Server Release Notes

ZENworks® Mobile Management 3.2.x

October 2015

Novell®

Legal Notices

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

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

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

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

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

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Table of Contents

ZENworks Mobile Management Server Release Notes

The *ZENworks Mobile Management* server is a component of *ZENworks Mobile Management* system that serves as a management and policy enforcement platform for mobile devices.

ZENworks Mobile Management 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 *ZENworks Mobile Management* device applications and also by using the ActiveSync protocol.

This document provides a history of releases including dates, known issues, and notes for the *ZENworks Mobile Management* Administrator.

Revision History

Date	Author	Description of Changes
2015.09.09	Anthony Costello	3.2.1 Update
2015.07.27	Anthony Costello	3.2.0 Update
2015.04.06	Anthony Costello	3.1.1 Update
2015.03.05	Anthony Costello	3.1.0 Update
2014.12.05	Anthony Costello	3.0.1 Update
2014.08.01	Anthony Costello	3.0.0 Update
2014.05.07	Anthony Costello	2.9.1 Update
2013.12.02	Anthony Costello	2.9.0 Update
2013.11.20	Anthony Costello	2.8.2 Update
2013.11.04	Anthony Costello	2.8.1 Update
2013.09.09	Anthony Costello	2.8.0 Update
2013.08.05	Anthony Costello	2.7.8 Update
2013.07.22	Anthony Costello	2.7.7 Update
2013.07.22	Anthony Costello	2.7.6 Update
2013.05.28	Anthony Costello	2.7.4 / 2.7.5 Updates
2013.05.06	Anthony Costello	2.7.3 Update
2013.04.12	Anthony Costello	2.7.2 Update
2013.04.03	Anthony Costello	2.7.1 Update
2013.02.05	Anthony Costello	2.7.0 Update
2012.12.03	Anthony Costello	2.6.1 Update
2012.10.29	Anthony Costello	2.6.0 Update
2012.07.30	Anthony Costello	2.5.5 Update
2012.07.16	Anthony Costello	2.5.4 Release

Installation Information

Date: 05/28/2013
Product: *ZENworks Mobile Management* Server

Requirements

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

- Windows Server 2008 R2 SP1 / 2008 with SP2 / 2003 R2 x64 / 2003
  - Including Microsoft IIS
  - Apply all Windows Server updates
    Note: Windows Server 2003 is not supported for *ZENworks Mobile Management* server versions 3.1.0 or greater.
- Microsoft SQL Server 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 R2
- An SMTP server

Installation Package

Name	Version
smailpp.dll	2.4.0.21
ntc_mdm_AdminAuthenticator.dll	2.7.0
ntc_mdm_AdminRoles.dll	2.7.0
ntc_mdm_AirProxy.dll	2.7.0
ntc_mdm_AirSyncParser.dll	2.7.0
ntc_mdm_APN.dll	2.7.0
ntc_mdm_AutoEmailChecker.dll	2.7.0
ntc_mdm_BaseQueryOffloader.dll	2.7.0
ntc_mdm_CommandBase.dll	2.7.0
ntc_mdm_ConfigFileReader.dll	2.7.0
ntc_mdm_CriticalLogger.dll	2.7.0
ntc_mdm_DatabaseInterface.dll	2.7.0
ntc_mdm_DatabaseLogger.dll	2.7.0
ntc_mdm_DatabaseLoggerWrapper.dll	2.7.0
ntc_mdm_DatabaseTaskScheduler.dll	2.7.0
ntc_mdm_HTTPInterface.dll	2.7.0
ntc_mdm_IOSMDMParser.dll	2.7.0
ntc_mdm_IOSMDMSync.dll	2.7.0
ntc_mdm_ISAPIRedirectFilter.dll	2.7.0
ntc_mdm_Jobs.dll	2.7.0

ntc_mdm_Licensing.dll	2.7.0
ntc_mdm_MailComposer.dll	2.7.0
ntc_mdm_MDMParser.dll	2.7.0
ntc_mdm_MDMSocket.dll	2.7.0
ntc_mdm_MDMSync.dll	2.7.0
ntc_mdm_SMTP.dll	2.7.0
ntc_mdm_WBXMLParser.dll	2.7.0

