.
7. Updated the Calendar Zoom Size policy for TouchDown to support calendar zoom of up to 500%.

Bug Fixes

1. Fixed an issue where hands-off enrollment could be enabled on an ActiveSync server without defining a domain. [3347]
2. Fixed an issue where Managed Apps installed through Local groups is not removed from the device when the user is removed from the local group. [280]
3. Fixed an issue where the Managed App web clip was assigned to users regardless of their liability type as long as they belonged to a local group/LDAP group/folder. [4800]
4. Fixed an issue where DEP devices failed to enroll if the SQL instance had a different Collation than the MDM database. [4840]
5. Fixed an Alert Settings service error within Compliance Manager when logged in as an Organization admin. [4861]
6. Fixed a general service error when attempting to add a new configuration under GO!Enterprise Workspace when logged in as an Organization admin.
7. Fixed sort functionality in the DEP Devices grid. [5018]
8. Fixed an issue with Custom Column search in the Smart Devices and Users grid where only 100 users are returned when over 100 should be. [5099]
9. Fixed an issue where a General Service Error was displayed when navigating to Managed Apps or when trying to remove an iOS app when logged in as an Organization Admin. [5063]

Version 3.9.1

Description: Update
Date: 2015.07.29

Changes/New Features

1. Windows 8.1/10 Support
    a. Enrollment with Federated and non-Federated Authentication
    b. Password Policies
    c. Device Policies
    d. Device Encryption
    e. Remote Lock
    f. Admin and User initiated Selective Wipe
    g. Remote Wipe
    h. Remote Ring
    i. Device Information
    j. Windows Push Notification Service (WNS) for sending push notifications
2. Miscellaneous Dashboard Changes
    a. Added support of the Allow Browser setting under Policy Suites -> Device Control for non-KNOX™ Android devices.
    b. Added the setting “Prompt for authentication to access Managed Apps” under System Management -> Organization settings to allow credential-based or token-based authentication when viewing Managed Apps from iOS and Android devices.
    c. Added a label to the device grid to distinguish between the Main grid, DEP grid and PowerShell devices grid.

Bug Fixes

1. Fixed an issue where a large number of upper ASCII characters entered in for an Organization name could cause the Dashboard to crash when saving.
2. Fixed an issue that could cause the deletion of an Organization to fail.
3. Fixed a display issue in the Dashboard where the default Liability setting in the User grid and the User profile for a user did not match.

Version 3.9.0

Description: Update
Date: 2015.07.08

Changes/New Features

1. ActiveSync Integration using PowerShell
    a. Added the ability to enable PowerShell under ActiveSync Servers in the Dashboard.
    b. Added the ability to retrieve a list of ActiveSync devices from an Exchange server and display them in a Discovered Devices grid in the Dashboard.
    c. Added Search, Device and Administration Panel functionality to the Discovered Devices grid.
    d. Added background and deletion syncing.
    e. Added the ability to display Discovered device information in the User Profile.
    f. Added the ability to notify users before their Quarantine date.
    g. Added the ability to get the Recovery Password for matched devices.
    h. Added PowerShell related columns to the following reports:
    i. Devices by OS Version and Platform
        ii. Devices by Platform and Model iii.
        Devices by Platform
2. Data Usage Monitoring
    a. Add Data Plans under Organization Management -> Organizational Control.
    b. Assign device phone and IMEI numbers to a data plan.
    c. Track the amount of data being used per device.
    d. Add a restriction in Compliance Manager for when a user resets the data on the device before the quota reset day.
    e. Send alert email and notifications to Admins and end users regarding how much data they've used.
    f. Added Data Usage information to the Device Panel of the Mini Admin.
    g. Added a Data usage plan report.
3. Added the ability to push GO!Enterprise Workspace configurations.
4. Added access control for the Desktop and Mobile User Self-Administration Portals under Policy Suites in the Dashboard.
5. Added Additional iOS 7/8 Features.
    a. Managed Domains (Security)
        i. Managed Email Domains
        ii. Managed Safari Domains
    b. Content Filter (Supervised Mode)
        i. Whitelist/Blacklist URLs
        ii. Bookmark URLs
    c. SSO Configuration (Corporate Resource) 6. PHP upgrade to 5.6.10.
7. Miscellaneous Dashboard changes
    a. Split the Device Panel and added an Administration Panel that contains the Security actions.
    b. The Enter key now performs a Search All from the Search Panel in the Mini Admin.
    c. Added a way to Switch Organizations under Alerts in the top right corner of the Dashboard.
    d. Added the ability set up and push an Enterprise App store via Web Clip for iOS devices under Organization Management > Managed Apps > iOS.

Bug Fixes

1. Fixed an issue with the iOS RemoveProvisioningProfile command when removing provisioning profile assignments via LDAP groups/folders.
2. Fixed an issue on the LDAP Servers page that allowed you to remove all domains from the table when at least one domain is required.

3. Fixed an issue under Android Wi-Fi Networks where the WEP Key settings weren't being retained on the second page of the wizard when the back button was clicked.
4. Fixed an issue where Local groups were not loading correctly when trying to assign resources to them.
5. Fixed an issue where a device that has been disabled, then a wipe was initiated, did not receive the wipe once being re-enabled.
6. Fixed an issue with the Passcode not compliant with requirements restriction not working properly within Compliance Manager.
7. Fixed issues which could cause the deletion of an Organization through the Dashboard to fail.
8. Fixed an issue with not being able to assign managed apps to the Single App mode of Supervised iOS devices.

Version 3.8.1

Description: Update
Date: 2015.04.07

***** Attention: Running NotifyMDM on Windows Server 2003 is no longer supported. *****

Changes/New Features

1. Upgraded PHP to version 5.6.6.
2. Removed Managed Apps from Policy Suites
    a. Local Groups corresponding to each Policy Suite will be created during the upgrade and users will be assigned to the appropriate Local Group.
3. Certificate Management
    a. Added the ability to have devices that use certificates issued by NotifyMDM to authenticate VPN connections in iOS devices.
4. Shared Users
    a. Added enrollment for DEP devices
    b. Added the ability to remove a Shared user from the Dashboard.
5. Added the following policies for Android OS 5.
    a. Device Control -> Device Features
        i. Allow screen capture
    b. Security Settings -> Password
        i. Password with no repeating numbers
    c. Policy Suites -> Resource Control
        i. Provision Managed Profile
6. Added the ability to provision the NotifyMDM app as a Device Owner app in Android OS 5.
7. Added a 'Help' link next to 'Logout' in the Desktop User Self-Administration Portal.
8. Removed the "Allow YouTube" setting for iOS devices from Policy Suites.

Bug Fixes

1. Fixed issues causing Kiosk mode on an Android Samsung KNOX™ device to be unstable.
2. Fixed an issue where the alert for "iOS APN Connectivity" did not display correctly in the Alerts grid.
3. Fixed an issue where an app is added within the Dashboard without a category, then change the view dropdown list to Category, the apps without a category assigned to them are not shown.
4. Fixed an issue where a second Apple DEP device enrolled to a user displayed on the Users and Devices Grid in the "Apple DEP Device" column as 'No'.
5. Other miscellaneous bug fixes.
6. Performance improvements.

Version 3.8.0

Description: Update
Date: 2015.03.09

***** Attention: This is the last version that will support Windows Server 2003. *****

Changes/New Features

1. Added Certificate Management
    a. Added Certificate Management under Organization Management.
    i. Added the ability to configure one or more Microsoft Active Directory Certificate Authorities on the GOEnterprise !MDM Server. ii. Added the ability to add, edit and remove Certificate Templates. iii. Added the ability to revoke and re-issue certificates.
    iv. Added the ability to view a list of certificates issued by the Certificate server.
    v. Added the ability to view a list of certificates issued for each user.
    vi. Implemented the ability to use with iOS ActiveSync and Wifi configurations.
2. Added Cisco ISE support.
    a. Added the ability to enroll a device via Cisco ISE and communicate with NotifyMDM
    b. Added the following into Compliance Manager:
    i. The ability to restrict network access by non-compliant devices. "Network Access" has been added as a Restriction option under Corporate Resources in Compliance Manager.
    ii. Two new violation checks in the Device Platform Restrictions -> Android
        1. Restrict if passcode not initiated on device
        2. Restrict if passcode is not compliant with data protection
    c. Added the ability to make an Organization admin an ISE Admin 3. FIPS Compliance.
    a. The MDM database can be re-encrypted to use Safelogic libraries for encryption.
    b. Re-encryption can be done via the Update Manager on the NotifyMDM server.
    c. After the data has been re-encrypted to use the Safelogic libraries, the NotifyMDM About section within the Dashboard will show "Cryptography: FIPS 140-2 certified AES encryption."
4. Added Shared Devices support.
    a. Added the ability to add a shared user to the Dashboard.
    b. Added the ability to enroll an Android or iOS device with the shared user's credentials to the NotifyMDM server.
    c. Added the ability to have a non-shared user Sign-in/Sign-out and have it tracked on the NotifyMDM server.
5. Added the iOS Activation Lock feature.
    a. The Device Activation Lock feature is controlled through the Find My iPhone setting on the device.
    b. Added the Activation Lock status to Device Information.
    c. Added the ability to send the Activation Lock from the User Panel and under Security.
    d. An "Allow Activation Lock" setting was placed under Supervised Mode. This determines if the device can be locked with Find My iPhone.
6. Added the ability to assign the WiFi resource to Local user groups.
7. Added the ability to upload an APN certificate that can be used with the device app when the app is distributed as an Enterprise app.
8. Added the ability to install recommended or force pushed iOS App Store apps to a device when the "Allow Installation of unmanaged apps" setting is enabled and the "Allow App Store" setting is disabled. **Note: This functionality will only work with iOS 7 and iOS 8 devices.**
9. Added the ability to automate most of the APN creation process from within the Dashboard.
10. Implemented the KNOX™ Device policy for the blacklisting and whitelisting of apps.
11. Implemented the KNOX™ Workspace policy for the blacklisting and whitelisting of apps.
12. Added the ability to send an APN or GCM message to a user from the User Panel in the Dashboard by adding the "Send Notification" hyperlink under Messaging.
13. Moved the following iOS policies out of Supervised Mode as they pertain to all iOS devices now.

