

Android App Release Notes

ZENworks® Mobile Management 3.0.x

January 2015

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 \(http://www.novell.com/info/exports/\)](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.

Copyright © 2012-15 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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 \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](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 for Android Release Notes	4
Revision History	4
Installation Information	5
Requirements.....	5
Installation Package.....	5
Known Issues	5
TouchDown.....	6
Version History	8
Version 3.0.1.....	8
Changes/ New Features.....	8
Bug Fixes.....	8
Version 3.0.0.....	8
Changes/ New Features.....	8
Version 2.9.3.....	9
Bug Fixes.....	9
Version 2.9.2.....	9
Changes/ New Features.....	9
Version 2.9.1.....	9
Changes/ New Features.....	9
Bug Fixes.....	9
Version 2.9.0.0.....	10
Changes/ New Features.....	10
Version 2.8.1.0.....	10
Changes/ New Features.....	10
Bug Fixes.....	10
Version 2.8.0.2.....	10
Changes/ New Features.....	10
Version 2.7.7.1.....	11
Changes/ New Features.....	11
Version 2.7.6.2.....	11
Changes/ New Features.....	11
Version 2.7.4.3.....	11
Changes/ New Features.....	11
Bug Fixes.....	11
Version 2.7.2.4.....	12
Changes/ New Features.....	12
Bug Fixes.....	12
Version 2.7.1.5.....	12
Changes/ New Features.....	12
Version 2.7.0.3.....	12
Changes/ New Features.....	12
Version 2.6.1.1.....	13
Changes/ New Features.....	13
Version: 2.5.5.3.....	13
Changes/ New Features.....	13
Bug Fixes.....	13
Version: 2.5.3.0.....	14

ZENworks Mobile Management for Android Release Notes

The *Novell ZENworks Mobile Management* application for Android devices is a component of the *ZENworks Mobile Management* enterprise MDM platform. The *ZENworks Mobile Management* application communicates with the Novell Mobile Management server.

ZENworks Mobile Management was designed to enable Android users to keep up-to-date with company security policies and management features, and to ensure the confidentiality and integrity of wirelessly transmitted corporate information.

ZENworks Mobile Management also enables you to access your company's recommended applications and utilize the self-servicing dashboard to locate a misplaced device or issue a lock/wipe command to a potentially compromised device.

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
2014.12.05	Anthony Costello	3.0.1 Update
2014.08.01	Anthony Costello	3.0.0 Update
2014.07.08	Anthony Costello	2.9.3 Update
2014.06.16	Anthony Costello	2.9.2 Update
2014.05.07	Anthony Costello	2.9.1 Update
2013.12.09	Anthony Costello	2.9.0.0 Update
2013.11.04	Anthony Costello	2.8.1.0 Update
2013.09.09	Anthony Costello	2.8.0.2 Update
2013.07.22	Anthony Costello	2.7.7.1 Update
2013.07.08	Anthony Costello	2.7.6.2 Update
2013.05.28	Anthony Costello	2.7.4.3 Update
2013.04.12	Anthony Costello	2.7.2.4 Update

2013.04.03	Anthony Costello	2.7.1.5 Update
2013.02.05	Anthony Costello	2.7.0.3 Update
2012.12.03	Anthony Costello	2.6.1.1 Update
2012.08.13	Anthony Costello	2.5.5.3 Update
2012.07.16	Anthony Costello	2.5.3.0 Release

Installation Information

Date: 05/28/2013

Product: *ZENworks Mobile Management* for Android Devices

Requirements

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

- Android OS version 2.2, 2.2.1, 2.3, 3.x, or 4.x for devices operating with native ActiveSync protocol
- Android OS versions 2.0/2.1, 2.2, 2.2.1, 2.3, 3.x, or 4.x for devices operating with the TouchDown app
 - TouchDown version 7.3.x

Installation Package

The *ZENworks Mobile Management* app is available on the Google Play Store.