Known Issues

ZENworks Mobile Management Server

1. The *ZENworks Mobile Management* product is not currently localized. Using non-English text in the dashboard might result in unexpected display of the text. [2037]
2. If the Web component of the *ZENworks Mobile Management* 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]
3. If Windows security update KB2509553 is installed on a Windows Server 2003 x64 server, the *ZENworks Mobile Management* SQL Database install does not work properly. Because of this, we recommend that you do not install Windows security update KB2509553 on a Windows Server 2003 x64 server where *ZENworks Mobile Management* will be installed. [5563]
4. An initially long load time can be experienced upon the first visit to the dashboard. You also experience this upon clearing your browser cache, because the dashboard reloads the entire Flash file. [7548]
5. When you are logged in to the Dashboard on multiple tabs within a browser, logging out on one tab causes a session error on the other tabs connected to that server. [7583]
6. Redirects are not handled properly for the ActiveSync server address URL. A possible workaround is to use the redirect address as the ActiveSync server address. [6965]
7. The organization name should not be changed if the iOS APNs certificate is being used. If the organization name is changed, policy changes and selective wipes could fail. [5445]
8. 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]

    The searches that are not working correctly have been disabled. These fields are still visible but text cannot be entered into them. [8586]
9. 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]
10. When the iOS APNs certificate is used, the Current Carrier Network is not being returned properly by the device. [5136]
11. 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 runs this way. If silent mode is not enabled for a given administrator, he or she cannot apply updates. [5197]
12. Clearing a violation on a single device clears the violation on all devices for that user. [8049]

13. When setting Administrator Role permissions in the dashboard, when the user who is logged in and applying the permission to the role that he or she is using, the user must log out and log back in for the new role permissions to take effect. [8633]
14. 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]
15. When exporting logs, only the records that have currently loaded within the data grid are exported. To get all of the data, a user must repeatedly scroll to the bottom of the data grid in order to export all desired records. [8709]
16. 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]
17. When Allow Profile Removal is set to Never under the iOS settings of the policy and the APNs certificate has been disabled, after enrolling an iOS device, the user cannot remove the MDM iOS Mobile Configuration Profile. [8754]
18. The local path for the default Web site is not removed when uninstalling the *ZENworks Mobile Management* server. [8793]
19. When you are installing the *ZENworks Mobile Management* 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]
20. Running a database task manually does not generate an entry in the Database Task Scheduler log. [8819]
21. The Devices by Connection schedule graph in the Activity Monitor counts the registered users whether they have a device registered to them or not. [8825]
22. Device Reports generated can be inaccurate because users who have no devices registered to them are included in the report. [8840]
23. Depending on the settings within the particular .swf file that is being uploaded as a plug-in, it is 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. To receive updates and compliance data to the ZENworks Mobile Management server, a check for updates must be performed manually in either the Update Manager section within the dashboard or the Update Manager app located on the ZENworks Mobile Management server. This is because basic authentication is being used to access the ZENworks Mobile Management Update server. These credentials will only have to be supplied one time after manually checking for updates. After doing so, update and compliance data checks will be performed automatically by the ZENworks Mobile Management server. [8951]
25. When you are attempting to add new users through LDAP to the *ZENworks Mobile Management* server, the eDirectory LDAP to GroupWise 2012 will displays a maximum of 250 users. [9005]
26. When authenticating to the ZENworks Update Server via Basic Authentication through the Update Manager, it is possible to see a crash of the Update Manager if the Basic Authentication credentials entered contain foreign characters. The languages tested where issues were seen are Chinese Simplified, Chinese Traditional, Japanese, Korean, Georgian, Hindi, and Thai. [9070]
27. When you add a user to the *ZENworks Mobile Management* server, selecting the Send Enrollment Message to send an SMS to the user does not send the message. This will be addressed in the next *ZENworks Mobile Management* server release.
28. When using server side Autodiscover, it is possible for an infinite loop of Autodiscovering to occur if the Autodiscover server is the ZENworks Mobile Management server. [9615]
29. After running the 2.6.0 update, all of the pre-existing location times become the Server Local Time recorded for when the server upgrade was performed. [9694]
30. This issue involves users that are added through LDAP and whose policy settings are obtained via a group or folder. When removed from the LDAP server, these users remain on the ZENworks Mobile Management server as they should, but keep the settings from the group or folder. [10518]
31. Currently, groups that do not contain a member attribute can be imported via LDAP into the dashboard. However, using a group without a member attribute does not work properly and returns an error about an invalid username or password. [10812, 10829]
32. 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]
33. 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.
34. 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. ZMM 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 v3.0.1+), subsequent upgrades of ZMM 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.