a. Allow Global Background Fetch while roaming
b. Force iTunes store password entry
c. Force pairing password for outgoing AirPlay requests

Bug Fixes

1. Fixed an issue where the ProfileList command for iOS devices gets stuck In-Flight. [2465]
2. Fixed an issue where an Organization admin is logged out of the Dashboard when trying to assign an Exchange corporate resource. [2533]
3. Fixed an issue with the Audit Trail table in the database to ensure the correct interface is being logged for the actions. [2254]
4. Fixed an issue where the contents of the Organization default drop downs did not refresh when another organization was selected. [303]
5. Fixed an issue with reports not displaying foreign characters correctly. [1439]
6. Fixed a display issue where the “0 users were found” dialog could appear when uploading, disabling or deleting an APN certificate in the Dashboard.
7. Fixed an issue where the device camera would not enable when the Allow camera policies under Device Control and Samsung KNOX™ Workspace are initially set to No, then are set to Yes.
8. Other miscellaneous bug fixes.
9. Performance improvements.

Version 3.7.2

Description: Update
Date: 2015.3.09

Bug Fixes

1. Miscellaneous bug fixes and performance related improvements.

Version 3.7.1

Description: Update
Date: 2014.11.10

Bug Fixes

1. Fixed an issue that could cause apps being force pushed to a device to fail if one of the apps being force pushed is already on the device.
2. Other performance related improvements.

Version 3.7.0

Description: Update
Date: 2014.10.06

Changes/New Features

1. Added support for Security Assertion Markup Language (SAML) authentication.
    a. Incorporated into Device Enrollment, Desktop and Mobile User Self-Administration portal authentication and downloading of Managed Apps.
2. Added additional support for KNOX™ Devices.

    a. Updated “Samsung KNOX™ Device Policies” in the Dashboard with sections for Alternative Home Screen, Application, Device Feature and Password policies supported by KNOX™ Devices.
        i. Added Alternative Home Screen policies.
        ii. Added additional Password and Restriction policies. iii. Added Email, Location, Browser and Roaming policies.
        iv. Added Developers mode policies.
    b. In the User Panel, added the ability to Reboot and Power off a device. Also added Unblock Password Entry which gives the ability to unlock the password entry field on a device.
3. Added support for KNOX™ Workspace.
    a. Added the ability to create and remove a Workspace container.
    b. Added Restriction and Password policies for the container.
    c. Added the Email policy.
    d. Added the ability to install Enterprise apps inside the container.
4. Added support for App Categorization in the Dashboard.
5. Under Organization Control, changed “Group E-mailing” to “Group Notifications” and added support for iOS APN and Google GCM push notifications.
6. Added the ability to upload and enable an Acceptable Use Policy to users on the NotifyMDM server. If enabled, users must accept the policy before they can enroll.
7. Added the ability to disable the ActiveSync proxy functionality of the NotifyMDM server.
8. Added the ability to enroll via a web page then push the App Store version of the NotifyMDM app as a managed app for iOS devices.
9. Added support for Web Clusters.
10. Added the following iOS 8 Settings:
    a. Application Policies
        i. Allow activity continuation, Allow Enterprise books backup, Allow Enterprise books metadata backup
    b. Supervised Device Restrictions
        i. Allow full wipe via device, Allow Spotlight results, Allow user to change restrictions c. iCloud Policies
        i. Allow managed apps cloud sync
11. Added the following iOS 7 and 8 device information settings to the Device Information page:
    a. Device ID, iTunes Account Active, iTunes Account Hash Value, Cloud Backup Enabled, Last Cloud Backup
12. Added the ability to see and install managed apps through the Desktop User Self-Administration Portal for iOS devices that have enrolled to the server via DEP.
13. Added the ability to name iOS Supervised devices in the Dashboard.
14. Added the ability to detect and report an Android OS build number.

Bug Fixes

1. Fixed an issue where the iOS HTTP Global Proxy profile was not being removed from a device.
2. Fixed an issue where the Activation/De-activation History graph populated data for the original organization if multiple organizations existed on the server.
3. Fixed an issue where the download count of an iOS app was not displaying properly in the Dashboard.
4. Fixed an issue where a policy schedule is assigned using Policy Schedules > Assign Schedule To Users displayed the wrong schedule in the user profile.
5. Fixed an issue where a policy suite assigned using Policy Suites > Assign Policy Suite To Users displayed the wrong policy suite in the user profile.
6. Fixed an issue with Android managed apps where the server was continuously attempting to push an older version of the app to the device even though a newer version of the app is already installed.
7. Fixed an issue where manually uploaded iOS managed apps (ipa and plist) were not force pushed to a device for an account set up with a Corporate liability when the Corporate liability sliders for the app are set to ‘Yes’ and the Individual liability is set to ‘No.’
8. Additional GCM performance and functionality improvements.

9. Additional Managed App performance and functionality improvements.

Version 3.6.3

Description: Update
Date: 2014.06.16

Changes/New Features

1. Added the ability to handle retina display iOS app icons for enterprise apps that are uploaded through the Dashboard.
2. Added a policy under Device Control > Device Features called “Allow user to remove enrollment.” This policy determines if a user is allowed to remove the MDM user account from the device.

Bug Fixes

1. Fixed an issue where DEP devices enrolled in VPP are not pushed managed apps.
2. Fixed an issue where encrypted Android devices were not reporting as so within the Dashboard.
3. Fixed an issue where the names of available LDAP groups were not populating when importing or selecting LDAP groups for iOS resources.
4. Fixed an issue that caused a blank Android app to be returned in the Installed Apps list.
5. Fixed an issue where assigning managed apps from multiple levels of assignment were not pushed to the device.
6. Made improvements to other areas of managed app functionality.

Version 3.6.2

Description: Update
Date: 2014.05.27

Changes/New Features

1. Added support for Apple’s Volume Purchasing Program (VPP).
2. Added support for Apple’s Device Enrollment Program (DEP).
3. Support for Samsung KNOX™ Devices.
    a. Exchange ActiveSync, Password, Security and Restriction Policies
    b. Device Statistics, Application Policies
    c. Kiosk Mode
4. Added Localization support to the Desktop and Mobile User Self-Administration Portals and iOS and Android NotifyMDM apps.
    a. Includes French, German, Italian, Spanish, Swedish, Brazilian Portuguese, Traditional Chinese, Simplified Chinese and Japanese
5. iOS and Android Managed Apps Dashboard Additions
    a. Added a column called “Download Count” to the Managed Apps data grids that will track how many times an app has been downloaded.
    b. Added the ability to limit the number of downloads for particular apps.
    c. Added “Apps Reports” under User and Device Reporting that give details for app assignment, app statistics and apps assigned to users.
    d. Added the Compliance Manager alert “Low application availability” under Alert Settings that can be configured to alert when an application in bulk is close to its availability limit.
6. Miscellaneous Dashboard Additions
    a. Added “Allow Unsigned Applications” and “Allow Unsigned Package Installation” policies for Android devices under Device Control > Applications.

b. Added a new column, 'VPP', to the Managed Apps data grid to differentiate between VPP managed apps and other managed apps.
c. Added one-click and keyboard arrow key navigation abilities to the Organization Management menu within the Dashboard.

7. Performance improvements for handling GCM functionality.

Bug Fixes

1. Addressed an issue that caused a service error when sorting System logs.
2. Removed the ability to perform a Selective Wipe for devices connecting to the NotifyMDM via ActiveSync only.

Version 3.6.1

Description: Update
Date: 2014.04.28

Changes/New Features

1. Added new ActiveSync Synchronization policy settings under Device Control specific to TouchDown.
    a. "Specific calendar age for synchronization"
        i. This setting determines a specific number of calendar days that can be synchronized.
        ii. This option can be suppressed with the "Allow appointment synchronization options" suppression under TouchDown > Suppressions.
    b. "Specific email age for synchronization"
        i. This setting determines a specific age for email to synchronize.
        ii. This option can be suppressed with the "Allow email synchronization options" suppression under TouchDown > Suppressions.
2. Renamed the "Allow personal hotspot" label. It now reads, "Enable personal hotspot."
3. To make sharing devices among users simpler, the "Remove Enrollment" option on the iOS device agent and the "Delete Account" option on the Android device agent will now selectively wipe the device in addition to unenrolling it.
4. Modified the behavior of the full wipe command. The device will now be removed from the user grid when the full wipe is completed.