Known Issues

1. The **Last Sync Data** section of the *ZENworks Mobile Management User Profile* might not display statistics for Android devices as expected. The following list explains how device functionality affects the information displayed for these statistics:
 - a. **Device IMEI**
Only global networks (GSM) give the devices an IMEI (International Mobile Equipment Identity). CDMA networks do not. Therefore, this statistic is blank for devices not using GSM networks.
 - b. **Battery Level**
Some devices might display an incorrect battery level. For example, the battery might be fully

charged, but display only 90%. This is a known issue with some Android devices and might indicate that the battery needs to be recalibrated. The recalibration process involves completely draining the battery until it shuts off, turning the device on again and letting it power off, and then completely charging it while powered off.

c. **Signal Strength**

Android devices running OS versions 1.5 or 1.6 might not report valid signal strength. Therefore, this statistic might display a zero (0).

d. **Device Encrypted**

If Require Device Encryption is enabled, Android devices running the TouchDown app encrypt only the TouchDown data. Because not all data is encrypted, this statistic displays No for Android devices using TouchDown.

2. In the *ZENworks Mobile Management User Profile*, the Status of a call and the Roaming status of a device displays as Unknown on an Android device phone log. This is a limitation of the device platform, because these statistics are not reported.
3. For Samsung Galaxy series devices, the storage card memory might display as double if the external storage card is unmounted. This is also true of the Galaxy Tab.
4. Even when *Minimum Password Length* is set to less than 4 on the server, the Galaxy S 4G device requires at least 4 characters. The device displays a message saying that the "PIN must contain at least 4 numbers."
5. Some Android devices ignore the inactivity timeout value passed to it from the policy suite rules set on the *ZENworks Mobile Management* server. Known devices with this limitation are HTC OS 2.2 (or greater) devices.
 - a. The inactivity timeout requirement can be enforced from the server and the timeout value is a maximum, which normally functions to allow the user to set the timeout on the device to a value up to and including the maximum. However on these devices, the maximum value sent from the server is ignored.
6. If native ActiveSync mail is being used, the enforcement of Allow Camera and Password Expiration might cause conflicts. Changes to these policies might not be implemented on the device as expected, because the device settings take precedence over changes to these policies from the *ZENworks Mobile Management* server. When using TouchDown, however, the policies are enforced as expected. [7366 / 7518]
7. The following issue has been observed on several Android devices. When a *Lock Device* command is sent to the device, the device powers off as expected. When the device is powered on again, the user is not prompted for the unlock password unless the *Inactivity Timeout* period has lapsed. This has been observed on HTC Droid Incredible, Status, and Thunderbolt; LG Spectrum; Samsung Galaxy S II Skyrocket; and Pantech Breakout. [3159]

TouchDown

These known issues apply only when you are using the TouchDown application.

1. Hands-off enrollment should not be used for Android devices with TouchDown. When you are using hands-off enrollment, initiating TouchDown enrollment through the *ZENworks Mobile Management* app does not work properly. [5636]
2. Changing the server name within the TouchDown application can cause decryption processes to fail. If there are server changes, you should re-enroll the *ZENworks Mobile Management* and TouchDown applications. [4896]
3. If a user happens to be in the TouchDown Settings when policies changes are synchronizing to the device, the TouchDown application might stop or display an error message. However, when TouchDown is re-opened, it is evident that the policies have been successfully synchronized. [4967]
4. TouchDown policies do not take effect on the device until the setting that was changed is refreshed. In other words, if you are viewing the setting when it is being updated, you must exit from the TouchDown option and then re-enter it before the update displays. [5007]
5. The functionality of *Show calendar info on notification bar*, *Show email info on notification bar*, and *Show task info on notification bar* policies is dependent upon several other policies. To successfully

display notifications, the following TouchDown settings must be configured on the device: In the Advanced TouchDown Settings, enable the *Notify on new mail* and the *Appointment reminders at non-peak times* options; configure *Email Alerts* and *Appointment Alerts* to “use system settings.” [5054]

6. The *Allow speak notification* option policy acts like a suppression policy when disabled, because it suppresses the setting on the device. However, it also turns off the speak notification functionality on the device. A suppression policy does not usually change the configuration on the device. If the Allow speak notification option policy is then enabled, the functionality on the device remains off and the user must turn it on in the TouchDown advanced settings. [4940]
7. On the Droid Pro, the Lock Device command fails. Neither the device or TouchDown is locked and the user does not receive a confirmation email. This is an issue with this particular device model. [5034]
8. If a *Maximum Inactivity Timeout* is set, the user still has the ability to select *Never Timeout* on the device. This is a function of the operating system that, at this time, cannot be controlled. [5097]