35. 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 *ZENworks Mobile Management* is interfacing to an ActiveSync server that is set to not allow non-provisionable devices, some Android devices might 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 hands-off registration, initiating TouchDown registration through the *ZENworks Mobile Management* 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 Samsung Galaxy Tab 3 does not adhere to the KNOX EMM HTTP Proxy Browser policy.
5. The Samsung KNOX EMM 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 EMM API by Samsung.
6. The serial number displayed on an Android device may not necessarily match the serial number that it returns to the ZMM server. Thus, what is displayed on the device may not match what is displayed in the ZMM Dashboard.
7. Samsung KNOX
    a. When the "Require encryption on the SD card" policy via KNOX EMM 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 EMM "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 devices 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. If a selective wipe is issued while the user is working in the Workspace container on the device, the selective wipe can be delayed anywhere from 10-20 minutes.
g. Blacklist/Whitelist of apps enforced via KNOX EMM controls the entire device. Blacklist/Whitelist of apps enforced via KNOX Workspace only controls the container.
h. When the KNOX workspace container is created, several apps are automatically installed 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 the whitelist active and have alerts, compliance restrictions, or both enabled, you will be restricted and/or alerted. **To avoid being restricted, you must put 'knox' in the whitelist.**

8. The serial number displayed on an Android device may not necessarily match the serial number that it returns to the ZMM server. Thus, what is displayed on the device may not match what is displayed in the ZMM Dashboard.
9. **Note:** The Certificate Management feature added in ZMM 3.1.0, it is not recommended 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, users are prompted for the password each time the configuration profile is loaded. [3938]
3. If *Require Minimum Password* Length is enabled on the *ZENworks Mobile Management* 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 *ZENworks Mobile Management* 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 is 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 corrects the issue. [4639]
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 you change 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 you are working with managed Enterprise apps, if the .ipa file will be hosted on the *ZENworks Mobile Management* server, the app should be generated with the *ZENworks Mobile Management* server address in the .plist.
9. When working with managed Enterprise apps, if the files is hosted somewhere other than the *ZENworks Mobile Management* server, the host server needs 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 you use the 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 for the web clip will become blank/white. This icon will still have the designated name and will open to a blank white screen. The icon will be removed after the device is reset. [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 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 ZMM server.
17. 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, the notification will automatically clear after it is opened from within the Notification center.
18. 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.
19. When the Enterprise version of the *ZENworks Mobile Management* app is pushed to the device (via the "Push ZENworks Mobile Management 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 ZENworks Mobile Management server version 3.2.0.
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 ZMM 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 Bluetooth is allowed on the device.
3. Windows 10
    - Encryption is not supported in Windows 10 Desktop.
    - Lock Device is not supported in Windows 10 Desktop.
    - Devices – Lock Device 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.

Version History

Version 3.2.1

Description: Update
Date: 2015.09.09

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.
    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.
2. Fixed an issue where managed apps installed through local groups are not removed from the device when the user is removed from the local group.
3. Fixed an issue where the Managed App web clip was being assigned to users regardless of their liability type as long as they belonged to a local group/LDAP group/folder.
4. Fixed an issue where DEP devices failed to enroll if the SQL instance had a different collation than the MDM database.
5. Fixed an issue that caused an alert settings service error to display within Compliance Manager when logged in as an Organization Admin.
6. Fixed sort functionality in the DEP Devices grid.
7. Fixed an issue with Custom Column search in the user grid where only 100 users were returned when over 100 should have been.
8. Fixed an issue that caused a general service error to display when an Organization Admin navigated to Managed Apps or tried to remove an iOS app.

Version 3.2.0

Description: Update
Date: 2015.07.27

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 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. Windows 8.1/10 Support
    a. Enrollment with Federated 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
3. 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.
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 > Managed Apps > iOS.
    e. Added support of the Allow Browser setting under Policy Suites -> Device Control for non-KNOX™ Android devices.
    f. Added the setting "Prompt for authentication to access Managed Apps" under System -> Organization setting to allow credential-based or token-based authentication when viewing Managed Apps from iOS and Android devices.
    g. 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 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.
9. 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.
10. Fixed an issue that could cause the deletion of an Organization to fail.
11. 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 3.1.1