Bug Fixes

1. Fixed an issue that prevented all of the iOS security actions from being made available on the Dashboard after the device initially checked into the server during enrollment.

Version 3.6.0

Description: Installer/Update
Date: 2014.04.07

Changes/New Features

1. Dashboard and User Self-Administration Portals now reflect the new product name, NotifyMDM, and new product logos and icons.
2. All instances of "Stop Managing Device" in the Dashboard and User Self-Administration Portals have been renamed, "Selective Wipe." The command's function has not been altered.
3. Upgraded PHP to use 5.3.28.
4. Increased the amount of time that a Dashboard service error will display before it fades out.

5. If no users are found when searching the User Grid, a pop up message will now display stating that the search was completed successfully and 0 users were found.
6. Various server performance improvements.

Bug Fixes

1. Fixed an issue in Compliance Manager for Whitelist App that prevented recipients from being added and saved for email and SMS alerts.
2. Fixed an issue that caused Non-LDAP users to have their assigned corporate resources deleted if an LDAP folder with those assigned corporate resources was deleted.
3. Fixed an issue that prevented all of a user's devices from being removed from the Dashboard User Grid when "Remove User" is selected.

Version 3.5.2

Description: Update
Date: 2014.02.13

Changes/New Features

1. Various server performance improvements.

Version 3.5.1

Description: Update
Date: 2014.02.10

Changes/New Features

1. Various server performance improvements.

Bug Fixes

1. Fixed some issues with Android Managed Apps functionality.
2. Fixed an issue with adding users to the dashboard via .CSV or LDAP as an Organization administrator.

Version 3.5.0

Description: Update
Date: 2014.01.13

Changes/New Features

1. Added the ability to assign managed apps to LDAP groups and folders.
2. Added new iOS 7 Restriction Settings:
    a. Under iOS Devices > Device Features
        i. Allow fingerprint for unlock
        ii. Allow lock screen control center
        iii. Allow lock screen notification view iv. Allow lock screen today view
    b. Under Policy Suite > iOS Devices > Supervised Mode

i. Allow AirDrop ii. Allow assistant user generated content

3. Added GCM logging to the dashboard.

Bug Fixes

1. Fixed an issue with the MDM App authorization failure alert where the device violation details will display in the user grid, however, the alert was never generated or displayed in the dashboard.
2. Fixed a refresh/display issue with the mini Admin actions in the dashboard User Grid.
3. Fixed an issue where adding a user with “Send enrollment message via SMS” selected failed to add the user to the user grid.
4. Fixed an issue that prevented mobile apps from installing on iOS 7 devices.
5. Fixed an issue where iOS devices were displaying the raw device model instead of the friendly name.
6. Other various dashboard and UI bug fixes.

Version 3.4.1

Description: Update
Date: 2013.12.10

Changes/New Features

1. Made changes to GCM functionality to now require a unique Sender ID and API Key on the server for GCM service.

Bug Fixes

1. Fixed an issue where a mobile app uploaded in the dashboard with an .ipa and a .plist did not install on iOS 7 devices.

Version 3.4.0

Description: Update
Date: 2013.12.02

Changes/New Features

1. Added support for Google Cloud Messaging (GCM) with Android devices.
    a. Security actions and policy changes performed from the Dashboard or User Self-Administration Portals will take effect immediately on the device.
    b. Enable or disable under System Management > Organization in the Dashboard.
2. Added the ability to create Local Groups.
    a. Located under Organization Management > Organization Control in the Dashboard.
    b. Configure groups with Policy Suite, Device Connection Schedule and Liability assignments.
3. iOS 7 Additions
    a. Added the ability to control Personal Hotspot under Policy Suites > iOS Devices in the Dashboard.
    b. Added the ability to display if a device has an active iTunes account under Device Information.
4. Miscellaneous Dashboard Changes
    a. The username field on the Dashboard login page is no longer case sensitive. [2241]
    b. Made changes to the dashboard login’s Organization drop-down, that allow the administrator to use the mouse wheel to scroll through the list of organizations. In addition, typing in

multiple characters of an organization's name will quickly take you to an organization in the list. [3796]

c. Added an option to the Mini Admin and User Profile for wiping the device SD card. The option has also been added into the Desktop and Mobile User Self-Administration Portals.
d. Scaled all of the charts under Choose Visible Charts in Activity Monitor to a uniform size. [11726]
e. TouchDown suppression settings that the administrator opts not to control are no longer overwritten when changes to a policy are saved or a user's policy is switched. [11814] f. The Context Sensitive Help heading for iOS Configurator has been changed from "iOS Configurator" to "iOS Configurator Devices".

Bug Fixes

1. Fixed an issue where LDAP groups are not displayed in the Add LDAP wizard, Group and Folder Configurations page (Import Groups) and Add User by LDAP wizard due to the userID attribute not being present in a group. [11853]
2. Fixed an issue that caused APNs to fail when an Android WiFi resource was assigned to an LDAP group or folder that had iOS device members. [11886]
3. Fixed an issue involving updates to an Android managed app that is force pushed. If the user declined the install of the updates, the app never prompted for install again and the versions of the app displayed in the dashboard and on the device did not match. [11892]
    - Note: To further avoid this issue, Administrators should ensure that the app version numbers in the NotifyMDM UI, under Organization Management > Application Management > Manage Applications, are current with the Play store versions.
4. Fixed an issue that caused an iOS device to receive an Android WiFi resource after the password of that resource was changed in the Dashboard. [11895]
5. Other various Dashboard and UI bug fixes.

Version 3.3.2

Description: Update
Date: 2013.09.19

Changes/New Features

1. Addressed an enrollment issue with iPads running iOS 7.

Version 3.3.1

Description: Update
Date: 2013.09.16

Changes/New Features

1. Setting the "Require TouchDown PIN" to 'ON' no longer enables require complex, alphabetic, numeric or biometric passwords as these are not ActiveSync password policies.
2. Enabled the "Require max inactivity time device lock" under Policy Suites > Security Settings > Device Inactivity and Locking by default for the lowest policy suite creation level.
3. Miscellaneous Dashboard Changes
    a. Renamed "iOS NMDM" under iOS Devices in Policy Suites. It is now labeled "Management"
    b. Renamed "Apply managed settings" under iOS Devices > Management. It is now labeled "Allow management of settings."

Bug Fixes

1. Fixed an issue with iOS devices where native ActiveSync prompts the device password incorrectly.
2. Fixed an issue when using the NotifyMDM API where the incorrect policy suite for a user could be listed in their User Profile. [11864]
3. Fixed an issue when adding a new Provisioning Profile that was caused entering a large amount of characters in the Display Name textbox. It now only accepts up to 64 characters. [11863]

Version 3.3.0

Description: Update
Date: 2013.09.03

Changes/New Features

1. Updated Context Sensitive Help icons and tooltips in the Dashboard.
    a. Removed the WebOS and Windows Phone columns.
    b. Added new columns for iOS Configurator and ActiveSync only devices
    c. The ActiveSync column represents WebOS, Windows Phone and BlackBerry 10 platforms.
2. Added the ability to specify the maximum number of devices allowed by a user.
3. Added the ability to do a search for iPad specific apps as well as apps for all platforms in the iTunes search and import either type of app.
4. iOS Additions
    a. In preparation for iOS 7
        i. Added the options and rejection reasons for the InstallApplication command.
        ii. Added the ability to manage a configuration file for the InstallApplication command. iii. Added the ability to retrieve configuration and feedback commands for Managed Apps from the device and view/export them from the device logs. iv. Added the ability to view the status reported by the device, via the ManagedApplicationsList command, on the Managed Apps data grid
5. Miscellaneous Dashboard Changes
    a. The “Record installed applications” option has been moved under iOS Devices > Applications in Policy Suites.
    b. Reworded “Managed Apps” to “Allow app management” under iOS Devices in Policy Suites.
    c. Replaced labels and text that referred to “Restricted Apps” with “Whitelists/Blacklists.”
    d. Added a new column called “Activation Date” to the Choose Visible Columns list. This will display the creation date for a user/device on the Dashboard.
6. Added the ability to suppress the device passcode and only force a passcode/PIN for TouchDown. [11833]

Bug Fixes

1. Fixed an issue where after an upgrade, Lock Device and Stop Managing Device alerts were incorrect.
2. Fixed an issue when logging into the Desktop User Self-Administration Portal. Logging in incorrectly with “domain\username” in the UserName field now results in a failed login instead of a blank screen. [11838]
3. Fixed an issue where iOS resources weren’t correctly prompting to update existing users when expiration times changed. [11846]

