Release Notes for ZENworks Mobile Management Server

ZENworks® Mobile Management 2.5.x

July 2012

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 5

Requirements 5
Installation Package 5

Known Issues 6

ZENworks Mobile Management Server 6
Android Devices 7
iOS Devices 8

Version History 9

Version 2.5.4 9
Key Features 9

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
2012.07.16	Anthony Costello	2.5.4 Release

Installation Information

Date: 07/16/2012
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	2.5.2
ntc_mdm_AdminRoles.dll	2.5.2
ntc_mdm_AirProxy.dll	2.5.2
ntc_mdm_AirSyncParser.dll	2.5.2
ntc_mdm_APN.dll	2.5.2
ntc_mdm_AutoEmailChecker.dll	2.5.2
ntc_mdm_BaseQueryOffloader.dll	2.5.2
ntc_mdm_CommandBase.dll	2.5.2
ntc_mdm_ConfigFileReader.dll	2.5.2
ntc_mdm_CriticalLogger.dll	2.5.2
ntc_mdm_DatabaseInterface.dll	2.5.2
ntc_mdm_DatabaseLogger.dll	2.5.2

ntc_mdm_DatabaseLoggerWrapper.dll	2.5.2
ntc_mdm_DatabaseTaskScheduler.dll	2.5.2
ntc_mdm_HTTPInterface.dll	2.5.2
ntc_mdm_IOSMDMParser.dll	2.5.2
ntc_mdm_IOSMDMSync.dll	2.5.2
ntc_mdm_ISAPIRedirectFilter.dll	2.5.2
ntc_mdm_Jobs.dll	2.5.2
ntc_mdm_Licensing.dll	2.5.2
ntc_mdm_MailComposer.dll	2.5.2
ntc_mdm_MDMParser.dll	2.5.2
ntc_mdm_MDMSocket.dll	2.5.2
ntc_mdm_MDMSync.dll	2.5.2
ntc_mdm_SMTP.dll	2.5.2
ntc_mdm_WBXMLParser.dll	2.5.2

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. 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]
25. 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]
26. 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.

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]

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. Saving changes to the liability, policy suite, organization name, signing certificate, APN certificate, and access rights requires a complete reload of the configuration profiles. [7649]
12. 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.

Version History

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.