Description: Update
Date: 2015.04.06

***** Attention: Running the ZENworks Mobile Management server on Windows Server 2003 is no longer supported. *****

Changes/New Features

1. Upgraded PHP to 5.6.
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 ZENworks Mobile Management to authenticate VPN connections in iOS devices.
4. Shared Users
    a. Added enrollment for Apple 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
        ii. Disable Fingerprint
    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 ZENworks Mobile Management app as a Device Owner app in Android OS 5+.
7. 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 uncategorized apps did not show up when viewing the apps by category in the dashboard. These apps now appear in the list as ‘uncategorized.’
4. Fixed an issue where a second Apple DEP device enrolled to a user displayed a status of ‘No’ under the *Apple DEP Device* column on the Users/Devices Grid.
5. Fixed a branding issue within the alert text for when the ZENworks app is not enrolled.
6. Fixed some tab display and layout issues with the Desktop User Self-Administration Portal when viewed within Internet Explorer.
7. Other miscellaneous bug fixes.
8. Performance improvements.

Version 3.1.0

Description: Update
Date: 2015.04.06

***** 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 ZMM 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 Wi-Fi configurations.
2. Added Cisco ISE support.
    a. Added the ability to enroll a device via Cisco ISE and communicate with ZMM
    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 ZMM server.
    c. After the data has been re-encrypted to use the Safelogic libraries, the ZMM 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 ZMM server.
    c. Added the ability to have a non-shared user Sign-in/Sign-out and have it tracked on the ZMM 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 Wi-Fi 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.

Bug Fixes

1. Fixed an issue where the ProfileList command for iOS devices gets stuck In-Flight.
2. Fixed an issue where an Organization admin is logged out of the Dashboard when trying to assign an Exchange corporate resource.
3. Fixed an issue with the Audit Trail table in the database to ensure the correct interface is being logged for the actions.
4. Fixed an issue where the contents of the Organization default drop downs did not refresh when another organization was selected.
5. Fixed an issue with reports not displaying foreign characters correctly.

6. Fixed an issue where a long NPNS certificate and key name can run outside the pop-up box of where the key is added.
7. Other miscellaneous bug fixes.

Version 3.0.1

Description: Update
Date: 2014.12.05

Changes/New Features

1. Added additional support for KNOX EMM.
    a. Updated “Samsung KNOX EMM Policies” in the Dashboard with sections for Alternative Home Screen, Application, Device Feature and Password policies supported by KNOX EMM.
        i. Added additional Password and Restriction policies.
        ii. Added additional policies under Device Features.
        iii. Added 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.
    c. Implemented the policy for the blacklisting and whitelisting of apps.
2. Added additional support for KNOX Workspace.
    a. Added the ability to install Enterprise apps inside the container.
    b. Implemented the policy for the blacklisting and whitelisting of apps.
3. Added support for App Categorization in the Dashboard.
4. Under Organization, changed “Group E-mailing” to “Group Notifications” and added support for iOS APN and Google GCM push notifications.
5. Added the ability to send an NPNS or GCM message to a user from the User Panel in the Dashboard by adding the “Send Notification” hyperlink under Messaging.
6. Added the ability to upload and enable an Acceptable Use Policy to users on the ZMM server. If enabled, users must accept the policy before they can enroll.
7. Added the ability to disable the ActiveSync proxy functionality of the ZMM server.
8. Added the ability to use tokens, constants or a combination of both when assigning corporate resources via LDAP in the Dashboard.
    a. Possible tokens are: {domain}, {username}, {emailaddress}
9. Added support for Web Clusters.
10. Added the ability to enroll via a web page then push the ZMM app as a managed app for iOS devices.
11. 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
12. 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
13. Moved the following iOS policies out of Supervised Mode as they now pertain to all iOS devices.
    a. Allow Global Background Fetch while roaming
    b. Force iTunes store password entry
    c. Force pairing passwords for outgoing AirPlay requests

14. 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.**
15. 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.
16. Added the ability to name iOS Supervised devices in the Dashboard.
17. Added an assignment type to specify either User or Device when creating Custom Columns.

Bug Fixes

1. Fixed an issue where the Activation/De-activation History graph populated data for the original organization if multiple organizations existed on the server.
2. Fixed an issue where the download count of an iOS app was not displaying properly in the Dashboard.
3. Fixed an issue where a policy schedule assigned using Policy Schedules > Assign Schedule To Users option displayed the wrong schedule in the user profile.
4. 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.
5. 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.
6. 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.'
7. Fixed a display issue where the "0 users were found" dialog could appear when uploading, disabling or deleting an APN certificate in the Dashboard.
8. Additional GCM performance and functionality improvements.
9. Additional Managed App performance and functionality improvements.