Version 3.2.1

Description: Update
Date: 2013.08.29

Changes/New Features

1. Added the ability to install Managed Apps through the Desktop User Self-Administration Portal for iOS devices.

Version 3.2.0

Description: Update
Date: 2013.08.19

Changes/New Features

1. Dashboard performance improvements.
2. Redesign of Organization Management in the Dashboard.
3. Redesign of the “Choose Visible Columns” overlay in Smart Devices and Users.
4. Removed the Corporate Resources tabs in User Profile and placed them in an expandable tree under Corporate Resources.
5. Added two new policies for Android Application Management.
    a. Record installed applications – when enabled, a list of all apps and their data usage will be stored.
    b. Record managed applications – when enabled, and Record installed applications is disabled, only a list of managed apps and their data usage will be stored.
6. In the Dashboard and User Self-Administration Portals, all instances of “Mobile Apps” have been changed to “Managed Apps.”
7. Dashboard label Change – “Archive files on device” as been changed to “Archive device file list.”
8. Added the ability to be able to search users by search criteria and assign them a policy schedule from the “Assign schedules to Users” pop up.
9. iOS Additions:
    a. Added support for Provisioning Profiles.
    b. In preparation for iOS 7:
        i. Added support for being able to specify and restrict additional keys on the device while it is in single app mode.
        ii. Added support for new Restriction policies in the Dashboard.
        iii. Added the ability to specify and send a message and/or a phone number when a Device Lock is sent from the Dashboard or User Self-Administration Portals.
        iv. Added support of the new queries to the DeviceInformation command for display in the dashboard (IsSupervised, IsDeviceLocatorServiceEnabled, IsDoNotDisturbInEffect, EthernetMacs, PersonalHotspotEnabled).
10. Added the ability to assign Android VPN and Wi-Fi Networks corporate resources through the right click functionality for LDAP Folders under Smart Devices and Users.
11. Added a new restriction option in compliance manager to restrict an Android user that disabled Device Administration.
12. The assigned corporate resource name field for all user corporate resources has been changed from a drop down to a label.
13. Changes were made to use the device time zone for time-based policy enforcement.
14. For BlackBerry 10 devices, the DeviceUID is now populated from the ASDeviceID.

Bug Fixes

1. Fixed an issue that caused a VPN profile to not be removed properly from a device. [11818]

Version 3.1.1

Description: Update
Date: 2013.08.05

Bug Fixes

1. Fixed a login issue to the User Self-Administration Portals.
2. Fixed an issue with how an Access Point profile was being sent to an iOS device.

Version 3.1.0

Description: Update
Date: 2013.07.29

Changes/New Features

1. Upgraded PHP to 5.3.26 [11414]
2. Added the ability to display BlackBerry 10 information in the Dashboard.
3. Added a new database task to remove devices that have been in a pending delete state for 30 days or more, after an administrator has issued the *Stop Managing Device* command. [9964]
4. Added the ability to have notifications sent to end users when certain actions are performed on their device. Those actions include, Enable/Disable device, Suspend/Resume device, Lock device, Full Wipe, Stop Managing device, Wipe Storage Card, Clear Passcode (iOS), Trigger APN (iOS). [10116]
5. Added a column in the Dashboard user grid for the NLES ClientDeviceSAKey. The column is labeled 'Linked Identifier'. [11696]
6. Added the ability to require an admin to change their password on initial login and added a "Change Password" link in the top right corner of the Dashboard. [11610]
    a. Note: This feature only applies to admin accounts that have been manually created on the NMDM server.
7. New Security policies include Android password requirement options and an option to allow dialing of any number for BlackBerry emergency dialing.

Bug Fixes

2. Fixed an issue where multiple locks could not be sent from the Desktop User Self-Administrative Portal without having to log out then log back in. [9329]

Version 3.0.0

Description: Update
Date: 2013.07.08

Changes/New Features

1. A version of the installer that does not offer the option to install and use SQL Express Edition is now available.
2. Time-based policies – A new option called "Policy Schedules" has been added under User Account Settings in Organization Management.
    a. The policy schedule will determine when a policy suite for work hours is used and when a policy suite for outside work hours is used.
    b. The schedule can be assigned to an individual user, all users in a LDAP group/folder or all the users in an organization.
    c. Resource Control policies added to disable resources for users associated with a policy suite that is in effect outside work hours.
3. iOS Configurator/Supervised Mode settings – New settings have been added in the iOS Devices section of Policy Suites under Organization Management.
    a. The new settings include:
        - Allow app removal
        - Allow configuration profile installation
        - Allow iMessage
        - Global HTTP Proxy Payload

- Single App Mode

4. Added the “Require TouchDown encryption” option in the TouchDown/Notify Email section of Policy Suites under Organization Management.
5. Added Android VPN support under Android Corporate Resources in Organization Management.
    a. Connection Types include F5 SSL and Cisco AnyConnect
6. Added support for additional VPN connection types.
7. Added an alert for APN Certificate Expiration under System Alerts in the Compliance Manager Alert Settings.

Bug Fixes

1. Fixed and issue in the Desktop User Self-Administration Portal where just the latitude and longitude coordinates are displayed when clicking on the “Locate Using Google Maps” button. [11597]
2. Fixed an issue where a service error would display when clicking the “Devices by Platform” and Devices by Platform and Model” reports. [11612]
3. Other various dashboard and UI bug fixes.

Version 2.8.5

Description: Update
Date: 2013.07.08

Changes/New Features

1. Fixed a password recovery display issue.
2. Optimized alerts performance for GMT+ systems.

Version 2.8.4

Description: Update
Date: 2013.06.25

Changes/New Features

1. Improved database performance.

Version 2.8.3

Description: Update
Date: 2013.06.10

Changes/New Features

1. “Blacklist Restrictions” in Organization Management has been renamed ”Restricted Apps” and now includes Whitelist restrictions.
2. Application Whitelist
    a. Added the ability to create a list of strings that filter whitelisted applications on user devices. The presence of a non-whitelisted app on a device can block access to email, shared files, app lists, or other organization resources.
    b. Added the ability to associate a Whitelist with a Policy Suite.

    c. Added the ability to display the assigned Whitelist in the User Profile and LDAP Group Configurations.
    d. Added the ability to restrict Corporate Resources based on whether a user violates the Whitelist.
    e. Added the ability to alert an Administrator when a device violates the Whitelist.
3. iOS App Store Integration
    a. An iTunes app search has been added in the dashboard under the Mobile Apps and Restricted Apps sections.
4. Added the ability to restrict an app by App Identifier.
5. Added the “Device Name” column to the User Data Grid in the dashboard and to the Desktop and Mobile User Self-Administration Portals.
6. Added the following device status columns to the User Data Grid: “Pending Remove” and “Suspended.”
7. From the System Management -> Organization page, administrators now have the ability to enter and display the AppleID with which the APN certificate was generated.

Bug Fixes

1. Fixed an issue in Compliance Manager where alerts were not issued if there were no resources selected for restriction. [11494]
2. Fixed a location tracking issue in which location coordinates displayed instead of the actual address of the device when selecting “Locate on Google Maps” and then clicking on the pin. [11500]
3. Fixed an issue where all device location data was set to the date on which the NotifyMDM server was updated. [11524]
4. Fixed an issue with iPhone 4 where data and voice roaming settings were being enabled automatically on the device. [11526]
5. Fixed a cross scripting vulnerability in php. [11570]
6. Other various dashboard and UI bug fixes.

Version 2.8.2

Description: Update
Date: 2013.04.29

Changes/New Features

1. Application Blacklist
    a. Added the ability to create a list of strings that filter blacklisted applications on user devices. The presence of a blacklisted app on a device can block access to email, shared files, app lists, or other organization resources.
    b. Added the ability to associate a Blacklist with a Policy Suite.
    c. Added the ability to display the assigned Blacklist in the User Profile and LDAP Group Configurations.
    d. Added the ability to restrict Corporate Resources based on whether a user violates the Blacklist.
    e. Added the ability to alert an Administrator when a device violates the Blacklist.

Bug Fixes

1. Fixed an issue with LDAP Periodic Updates and foreign language databases. [11179]
2. Fixed an issue that caused an error when sorting File Share by version. [11077]
3. Fixed an issue that required an administrator to select the device type a second time before continuing with an addition to the Mobile Apps list. [3182]
4. Other various dashboard and UI bug fixes.

Version 2.8.1

Description: Update
Date: 2013.04.22

Changes/New Features

1. Desktop and Mobile USAP changes to match the re-designed user and device administration options that were implemented in the 2.8 dashboard.
2. Support for Windows RT. [11188]

Bug Fixes

1. Fixed an issue that returned an LDAP Service Error in the dashboard when a group on the LDAP server contains an '&' in its name. [11162]
2. Fixed an issue where Mobile App permissions do not work correctly when "Manage Mobile Apps" is set to 'No'. [11382]
3. Other various dashboard and UI bug fixes.