Version History

Version 3.0.1

Description: Update

Date: 2014.12.05

Changes/ New Features

1. Added additional support for KNOX EMM.
 - a. Added additional Password and Restriction policies.
 - b. Added Roaming policies.
 - c. Added Developer Mode policies.
 - d. Added the ability to reboot or power off the device.
 - e. Added the ability to unblock password entry on the device.
 - f. Added support for blacklisting and whitelisting apps.
2. Added support for KNOX Workspace.
 - a. Added Restriction and Password policies for the container
 - b. Added the ability to install Enterprise apps inside the container.
 - c. Added support for blacklisting and whitelisting apps.
3. Added the ability to display an Acceptable Use Policy. When enabled on the ZMM server, users must accept the policy before they can enroll.
4. Removed the prompt to manually enroll ActiveSync when ZMM is configured via Samsung KNOX.

Bug Fixes

1. Fixed an app crash when trying to send the Device Name back to the server.
2. Fixed an issue that sometimes prevented Enterprise APKs from downloading and installing successfully.
3. Other performance and functionality improvements.

Version 3.0.0

Description: Update

Date: 2014.08.01

Changes/ New Features

1. Added the ability to have the ZMM app enroll via SAML authentication.
2. Added additional support for KNOX EMM.
 - a. Added Alternative Home Screen policies.
 - b. Added additional Password and Restriction policies.
 - c. Added Location and Browser policies.
3. Added support for KNOX Workspace.
 - a. Added the ability to create and remove 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.
4. Added the ability to detect and report the Android OS build number.

Version 2.9.3

Description: Update
Date: 2014.07.08

Bug Fixes

1. Fixed an issue with SD card encryption enforcement.
2. Fixed a KNOX EMM configured native ActiveSync account problem that caused a high amount of ActiveSync traffic to be sent to the server.

Version 2.9.2

Description: Update
Date: 2014.06.16

Changes/ New Features

1. Added support for Samsung KNOX EMM which includes the following:
 - a. Collection of new device statistics including Device Name and Bluetooth MAC Address.
 - b. Auto provisioning of Samsung email client on SAFE and KNOX EMM devices.
 - c. Use of SAFE APIs to apply password policy on Samsung SAFE and KNOX EMM devices.

Version 2.9.1

Description: Update
Date: 2014.05.07

Changes/ New Features

1. Added an option to selectively wipe the device when the user unenrolls the *ZENworks Mobile Management* account.
2. Added localization options for French, German, Italian, Brazilian Portuguese, Spanish, Swedish, Simplified Chinese, Traditional Chinese, and Japanese.
3. Added support for ActiveSync synchronization policies for TouchDown: *Specific calendar age for synchronization* and *Specific email age for synchronization*.
4. Added support for KNOX Standard (Samsung SAFE) devices.

Bug Fixes

1. Fixed an issue that prevented launching the correct app in the Google Play store when multiple apps are being force pushed to the device.
2. Fixed an issue with the "Require TouchDown PIN" option.
3. Fixed an issue that if the password changes on the GO!Enterprise server and the device is in direct push, the password prompt on the device would refresh every five seconds preventing the end user from changing their password on the device.

Version 2.9.0.0

Description: Update
Date: 2013.12.09

Changes/ New Features

1. Added support for Novell Filr.

Version 2.8.1.0

Description: Update
Date: 2013.11.04

Changes/ New Features

5. Added support for Google Cloud Messaging (GCM).
6. When an authentication failure is detected, the app will prompt for a new password to be entered. [DE102]

Bug Fixes

1. Fixed an issue which caused the app to crash because of a security exception not being handled properly. [11891]

Version 2.8.0.2

Description: Update
Date: 2013.9.09

Changes/ New Features

1. Changed the "Mobile Apps" label to "Managed Apps."
2. Changes were made to accept time-based policies on the device, based on device time zone.
3. Added a way for the device to report if administrator permissions were removed from the ZENworks Mobile Management app.
4. Fixed an issue where the size of the *ZENworks Mobile Management* app continued to increase with every sync cycle when an app that the server cannot recognize has already been installed by the user is force pushed to the device. [11217]
5. Added a prompt to enter the ActiveSync password when enrolling TouchDown from the *ZENworks Mobile Management* device app.