Version 3.0.0

Description: Update
Date: 2014.08.01

Changes/New Features

1. Added support for Apple's Device Enrollment Program.
2. 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.
3. Added additional support for KNOX EMM.
    a. Updated "Samsung KNOX EMM Policies" in the Dashboard with sections for Alternative Home Screen, Applications, Browser Policy, Device Features Email Policy and Password policies supported through the KNOX EMM API.
        i. Added Alternative Home Screen policies.
        ii. Added additional Password and Restriction policies.
        iii. Added Email, Location and Browser policies.
4. 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 push an Exchange profile into the workspace.
5. Added the ability to detect and report an Android OS build number.
6. Added the ability to handle retina display iOS app icons for enterprise apps that are uploaded through the Dashboard.
7. 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 ZMM user account from the device.

Bug Fixes

1. Fixed an issue in which the iOS HTTP Global Proxy profile was not being removed from a device.
2. Fixed an issue in which encrypted Android devices were not reporting as so in the Dashboard.
3. Fixed an issue in which 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 in which assigning managed apps from multiple levels of assignment were not pushed to the device.
6. Fixed other various issues seen with managed app functionality.
7. GCM performance and functionality improvements.

Version 2.9.1

Description: Update
Date: 2014.05.07

Changes/New Features

1. Added support for Apple's Volume Purchase Program license model, functional for iOS devices running 7.0.3+.
2. Added support for Samsung KNOX Standard, which utilizes the API to enforce password, security, and restriction policies, report devices statistics, and push a Exchange ActiveSync profile to the device.
3. Added localization options to the Desktop and Mobile User Self-Administration Portals and iOS and Android apps. Options include: French German, Italian, Brazilian Portuguese, Spanish, Swedish, Simplified Chinese, Traditional Chinese, and Japanese.
4. Increased the time that a Dashboard service error is displayed before it fades out.
5. Devices statistics Serial Number, WiFi MAC Address, IMEI Number for Android BlackBerry and Windows 8 devices can now be retrieved and displayed in the Dashboard.
6. All instances of "Stop Managing Device" in the Dashboard and User Self-Administration Portals have been renamed, "Selective Wipe." The command's functionality has not been altered.
7. Upgraded PHP to use 5.3.28.
8. 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.
9. Added new ActiveSync Synchronization policy settings under Device Control specific to TouchDown.
    a. "Specific calendar age for synchronization" (US366 and US377)
        - This setting determines a specific number of calendar days that can be synchronized.
        - This option can be suppressed with the "Allow appointment synchronization options" suppression under TouchDown > Suppressions.
    b. "Specific email age for synchronization"
        - This setting determines a specific age for email to synchronize.
        - This option can be suppressed with the "Allow email synchronization options" suppression under TouchDown > Suppressions.
10. Renamed the "Allow personal hotspot" label. It now reads, "Enable personal hotspot."
11. To make sharing devices among users simpler, the "Remove Enrollment" option on an iOS device agent and the "Delete Account" option on an Android device agent will now selectively wipe the device in addition to unenrolling it.
12. Modified the behavior of the Full Wipe command. The device will now be removed from the user grid when the full wipe is completed.
13. 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.
3. Fixed an issue in Compliance Manager for Whitelist App that prevented recipients from being added and saved for email and SMS alerts.
4. Fixed an issue that caused Non-LDAP users to have their assigned corporate resources deleted if an LDPA folder with those assigned corporate resources was deleted.
5. Fixed an issue that prevented all of a user's devices from being removed from the Dashboard User Grid when "Remove User" is selected.
6. 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 2.9.0

Description: Update
Date: 2013.12.02

Changes/New Features

1. Added the ability to add a Filr server under Organization > Application Management, then assign a server configuration via LDAP groups/folders or local groups.
2. Added the ability to assign managed apps to LDAP groups and folders.
3. Updated ZMM documentation links in the dashboard.
4. Updated the ZMM default welcome letter.
5. Added new iOS 7 Restriction Settings:
    a. Under iOS Devices > Device Features
        - Allow fingerprint for unlock
        - Allow lock screen control center
        - Allow lock screen notification view
        - Allow lock screen today view
    b. Under Policy Suite > iOS Devices > Supervised Mode
        - Allow AirDrop
        - Allow assistant user generated content
6. Added GCM logging to the dashboard

Bug Fixes

1. Fixed an issue with the MDM App authorization failure alert. Device violation details would 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 2.8.2

Description: Update
Date: 2013.11.20

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.
2. Fixed an issue that caused a mobile app uploaded in the dashboard with an .ipa and a .plist to fail to install on iOS 7 devices.