Version 2.8.0

Description: Update
Date: 2013.04.08

Changes/New Features

1. Basic Android App Management
    a. Added the ability to force push an app to the device.
    b. Added the ability to update and remove apps on the device.
    c. Added the ability to display the app version on the NotifyMDM server.
    d. Added the option to be able to remove an app when a selective wipe is performed.
2. iOS Corporate Resources
    a. Added the ability to set up Access Points. [2987]
    b. Added the ability to set up Web Clips. [2987, 6209]
3. iOS Configurator support
    a. Added the ability to export the MDM profile from the dashboard and load it onto a device through Configurator.
4. Re-designed user and device administration options in the dashboard.
    a. Renamed "Clear Device Enrollment" to "Reset for Enrollment."
    b. Added "Suspend Device." The device is managed while suspended, but blocked from corporate resources.
    c. Added "Stop Managing Device." This will replace/combine Selective Wipe and Delete Device.
    d. The "Remove User" button will now remove the selected user and all associated devices.
5. Support for Safari web browser.

Bug Fixes

1. Various dashboard and UI bug fixes.

Version 2.7.1

Description: Update
Date: 2013.02.25

Bug Fixes

1. Fixed an issue with the authentication mechanism used when connecting to an ActiveSync server where a user may see an authentication failure error after the upgrade to 2.7.0. This issue is seen when:
    a. An account was set up where they did not have an '@' in their username, and
    b. The ActiveSync server that the user was assigned to did not have a domain linked to it or did not have a domain entered in their user profile, and
    c. The specific ActiveSync server will not accept a leading '\' as part of their username.
2. Fixed an issue where policy settings were not being applied when an older NotifyMDM Android app (pre - 2.7.0) was being used on the device. [11008]

Version 2.7.0

Description: Update
Date: 2013.02.19

Changes/New Features

1. New, localizable installer with logging. [8889]
2. Dashboard Updates
    a. User Profile redesign.
    b. Layout change to the Organization Management page.
    c. Addition of an Organization Licensing page under System Administration, so all organization licenses and their seat counts can be viewed in one location. [9589, 9663]
    d. Added Wi-Fi Networks under *Android Corporate Resources*.
    e. Smart Devices and Users page redesign to include an LDAP tree/hierarchy.
        i. Added the ability to search users and devices in the hierarchy.
3. Advanced LDAP Functionality
    a. Hands-off enrollment using LDAP [4399, 8485]
    b. Import of email address, first name, last name from the LDAP Server when adding a new user [3769]
    c. Policies can be assigned to LDAP groups. [4789]
    d. Groups can be prioritized for policy settings to resolve conflicts.
    e. Corporate Resources can be assigned to LDAP groups.
    f. A periodic update option can be configured to check the LDAP server for changes. [8622]
4. Added the ability for larger file uploads, up to 100 MB, on the NotifyMDM server. [4624]

Bug Fixes

1. Fixed with the addition of Advanced LDAP functionality:
    a. The email address of a user was not being retrieved properly during enrollment. [2378]
    b. An issue that did not allow the option for additional LDAP fields to be used as a username. [3107]
    c. The username would be truncated on the dashboard after importing users from an LDAP server. [3580]
2. Fixed a "Right Truncation" SQL error that populated into the MDM error log. [3740]
3. Fixed a location violation in Compliance Manager where Android, BlackBerry and iOS devices attempt to check in with their location, but were unable to do so, thus causing them to fall out of compliance. [6581]

4. Fixed an issue with iOS devices that prevented managed mobile apps from being updated properly from the dashboard. [10532]
5. Fixed an issue that caused iOS mobile apps that experienced errors while installing to prevent other apps from installing. [9807]
6. Fixed an issue with iOS devices that allowed profiles to be installed after an expiration date has passed. [9918]
7. Fixed an issue where the Autodiscover information for a user was not being reset after the ActiveSync server changed. [9785]
8. Fixed a display issue that caused the APN certificate to show as disabled when an Administrator's default view at login was the System view. [9923]
9. Other various dashboard and UI bug fixes.

Version 2.6.1

Description: Update
Date: 2012.12.10

Changes/New Features

1. Added support for iOS Profile Expiration (iOS 6+).
2. Added new Admin-configurable TouchDown Policies.
3. Added support for OpenID.
4. Added support for SMTP AUTH LOGIN authentication.
5. Implemented performance improvements for Context Sensitive Help (CSH) and added a new column, "TD for iOS."

Bug Fixes

1. Corrected an issue with TouchDown for Android in which a Full Wipe sent to the device only wiped the TouchDown app and not the device's full memory. [7552]
2. Addressed an issue where iOS devices were immediately restricted upon enrollment due to the compliance setting, "Restrict if iOS APN profile is not enrolled." [9447]
3. Fixed an issue that caused group emails to send messages to deleted users. [9536]
4. Corrected an issue with iOS mobile apps not properly loading when HTTPS was used in the URL. [9720]
5. Various dashboard and UI bug fixes.

Version 2.6.0

Description: Update
Date: 2012.10.29

Changes/New Features

1. Support for PHP 5.3.17.
2. Added Context Sensitive Help to the Policy Suite options.
3. Features have been implemented to test various connection resources (ActiveSync server, LDAP server, SMTP server, etc.) from the Dashboard.
4. Implemented Activity Monitor changes to increase performance.
5. iOS Settings Dashboard additions:
    a. Exchange server settings - Allow Move (iOS5+) and Use Only in Mail (iOS5+)
    b. Support for iOS Policies – "Allow Passbook while device is locked" and "Allow Shared Photo Streams"

6. Data Usage by Device report - Changed the report format to be consistent with the rest of the Dashboard reports. Added a look up.
7. Changed the look of Location Data in the User Profile by adjusting the layout for the date chooser, times grid and map area. Added map controls for scale, map type and zoom.
8. Addressed a timestamp issue so that end users are prevented from manipulating the time reported by the location tracker. [9220]

Bug Fixes

1. Auto complete has been disabled for the username, domain and password fields on the Mobile and Desktop User Self Administration Portals. [2709]
2. Fixed an issue in Compliance Manager that caused Low Memory Alerts and Low Battery Alerts to be triggered for deleted users. [7859]
3. Corrected an issue where the maximum email age for synchronization setting was updating ActiveSync servers, but not the Exchange servers assigned to iOS devices. [7972]
4. The username field for a subscribed calendar is no longer a required field. [8149]
5. Added a secure flag to all cookies sent over SSL. [8304/8305]
6. Disallowing Read Only access for reports in the administrator role permissions only prevented an administrator from exporting report data. Now it prevents the administrator from viewing reports altogether. [8596]
7. Fixed an issue that caused Sprint and Verizon iOS 5.1.1 and higher devices to return a pop up stating “Could not activate cellular data network” when policy changes to “Allow voice roaming” or “Allow data roaming” were made. [8660]
8. Fixed an issue with the Administrative Roles reports that prevented data from exporting properly when information was collapsed in the grid. [8744]
9. Fixed an issue that caused the failure of client certificate installations from the Mobile USAP. [9169]
10. Fixed an issue that made Wipe options unavailable in the Desktop USAP for Android devices enrolled with NotifyMDM only. [9233]
11. Improved the logging for network errors in the Licensing Log. [9338]
12. Other various Dashboard and UI bug fixes.

Version 2.5.5

Description: Update
Date: 2012.08.13

Changes/New Features

1. Rebranding of the Mobile User Self Administration Portal.
2. Added a background thread on the NotifyMDM server that updates LDAP Custom Columns for users once every 24 hours.
3. Update Manager Dashboard and app: A button has been added for re-downloading updates that may have failed while downloading. [9182]

Bug Fixes

1. Fixed an issue where a selective wipe would fail for an iOS device because no secondary profiles are detected. [7950]
2. Fixed a few issues where File Share permissions were not saving correctly in the dashboard. [8441, 8446, 9251, 9262]
3. Fixed an issue where after configuring a Wifi network and turning on the option for Auto Join, the Auto Join option is not sent to an iOS device. [8458]
4. Fixed an issue where the logging data grids can take a long time to sort by column. [8717]
5. Fixed an issue with iOS devices where an error is continually returned when an app is already on the device and that same app is then forced to the device to be installed again. [9023]
6. Fixed an issue where a file would not upload into the File Share due to bad date properties on the file. [9077]

7. Fixed an issue where iOS devices that do not have device statistics are unable to select the clear passcode option in the Dashboard. [9105]
8. Other miscellaneous Dashboard bug fixes. [5896, 7993, 8545, 8631, 8863, 9055]

Version 2.5.4

Description: Update
Date: 2012.07.23

Changes/New Features

1. Rebranding of the Desktop User Self Administration Portal.
2. Autodiscover UI display of the resolved server address in User Profile.
3. iOS/APN Profile Reload Changes
    a. APN profile will not reload on the device unless changes are made to access rights, topic or URL only. [8269]
    b. Changes to iOS Devices policy settings should no longer cause all profiles to reload on device. [8408]
4. Database Task Scheduler Changes
    a. Upon completion, scheduled tasks will appear within logs and be listed with its respective name. [8818]
    b. A new task was added for defragmenting indexes. This will be turned on by default. [8931]
    c. The default execution time for tasks is now separated by 30-minute intervals, starting at midnight (database server local time). [9020]

Bug Fixes

1. Fixed the Group Emailing functionality located in the dashboard.
2. Fixed an issue where all iOS resource assignments were not being retained when clearing device enrollment. [9090]

