Server Release Notes

ZENworks® Mobile Management 2.9.x

May 2014

Novell®

Legal Notices

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

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

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

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

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

Novell Trademarks

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

Third-Party Materials

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

Table of Contents

ZENworks Mobile Management Server Release Notes 4

Revision History 5

Installation Information 6

Requirements 6
Installation Package 6

Known Issues 7

ZENworks Mobile Management Server 7
Android Devices 9
iOS Devices 9

Version History 11

Version 2.9.1 11
Changes/New Features 11
Bug Fixes 11
Version 2.9.0 12
Changes/New Features 12
Bug Fixes 12
Version 2.8.2 12
Changes/New Features 12
Version 2.8.1 13
Changes/New Features 13
Bug Fixes 13
Version 2.8.0 14
Changes/New Features 14
Bug Fixes 15
Version 2.7.8 15
Bug Fixes 15
Version 2.7.7 16
Changes/New Features 16
Bug Fixes 16
Version 2.7.6 16
Changes/New Features 16
Bug Fixes 17
Version 2.7.4 / 2.7.5 17
Changes/New Features 17
Bug Fixes 17
Version 2.7.3 18
Changes/New Features 18
Bug Fixes 18
Version 2.7.2 18
Changes/New Features 18
Bug Fixes 18
Version 2.7.1 19
Changes/New Features 19
Bug Fixes 19
Version 2.7.0 19
Changes/New Features 19
Bug Fixes 20
Version 2.6.1 20

Changes/New Features 20
Bug Fixes 20
Version 2.6.0 21
Changes/New Features 21
Bug Fixes 21
Version 2.5.5 22
Changes/New Features 22
Bug Fixes 22
Version 2.5.4 22
Key Features 22

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
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
- 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]

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]

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]

Version History

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.