Version 2.8.1

Description: Update
Date: 2013.11.04

Changes/New Features

1. Added support for Google Cloud Messaging (GCM) with Android devices.
    - Security actions and policy changes performed from the Dashboard or User Self-Administration Portals will take effect immediately on the device.
    - Enable or disable under System Management > Organization in the Dashboard.
2. Added the ability to create Local Groups.
    - Located under Organization Management > Organization Control in the Dashboard.
    - 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, DE101]
    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, DE3]
    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. [DE98]
    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, US262]
    f. The Context Sensitive Help heading for iOS Configurator has been changed from "iOS Configurator" to "iOS Configurator Devices". [DE88]

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 Wi-Fi 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]
4. Fixed an issue that caused an iOS device to receive an Android Wi-Fi resource after the password of that resource was changed in the Dashboard. [11895]
5. Other various Dashboard and UI bug fixes.

Version 2.8.0

Description: Update
Date: 2013.09.09

Changes/New Features

1. Dashboard performance improvements. (US241)
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 (US235)
    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.” (DE51)
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). (US230)
        v. Added the options and rejection reasons for the InstallApplication command.
        vi. Added the ability to manage a configuration file for the InstallApplication command.
        vii. Added the ability to retrieve configuration and feedback commands for Managed Apps from the device and view them on and export them from device logs.
        viii. Added the ability to view the status reported by the device, via the ManagedApplicationsList command, on the Managed Apps data grid.
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. (US248)
11. Added a new restriction option in compliance manager to restrict an Android user that disables Device Administration.
12. The assigned corporate resource name field for all user corporate resources has been changed from a drop-down field to a labeled field. (DE49)
13. Changes were made to use the device time zone for time-based policy enforcement. (DE47)
14. For BlackBerry 10 devices, the DeviceUID is now populated from the ASDeviceID. (US245)

15. Added the ability to install Managed Apps through the Desktop User Self-Administration Portal for iOS devices.
16. 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.
17. Added the ability to specify the maximum number of devices allowed by a user.
18. Added the ability to do a search for iPad specific apps in the iTunes search and import either iPad only apps or apps that function for all iOS devices.
19. Miscellaneous Dashboard Changes
    a. The “Record installed applications” option has been moved to the iOS Devices > Applications category in Policy Suites.
    b. Renamed “iOS MDM” under iOS Devices in Policy Suites. It is now labeled “Management”
    c. Renamed “Apply managed settings” under iOS Devices > Management. It is now labeled “Allow management of settings.”
    d. Replaced labels and text that referred to “Restricted Apps” with “Whitelists/Blacklists.”
    e. Added a new column called “Activation Date” to the Choose Visible Columns list. This will display the creation date for a user/device in the User Grid.
20. Added the ability to suppress the device passcode and require only a passcode/PIN for TouchDown. [11833]
21. Setting the “Require TouchDown PIN” to ‘ON’ no longer enables require complex, alphabetic, numeric or biometric passwords, as these are not ActiveSync password policies.
22. 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.

Bug Fixes

1. Fixed an issue that caused a VPN profile to not be removed properly from a device. [DE59, 11818]
2. Fixed an issue where after an upgrade, Lock Device and Stop Managing Device alerts were incorrect.
3. 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]
4. Fixed an issue where iOS resources weren’t correctly prompting to update existing users when expiration times changed. [11846]
5. Fixed an issue with iOS devices where native ActiveSync prompted the device password incorrectly.
6. Fixed an issue when adding a new Provisioning Profile that was caused by entering a large amount of characters in the Display Name textbox. It now only accepts up to 64 characters. [11863]

Version 2.7.8

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 2.7.7

Description: Update
Date: 2013.07.22

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 security 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 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]
    - Note: This feature only applies to admin accounts that have been manually created on the *ZENworks Mobile Management* server.
6. New Security policies include Android password requirement options and an option to allow dialing of any number for BlackBerry emergency dialing.