Version 2.5.3

Description: Update
Date: 2012.07.23

Changes/New Features

1. Customer column filtering for user grid and policy suite assignment changes.
2. Improvements to multiple devices per enrollment.
3. Implementation of Autodiscover on the backend.
4. iOS/APN Change
    a. APN chaining has been implemented. When there are several commands queued for the device, only 1 APN is needed for the device to process all commands. [6811]
5. Dashboard access restrictions when a license is invalid.
    a. System and Organization administrators will have access to System Management, but no other views

Bug Fixes

1. Fixed a grid refresh issue while scrolling for System/Organization Administrative Roles. [9084]
2. Fixed an issue where the items in the custom column drop down box were not displayed in ascending order. [8712]

3. Fixed an issue where after encrypting an Android tablet, native ActiveSync on the device does not sync with the server. [8133]
4. Fixed an issue with Mobile Apps not being able to install onto a Symbian device. [8506]

Version 2.5.2

Description: Update
Date: 2012.07.16

Changes/New Features

1. Updated to use PHP 5.3.10.
2. Role Based Administration UI
    a. Within the NotifyMDM Dashboard:
        i. Set administrators to the default Full, Support or Restricted admin roles.
        ii. Create custom admin roles.
        iii. Restrict Organization Admin Roles to privacy protect by User or Policy Suite.
3. Advanced Logging
    a. Logging can be viewed in the dashboard at a user level under the User Profile and at a system or organization level under System.
4. Enrollment Redesign
    a. Addressed issues with license seat counts and device statistics not displaying properly after enrolling/re-enrolling multiple devices per user. [7631, 7839]
5. Additional Reporting for Administrative Role reports and Data Usage by DeviceSAKey
6. Added the ability to prevent the automatically generated email messages for device wipes and locs from being sent out by the NotifyMDM server. This can be done within Compliance Manager. [7855]

Bug Fixes

1. Fixed an issue where an Organization Administrator could disable themselves in the dashboard. [2841]
2. Fixed an issue where Android devices require encryption after hands-off enrollment event though it is not required within the policy suite on the NotifyMDM server. [7538]
3. Fixed an issue where after encrypting an Android tablet, native ActiveSync on the device does not sync with the server. [8133]

Version 2.3.0

Description: Update
Date: 2012.04.13

Upgrade Notes

1. Customers who have Corporate Resource Restrictions for the following Access Policies will need to verify their settings under Device Platform Restrictions after completing the upgrade. a. Restrict if policy out of date
    b. Restrict if location not updated
    c. Restrict user NotifyMDM connections

Changes / New Features

1. User Grid
    a. Added the Last iOS APN Timestamp to the user grid
2. Compliance Manager
    a. “Access Policies” has been renamed “Access Restrictions”
    b. “Device Restrictions” has been renamed “Device Platform Restrictions”
    c. Moved several Access Restrictions into Device Platform Restrictions. The corresponding Alerts have been moved from Access Restriction Based Alerts to Non-Access Restriction Based Alerts:
        i. Restrict if policy out of date
        ii. Restrict if location not updated
        iii. Restrict user NotifyMDM connections
    d. Added additional Device Platform Restrictions for the iOS Platform:
        i. Restrict if no iOS APN connectivity
        ii. Restrict is iOS APN profile not installed
    e. Added an iOS APN Timeout setting to Watch Lists
3. Supported Devices
    a. Added a means for an Admin to allow only officially supported (certified by Notify Technology) devices to connect to the server [8013]
    b. Added a means for an Admin to add non-certified device manufacturers, models, and operating systems to a supported devices list. In this first phase, this is accomplished with database commands. Customizing the supported devices list via the Dashboard will be implemented in subsequent development phases.

Bug Fixes

1. Fixed an issue resulting in unnecessary iOS profile reload prompts. [7649,8182,8227]
2. Fixed an issue resulting in the inability to remove an Organization from the server. [8228]
3. Fixed an issue with multi-select functionality on the Alerts grid. [8296]
4. Changed incorrect text labels under Smart Devices and Users. [4756,4757]
5. Fixed a User Profile issue when disabling APN certificates. [8397]

Version: 2.2.0

Description: Update
Date: 2012.03.28

Changes / New Features

1. Administrator Roles
    a. Added a new default administrator role for restricted admin.
        i. The restricted admin will have similar access as a support admin, but no access to any of the audit data.
    b. Added the framework to add new Administrator Roles
2. Administrator Audit Trails
    a. Added a means to record changes to a policy suite
    b. Added a way to log any security actions for the user. Items covered in this are any of the mini-admin actions, like wipes and locking the device.
3. Buttons in the menu bar have been reformatted. They will now follow a new color scheme.
4. Subscribed Calendars have been added to the restrictions in compliance manager. [8034]

Bug Fixes

1. Fixed an issue with locking an android device from the dashboard. [8186]

2. Changed the behavior when exporting a device log. [8143]
3. The Activity Monitor has been corrected, so it will show the proper number of elements. [8130]
4. Corrected an issue when downloading client certificates from the mobile USAP. [7958]

Version: 2.1.1

Description: Update
Date: 2012.03.13

Upgrade Notes

1. Version 2.1.0 should not be applied without version 2.1.1

Bug Fixes

1. Enhancement for upgrade process.
2. Fixed an issue with syncing a policy change and Apple advanced MDM functionality.

Version: 2.1.0

Description: Update
Date: 2012.03.08

Upgrade Notes

1. Version 2.1.0 should not be applied without version 2.1.1

Changes / New Features

1. Activity Monitor
    a. Fifteen additional graphs have been added to the Activity Monitor giving an administrator a total of 34 graphs from which to choose.
    b. The Devices by Platform chart has been changed to Devices by Platform -> OS -> Model.
        i. The behavior of this chart is now interactive, where clicking on slices of the graph will reveal the OS or device models.
        ii. There is now a back button at the bottom right which will take you to the previous level of the chart.
    c. The Activity Monitor will retain the last state. [3212]
2. Policy Suite changes for iOS Devices, to incorporate additional iOS 5 functionality.
3. Newly added support for Subscribed Calendars. These will act the same way as the other iOS resources. [5455]
4. Corporate Resources for iOS Devices in Organization Management has been realigned because of the addition of Subscribed Calendars. [7869]
5. The dashboard logo and login logo have moved from the Plug-Ins section to System Settings. [7909]
6. Device Restrictions in Compliance Manager is now more flexible, where now you do not need to enter a manufacturer and a model before selecting a minimum and maximum OS.
7. The user grid now has the option to see the installed and managed profiles on the device. [7393]
8. Showing error messages in the dashboard are more user friendly. [7908, 7926]

Bug Fixes

1. Secondary configuration profiles remain on the device after Clear Device Enrollment. [6294]

2. The AuthPlain option has been removed for mail servers in iOS resources. [6348]
3. Downloading items from the file share now takes less time. [6431]
4. The last run time and next run time for database task scheduler are now accurate. [7438, 7462, 7463, 7464]
5. Description and notes will now save properly in file share. [7818]
6. Uploading a certificate in the desktop USAP page has been fixed. [8020]
7. Downloading a certificate in the mobile USAP page has been fixed. [8021]
8. Fixed an issue with searching by platform in the user grid. [8086]
9. Optimized removing company resources for an iOS device in violation. [8048]

Version: 2.0.1

Description: Update
Date: 2012.02.09

Changes / New Features

1. Added a policy suite setting to enable or disable the multiple devices feature.
2. Ability to send the user's device an SMS during hands-on enrollment to simplify the process.

Version: 2.0.0

Description: Update
Date: 2012.02.09

Upgrade Notes

1. Customers who are upgrading MUST use the Update Manager to apply version 2.0.0. Only customers performing their initial installation should use the NotifyMDM installer.
2. With this release, it is recommended that upgrading customers set their JobsSleep to 5 in MDM.ini. After making the change to the ini file, IIS must be restarted. Note that customers who install 2.0.0 as their initial release will have this value set by default and do not need to make a change to the MDM.ini.
3. Warnings and Alerts Settings defined in NotifyMDM v1.9.x will NOT be retained during upgrade. To configure these settings, please refer to the Recommended Best Practices for Upgrade guide on the NotifyMDM portal.
4. Warning notifications on the Activity Monitor and Alerts view will NOT be retained during upgrade. [7888]

Changes / New Features

1. Introduction of Compliance Manager feature.
    a. This includes the following:
        i. Manage Access Policies for user and/or device connectivity
            1. Setting the "Restrict if Policy Out of Date" Access Policy to a value higher than the JobsSleep in the MDM.ini file can cause a state of restriction even if the user is in Compliance with the Access Policy. [6599]
            2. Running NotifySync only without enrolling the NMDM component can trigger the "Restrict BBPs without NS" Access Policy. When enrolling with the latest

NotifySync app it is only possible for this to happen in the case of a migration (from NotifySync only to NotifySync + NotifyMDM). [7618]

3. The "ActiveSync Authorization Failures" Access Policy can be triggered at a rate faster than intended on both iOS and TouchDown devices. Each of these ActiveSync clients attempt to authorize multiple times prior to reporting that the authorization failed on the device. [7530 / 7740]

ii. Create specific Device Restrictions for accessing resources
iii. Create User Exceptions for connectivity and resource permissions
iv. Watch connectivity of specific users

1. The "ActiveSync Timeout" setting is checked differently depending on whether the connection being used is Direct Push or Scheduled Push. A user may be seen as not being in Compliance in the user grid due to the ActiveSync connection being refreshed upon the creation of a new connection, instead of the continuation of a connection as seen with Direct Push. The device will still be treated as if it were in Compliance. [7289]

v. Manage Alert Settings
vi. Add Alert Recipients for Email and SMS Alert notifications
vii. Send e-mail to users when they have been restricted.

b. SIM card removed or changed Restriction and Alert are not working reliably with global phones. Due to CDMA Network based devices (ie. Sprint and Verizon) setting their IMSI Number on the phone hardware and not the SIM card, tracking the status of the SIM card is not reliable. [7490]

2. Removed Warnings from the Activity Monitor and Alerts view of the Dashboard. Alerts are now the only method of Administrator notification.
3. Added new columns to the Smart Users and Devices grid
    a. ActiveSync Authorization Failures
    b. NotifySync Authorization Failures
    c. IMSI Number
    d. SIM Card Removed or Changed
    e. Violation Status
4. Added Compliance Reports to the User and Device Reporting options.
    a. Access Policy Violations
    b. Exceptions by User
    c. Restricted Device
    d. Restrictions by User
    e. User exceptions

Bug Fixes

1. Changed the retry from 60 minutes to 15 minutes for APN requests that have timed out. [7638]

Version: 1.9.3

Description: Update
Date: 2012.01.20

Bug Fixes

1. Fixed a memory leak that occurred when sending an APN that resulted in an error.
2. Improved handling of APNS error codes.

Version: 1.9.2

Description: Update
Date: 2011.12.29

Changes / New Features

1. Activity Monitor
    a. Thirteen additional graphs have been added to the Activity Monitor giving an administrator a total of 19 graphs from which to choose.
    b. A translucent Overlay screen has been added to give the administrator a method for opening a list of available graphs, previewing graphs, and choosing the 6 graphs to be displayed.
    c. The 6 graphs in the displayed in the dashboard are remembered for the next dashboard login.
2. Database Task Scheduler
    a. Database task scheduler gives an administrator with full system admin credentials the ability to maintain database tables.
    b. System admin can schedule standard database cleanup tasks for a table or custom stored procedures to run at regular intervals.
    c. An administrator can remove, edit, or enable/disable database tasks.
    d. A database task can be run at any time (on-demand) outside the regularly scheduled runtime.
3. Multiple Devices
    a. Support for Multiple Devices per user account. This replaces the method formerly used to achieve multiple device enrollments, which required the creation of alias user accounts on the mail server.
    b. Successful enrollment of multiple devices requires that each device be fully enrolled against a user's account before a subsequent device is added. The account protocol used on each device must be the same.
    c. User Self Administration portals allow users to select which device to manage.

Bug Fixes

1. Implemented a change that allows devices using ActiveSync protocol 14.1 to enroll and function with NotifyMDM. [6337 / 6708]
2. Corrected an issue which prevented using Clear Enrollment if only ActiveSync had synchronized for a device. [7263]

Version: 1.9.1

Description: Update
Date: 2011.12.06

Bug Fixes

1. Improved Report exporting:
    a. Fixed an issue with character encoding [6502]
    b. Resolved issue with column headers being duplicated [7153]
    c. When using CSV export, corrected a problem with commas within the data [7156]
2. Fixed an issue where "Clear Enrollment" would fail if there is an app removal queued for the device. This applies to apps that are managed via the iOS Developer Enterprise Program (iDEP) advanced MDM functionality. [7173]

3. This applies to both the VPN configuration and the WiFi network configuration for iOS devices. If the configuration is loaded to the device, then deleted by the user, the configuration was not resent to the device. This has been corrected. [7168]
4. Added a 'Scale to Fit' option to the Plug-ins page. When selected, the SWF expands in size until reaching the display window constraints. When not selected, the SWF will display at the initial size. [7095 / 7100]

Version: 1.9.0

Description: Update
Date: 2011.12.06

Changes / New Features

1. Additional capabilities for managing mobile applications for iOS 5 users. Requires the use of Apple Developer Enterprise Program (iDEP) advanced MDM functionality. Added features include:
    a. Administrators can view, install, uninstall, or edit mobile apps at the user level.
    b. Administrators can install apps automatically (force push) to all iOS 5 users associated with a policy suite.
    c. Ability to add enterprise (in-house) apps or iTunes apps to the Mobile App list.
    d. Ability to add and manage redemption codes associated with apps obtained via the Apple Volume Purchase Plan (VPP).
    e. Ability to control whether a user can backup app data via iTunes.
    f. Ability to tag an app added to the Mobile App list to be removed, along with any data associated with the app, when the MDM profile is removed.
    g. When editing an app on the Mobile App list, administrators have the ability to force an app update on devices that have already had the app installed on the device via MDM.
2. Policies have been added for iOS 5 devices on systems that employ the Apple Developer Enterprise Program (iDEP) advanced MDM functionality. These policies include:
    a. a rule that determines whether apps can be managed for users associated with a particular policy suite
    b. allow/disallow voice roaming
    c. allow/disallow data roaming
3. For organizations with Apple Developer Enterprise Program (iDEP) advanced MDM functionality, what was a single iOS Configuration Profile on an iOS 5 device is now split into 3 profiles: ActiveSync, Restrictions, and Passcode. In addition, there is an individual profile for each iOS Resource assigned to a user. When polices or resource information are edited, only the profile affected is updated. [6328]
4. Information associated with apps added to the Mobile App list for Android, BlackBerry, Symbian, and Windows Mobile users can be edited.
5. Added the ability to export reports in a .CSV or .XLS format. Additional report functionality includes: the ability to rearranged columns, change the report sorting order, and collapse/expand parent groups.
6. Ability to deploy client authentication certificates (or identity certificates). Functionality includes:
    a. The ability for administrators to upload the certificate to the user profile and manage the certificate via the dashboard.
    b. The ability for a user to upload the certificate to his/her user profile and install the certificate on a device via the Desktop User Self-Administration portal.
    c. The ability for a user to install the certificate on a device via the Mobile User Self-Administration portal.
7. Improved Back/Forward navigation functionality in the dashboard's System Management view.
8. Added a Plug-in feature, which allows an administrative user to implement a server interface with NotifyMDM. Includes the ability to add a customized login logo, dashboard logo, and plug-in icon.

Requires development, on the company's (or administrator's) part, of a plug-in SWF. Contact Notify Technology for more information.

9. When an APN cert is added after devices are already enrolled, the configuration must be reloaded. There is now a configuration reload triggered automatically when the APN is added. [5671]
10. When using an APN cert, the device's Phone Number is able to be reported to the NotifyMDM server. Previously, the phone number was only shown in a user's profile under the 'iOS MDM Settings' > 'Device Information'. This is now also displayed in the Last Sync Data and the user grid. [5696]

Bug Fixes

1. Change to correctly handle ActiveSync server address URLs that contain a slash as seen with Lotus Traveler and with Google Apps Premier. [6711]
2. Corrected issues with deletion of Organizations. [3471 / 3957 / 5661]
3. Added additional Ratings policies. [5581 / 5583]
4. Corrected an issue that could result in the configuration profile(s) arriving to the device as unsigned when a signing certificate has been added. [6459 / 6474]
5. For an APN cert, the Server URL and Check in URL can now be edited. [5679]
6. When adding an APN cert, the Check in URL will default to SSL. SSL is required by iOS 5 devices. [6707]

Version: 1.8.4

Description: Update
Date: 2011.10.07

Changes / New Features

1. Device Registration will now be known as Enrollment in NotifyMDM. [6008]
2. Enabled downloading files and the apps from the server in smaller chunks. This requires a 1.8.4 device app.
3. Extended support for managing Mobile Apps to Windows Mobile and Symbian devices. [5991]
4. Added the ability to customize the accuracy of device location. This is supported by 1.8.4 device apps on BlackBerry, Android and iOS. In Windows Mobile the user can choose the positioning technology but not the distance traveled after which the device syncs.
5. Added battery status information to the dashboard statistics for Symbian devices. [5759]
6. Added options on the User Self-Administration Page to perform device commands for Symbian devices. [5864]
7. Added a new setting to enable the administrator to set http timeout for downloading software updates. [5977]
8. For organizations with Developer Enterprise Program (iDEP) advanced MDM functionality, organization administrators (in addition to system administrators) can now change iOS MDM policy settings, view advanced iOS MDM information in the user profile, and issue a selective wipe to an iOS device. [6037]
9. Administrative preferences are saved for the Smart Devices and Users grid, specifically, the columns selected for viewing and column order. [2761]

Bug Fixes

1. Fixed an issue that was preventing administrators from removing an item from the Mobile Apps list on the server. [6170]

2. Fixed an issue with File Share in which files with very long extensions could not be added to the list. [5719]
3. Fixed an issue with Selective Wipe that occurs on iOS devices that were added to the server before Developer Enterprise Program (iDEP) advanced MDM functionality is implemented on it. [5658]
4. Added the option to Clear Passcode for iOS device registered on a server that utilizes Developer Enterprise Program (iDEP) advanced MDM functionality. [5674 / 5675]
5. Resolved an issue where a device was unable to sync location data after receiving an SMS message from a phone with a very long phone number. [6013]
6. Fixed the attachment download issue with Kerio mail server accounts. [5600]
7. Fixed an issue with Device by Liability Reports: Devices enrolled via the Hands-off method were not correctly grouped by liability status (Individual/Corporate). [6110]
8. "Card Clear Confirmation" emails, sent when the user clears his/her storage card, will now read, "Wipe Storage Card Confirmation". [6331]
9. Selective Wipe command for iOS Device will also send a "Selective Wipe Confirmation" email, along with the "Lock Device" command and email. [6217]
10. Code clean-up.
11. Fixed memory leaks.
12. Fixed miscellaneous UI issues.