Bug Fixes

1. 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 2.7.6

Description: Update
Date: 2013.07.22

Changes/New Features

1. Time-based policies – A new option called "Policy Schedules" has been added under User Account Settings in the *Organization* view.
    a. The policy schedule determines 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.
2. iOS Configurator/Supervised Mode settings – New settings have been added in the iOS Devices section of Policy Suites under the *Organization* view.
    a. The new settings include:
        - Allow app removal
        - Allow configuration profile installation
        - Allow iMessage
        - Global HTTP Proxy Payload
        - Single App Mode
3. Added the "Require TouchDown encryption" option in the TouchDown section of Policy Suites under the *Organization* view.
4. Added Android VPN support under Android Corporate Resources in the *Organization* view.
    a. Connection Types include F5 SSL and Cisco AnyConnect.

5. Added support for a variety of VPN connection types for iOS devices, in addition to the existing IPSec VPN.
6. Display the APNs Certificate expiration date in the UI and added an alert for APNs Certificate Expiration under System Alerts in the Compliance Manager Alert Settings.
7. Added a policy that enables administrators to automatically push the TouchDown license to Android devices which use the TouchDown app.

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 2.7.4 / 2.7.5

Description: Update
Date: 2013.05.28

Changes/New Features

1. "Blacklist Restrictions" in Organization 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
    f. 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 -> Organization page, administrators now have the ability to enter and display the AppleID with which the APN certificate was generated.
8. Added database cleanup jobs:
    a. *Alerts* – to clear old messages from the Alerts grid.
    b. *Rollover Logs* – to clear records from usage logs.

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 ZMM 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 2.7.3

Description: Update
Date: 2013.05.06

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 that caused the iOS Wi-Fi resource proxy information to be sent incorrectly. [11336]
2. Fixed an issue with LDAP Periodic Updates and foreign language databases. [11179]
3. Fixed an issue that caused an error when sorting File Share by version. [11077]
4. 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]
5. Other various dashboard and UI bug fixes.

Version 2.7.2

Description: Update
Date: 2013.04.12

Changes/New Features

1. Desktop and Mobile User Self-Administration Portal changes that match the re-designed user and device administration options that were implemented in the v2.8 dashboard.
2. Added support for Windows RT. [11188]
    a. At this time, a Windows RT device cannot be properly restricted through Compliance Manager due to an unrecognized device platform value that it returns to the ZENworks Mobile Management server.

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 that caused Mobile App permissions to work incorrectly when "Manage Mobile Apps" was disabled. [11382]
3. Other various dashboard and UI bug fixes.

Version 2.7.1

Description: Update
Date: 2013.04.03

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 ZENworks Mobile Management server.
    d. Added the option to be able to remove an app when a *Stop Managing Device* is performed.
2. iOS Corporate Resources
    a. Added the ability to set up Access Points.
    b. Added the ability to set up Web Clips.
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. Support for Safari web browser.
5. Re-designed user and device administration options in the dashboard.
    a. The “Clear Device Enrollment” option is now labeled “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.
6. Added the ability to pull ZENworks Mobile Management reports through Jaspersoft reporting software.

Bug Fixes

1. Fixed a php vulnerability in the desktop and mobile USAP pages. [806286, 806290]
2. Fixed a UI issue where the Android Wi-Fi description is cut off under the Compliance Manager global restrictions section. [807110]
3. Fixed an issue where a user was not being removed from the dashboard User Grid after a certain expiration date. [803350]
4. Other various dashboard and UI bug fixes.

Version 2.7.0

Description: Update
Date: 2013.02.05

Changes/New Features

1. New localizable installer with logging. [8889]
2. OpenID support.
3. Dashboard Updates
    a. User Profile redesign.
    b. Layout change to the Organization view.
    c. Addition of an Organization Licensing page under *System Administration*, so all organization licenses and their license types can be viewed in one location. [9589, 9663]
    d. Added Wi-Fi Networks under *Android Corporate Resources*.
    e. Users page redesigned to include an LDAP tree/hierarchy.
        - Added the ability to search users and devices in the hierarchy

4. 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] [765211]
    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]
5. Added the ability for larger file uploads, up to 100 MB, on the ZENworks 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] [784530]
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: 2012.12.03

Changes/New Features

1. Added support for iOS Profile Expiration (iOS 6+).
2. Added new Admin-configurable TouchDown Policies.
3. Added support for SMTP AUTH LOGIN authentication.
4. 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 ZENworks Mobile Management 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: 2012.07.30

Changes/New Features

1. Added a background thread on the ZENworks Mobile Management server that updates LDAP Custom Columns for users once every 24 hours.
2. Added a “Reload Updates” button in the Dashboard and Update Manager. [9183]

Bug Fixes

1. Fixed an issue that caused a selective wipe to fail for an iOS device because no secondary profiles were detected. [7950]
2. Fixed a few issues that prevented File Share permissions from saving correctly in the dashboard. [8441,8446, 9251, 9262]
3. Fixed an issue that prevented the Auto Join option from being sent to an iOS device after configuring a Wifi network and turning on the option for Auto Join. [8458]
4. Fixed an issue that caused logging data grids to take a long time to sort by column. [8717]
5. Fixed an issue occurring on iOS devices that caused an error to continually return when an app was already on the device and that same app was then forced to the device to be installed again. [9023]
6. Fixed an issue that prevented a file from uploading into the File Share because of bad date properties on the file. [9077]
7. Fixed an issue that prevented administrators from selecting the *Clear Passcode* option in the Dashboard for iOS devices without device statistics. [9105]
8. Other miscellaneous Dashboard bug fixes. [5896, 7993, 8545, 8631, 8863, 9055]

Version 2.5.4

Description: Initial Public Release
Date: 2012.07.16

Key Features

1. Options for adding users to the server:
    a. Manual
    b. .CSV Import
    c. LDAP Import
    d. Hands-Off
2. Monitoring of device last sync and location data, phone/SMS logs, and more under the user’s profile.
3. Management of policies on the device through policy suites.
4. Multiple devices per user support.
5. Activity Monitor
    a. 34 graphs to choose from.
    b. A translucent overlay screen can be opened to select a list of available graphs, preview the graphs, and choose the 6 graphs to be displayed.
    c. The 6 graphs displayed in the dashboard are remembered for the next dashboard login.
6. Compliance Manager
    a. You can manage access policies for user and/or device connectivity
    b. You can create specific device restrictions for accessing resources
    c. You can create user exceptions for connectivity and resource permissions
    d. You can watch connectivity of specific users
    e. You can manage alert settings
    f. You can add alert recipients for email and SMS alert notifications
    g. You can send e-mail to users when they have been restricted.

7. Database Task Scheduler
    a. An administrator with full system credentials can maintain database tables.
    b. A 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.
8. 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.
    b. You can request a device's log from the dashboard. When the device receives the request it will respond by sending the log, which can then be acted upon within the dashboard.
        i. Android
        ii. iOS
9. Role Based Administration
    a. You can set administrators to the default Full, Support or Restricted admin roles.
    b. You can create custom admin roles.
    c. You can restrict Organization Admin roles to privacy protect by user or policy suite.
10. Administrator Audit Trails
    a. Changes are tracked within the database.
    b. Changes to a Policy Suite are recorded.
    c. Security actions for the user are logged. Items covered in this are any of the mini-admin actions, like wipes and locking the device.
11. Data Reporting:
    a. Device reports
    b. User reports
    c. Compliance reports
    d. Administrative roles reports
    e. You can export reports in a .CSV or .XLS format.
    f. Additional report functionality includes the ability to rearrange columns, change the report sorting order, and collapse/expand parent groups.
12. Update Manager
    a. An integrated update management feature that will facilitate software updates to the *ZENworks Mobile Management* server. These features include the dashboard's *Update Management* section and the *Update Manager Application*, which is used on the physical *ZENworks Mobile Management* servers to apply updates.
13. Support for TouchDown policies and suppressions. Features include:
    a. Automatically initiate TouchDown enrollment after *ZENworks Mobile Management* enrollment.
    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).
14. 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 profiles in order to start using the APNs. They are not automatically prompted to perform this step. Additionally, when the new profile is loaded, they are prompted for an ActiveSync account password.

    When you use an APNs certificate, the device connection schedule should not be set to a short interval (such as 1 minute).

    Features include:
    a. The ability to view additional device statistics such as Available Device Capacity, IMEI/MEID, Phone Number, and many more. To view the stats, go to Smart Devices and Users, view a user's profile and choose 'iOS MDM Settings' > 'Device Information'.
    b. The ability to view a list of installed applications. To view the applications, go to 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. The 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. The ability to silently update/remove configuration profiles that are managed by the *ZENworks Mobile Management* server. The initial installation of the configuration profile still requires user interaction.
e. The ability to selectively wipe the mail, calendar, and contact data that is managed by the *ZENworks Mobile Management* server. This security action can be performed by the administrator in the dashboard or by the user in the USAP.
f. The ability to lock a device. This security action can be performed by the administrator in the dashboard or by the user in the USAP.
g. The ability to Clear Passcode. This security action can be performed by the administrator in the dashboard.