Version: 1.8.3

Description: Update
Date: 2011.09.23

Bug Fixes

1. Fixed an issue that prevented iOS apps with no name from being stored in the database, on servers that utilize Developer Enterprise Program (iDEP) advanced MDM functionality.
2. Fixed an issue that prevented installing CalDAV/CardDAV profiles when the Principal Address was larger than 65 characters, on servers that utilize Developer Enterprise Program (iDEP) advanced MDM functionality.

Version: 1.8.2

Description: Update
Date: 2011.09.20

Bug Fixes

1. CalDAV and CardDAV's Principal Addresses are no longer defined in Organizational Management. They are now defined when assigning CalDAV or CardDAV to a user.
    a. If a Principal Address is already defined, the information will not be retained when upgrading to 1.8.2. Please enter this information in the relevant User Profiles.
2. Group Name and Shared Secret, defined in VPNs under Organization Management, are now optional fields and can be left blank.

Version: 1.8.1

Description: Update
Date: 2011.09.01

Bug Fixes

1. Fixed issues with the feature which allows an administrator to request a device's log.
    a. Feature was not working correctly for iOS and BlackBerry devices.
    b. Updated the NotifyMDM App version requirement which is displayed for iOS devices.
    c. Fixed an issue in which the extension of the requested log file was being ignored.
2. Fixed an issue in which NotifyMDM may reuse resources incorrectly.

Version: 1.8.0

Description: Update
Date: 2011.08.09

Changes / New Features

1. Added an integrated update management features that facilitate software updates to the NotifyMDM server. These features include the dashboard's **Update Management** section and *the **Update Manager Application***, which is used on the physical NotifyMDM server(s) to apply updates.

    Update Management in dashboard:
    a. The NotifyMDM server automatically checks for updates once every 24 hours and whenever a manual license validation is initiated (in Organization Settings). You can also initiate a check by using the 'Check For Updates' button in the **Update Management** page of the dashboard.
    b. When an update is available, system administrators logging into the NotifyMDM dashboard will see a notification for the update in the lower left corner of the dashboard. The notification fades away automatically or the administrator may dismiss it. Clicking on the notification will navigate to the **Update Management** section of the dashboard.
    c. The administrator can view information about the available update(s) or download the update(s).

    Update Manager Application:
    a. Windows application that is accessed via a desktop shortcut on the NotifyMDM server.
    b. Ability to apply updates to the NotifyMDM server. Applying updates can only be performed by System Administrators that have the Full Admin role.
    c. Ability to check for new updates and read change logs for the updates.

Version: 1.7.0

Description: Update
Date: 2011.07.12

Changes / New Features

1. Added support for advanced Apple MDM API by using the Apple Developer Enterprise Certificate. An APNs certificate must be added to each organization that wants to use the API. If there are existing registered users when the APNs is added, the iOS users must reload their profile in order to start using the APNs. They will not be automatically prompted for perform this step. Additionally, when the new profile is loaded, they will then be prompted for their ActiveSync account password.

   Note that when using an APNs certificate, the device connection schedule should be not be set to a short interval (such as 1 minute). [5381]

   Features include:
   a. Ability to view additional device statistics such as Available Device Capacity, IMEI/MEID, Phone Number, and many more. To view the stats, in Smart Devices and Users, view a user's profile and choose the 'iOS MDM Settings' > 'Device Information'.
   b. Ability to view a list of installed applications. To view the applications, in Smart Devices and Users, view a user's profile and choose the 'iOS MDM Settings' > 'Installed Applications'. This feature can be controlled by 'Record installed applications' in the Policy Suite > iOS Devices > iOS MDM.
   c. Ability to view a list of installed configuration profiles. To view the applications, in Smart Devices and Users, view a user's profile and choose the 'iOS MDM Settings' > 'Configuration Profiles'. This feature can be controlled by 'Record installed configuration profiles' in the Policy Suite > iOS Devices > iOS MDM.
   d. Ability to silently update/remove configuration profiles that are managed by NotifyMDM. The initial installation of the configuration profile will still require user interaction.
   e. Ability to 'Selective Wipe' the mail, calendar, and contact data that is managed by NotifyMDM. This security action can be performed by the administrator in the dashboard or by the user in the USAP.
   f. Ability to Lock Device. This security action can be performed by the administrator in the dashboard or by the user in the USAP.
   g. Ability to Clear Passcode. This security action can be performed by the administrator in the dashboard.
2. 'Clear Storage Card' has been renamed to 'Wipe Storage Card'. [5554]

Bug Fixes

1. Selective Wipe feature has been disabled for Windows Mobile devices. [5082]
2. The tooltips for Selective Wipe and Full Wipe have been updated. [5542, 5623]
3. Corrected an issue with Organization names that contain special characters. Previously, if an Organization's name has any special characters in it, the configuration profile could not be loaded. An error was displayed on the device stating "Cannot Install Profile, Safari could not install a profile due to an unknown error." [5103]
4. Modified the High security level to change application rating from 'Don't Allow Apps' to '12+'. [5041]
5. Modified the High security level to default all policies to the same for both Corporate and Individual liability. [5365]

Version: 1.6.0

Description: Update
Date: 2011.06.21

Changes / New Features

1. Added support for TouchDown policies and suppressions. Features include, but are not limited to:
    a. New setting to automatically initiate TouchDown registration after NotifyMDM registration.
    b. Policies to control values in general settings, phone book settings, signature, and widget settings in TouchDown.
    c. Suppressions to completely hide TouchDown settings from the end user (menu items are not shown).
2. Changed wording of security features to better explain their behavior:
    a. Clear Device is now Selective Wipe
    b. Wipe Device is now Full Wipe
3. A new Warning / Alert setting has been added for 'TouchDown Policy Override Detection'. This warning is triggered when a user uses the Quick Configuration button within the TouchDown app. This would indicate the account information has changed and may not match NMDM registration. Administrators may wish to act on this information by disabling the user, deleting the user, reaching out via e-mail, etc.
4. Added a feature that allows the administrator to request a device's log via the dashboard. When the device receives the request it will respond by sending the log, which can then be acted on in the dashboard. The administrator can save the log to a file and view it in a word processing application. Requires:
    a. Android NotifyMDM v1.6.0.14 or greater. The logcat will be retrieved.
    b. iOS NotifyMDM app v1.5.1 or greater
    c. NS/NotifyMDM app v4.9.2 or greater. An SD card is required and logging must be enabled on the device for this feature to work.
5. Sections within the Policy Suite can now be collapsed and expanded to improve usability.
6. The Welcome letter settings have been moved to its own section in the Policy Suite.
7. Policy Suite defaults have been modified so that look back settings are never more than one month.
    a. Maximum calendar age for synchronization
    b. Maximum email age for synchronization
8. The Sync Schedule has been renamed to Device Connection Schedule. This is the schedule for the NotifyMDM app connecting to the NotifyMDM server.
9. Refreshing of the Smart Devices and Users grid has been improved. When the administrator navigates to another view and then back to the grid, the data in the grid is refreshed. The last search criteria and the previously selected user will be retained.

Bug Fixes

1. The Policy Suite options for Allow all and Deny all will now set the values of drop downs as well as sliders.

Version: 1.5.1

Description: Update
Date: 2011.05.23

Changes / New Features

1. Changes to support multiple IIS worker processes (i.e. web garden).
2. Changes to make use of SQL connection pooling.

Version: 1.5.0

Description: Initial Public Release
Date: 2011.04.04

Changes / New Features

1. Options for adding users including: manual, hands-off, LDAP import, csv import.
2. Management of policies on the device.
3. Monitoring of device statistics, location, SMS/MMS messages, and more.
4. Reporting of data.
5. Jailbreak detection and blocking of jailbroken/rooted iOS/Android devices.
6. Improved labels in Warnings and Alerts view.
7. Added support for multiple domains associated with an ActiveSync server.

Bug Fixes

1. LDAP authentication for administrative logins.
2. Corrected display issues with time zone.
3. Adding a user that previously existed and was removed.
4. Corrected labeling issues with ownership and liability.