Version 2.7.7.1

Description: Update
Date: 2013.07.22

Changes/ New Features

1. Added additional device unlock settings that block pattern unlock.
 - Allow Biometric weak – Supported in Android OS 4.0 and up.
 - Complex Password – Supported in Android OS 3.0 and up
 - If complex is set on a policy for a device that doesn't support it, the next level of security down will be implemented, which is alphanumeric.
 - Alphabetic Password – Supported in Android OS 2.2 and up.
 - Numeric Password – Supported in Android OS 2.2 and up.

Version 2.7.6.2

Description: Update
Date: 2013.07.08

Changes/ New Features

1. Added support for various VPNs that can be set up as a corporate resource on the *ZENworks Mobile Management* server.
2. Added support for a TouchDown volume license key to be pushed down from the server to devices which use the TouchDown application.

Version 2.7.4.3

Description: Update
Date: 2013.05.28

Changes/ New Features

1. Added the ability to view on the device, criteria set by the administrator that restrict blacklisted apps.
2. Added the ability to download multiple files from File Share simultaneously. [5494]
3. Added the ability to see the criteria of a Whitelist, set by the administrator, on the device.

Bug Fixes

2. Fixed an issue in which an interrupted download caused the message, "Downloading File" to continuously display. [5497]
3. Fixed an issue that caused file transfers to stall when commands were forced to the device. [11342]

Version 2.7.2.4

Description: Update
Date: 2013.04.12

Changes/ New Features

1. Added functionality that reinforces password requirements on the device when they are enabled in the user's policy suite. If the initial prompt to set up an unlock password is dismissed, the device prompts again two minutes later. If the second prompt is dismissed without creating a password, the device will ask again after 60 minutes. If that password prompt is dismissed, the device will repeat the request for a password every 5 seconds thereafter, until a password has been created.
2. Added device encryption prompts to the Mobile Apps and File Share device options. If the policy suite assigned to the user requires device encryption, but the device does not have it enabled, a pop up appears stating that you must enable encryption on the device before you can access the mobile apps or file share list.

Bug Fixes

1. Fixed an issue where mobile apps that were downloaded through the ZENworks Mobile Management app were not getting removed when a "Stop Managing Device" command was sent to the device. [11344]

Version 2.7.1.5

Description: Update
Date: 2013.04.03

Changes/ New Features

1. Added support for the new user and device administrator options (Suspend Device and Stop Managing Device) added to the 2.7.1 ZENworks Mobile Management server.
2. Added support for Basic Android App Management that is included in the 2.7.1 ZENworks Mobile Management server.

Version 2.7.0.3

Description: Update
Date: 2013.02.05

Changes/ New Features

1. Added support for syncing a Wifi configuration from the ZENworks Mobile Management server. [7477]
2. Removed the prompt for the existing ActiveSync password update option so as not to give the false impression that the password can be updated on the device and reflected back to the server. [9682]

Version 2.6.1.1

Description: Update
Date: 2012.12.03

Changes/ New Features

1. Added support for the GetNetworkSettings command from the ZENworks Mobile Management server.
2. Added support for additional TouchDown policies and settings.

TouchDown for Android v7.3.00052 introduces several new device settings. Depending on how the administrator has configured these new settings on the server side, a user of this TouchDown version who upgrades to ZENworks Mobile Management for Android, v2.6.1.1 might experience changes in device behavior. If administrative policies do not allow access, a user might even notice that some settings are no longer available on the device.

Version: 2.5.5.3

Description: Update
Date: 2012.08.13

Changes/ New Features

1. Tabs have been added to the app for easier access to File Share and Mobile Apps. [8383]
2. Added support for TouchDown's password configuration. [7692]

Bug Fixes

1. Fixed an issue that caused activity to be logged regardless of whether logging was enabled or disabled in the log settings. [5024]
2. Fixed a display issue with the 'Refresh' icon while in direct push. [8691]
3. Addressed various bugs pertaining to TouchDown.
 - a. Fixed an issue where the ZENworks Mobile Management app registered TouchDown, but the Dashboard did not indicate as such and suppressions were not enforced. [6044, 7843]
 - b. Clarified the text in the ZENworks Mobile Management enrollment success prompt that appears when TouchDown is detected. The text now instructs the user to configure the ActiveSync account through TouchDown. [9226]
 - c. Fixed an issue in which changing the password in the ZENworks Mobile Management app caused a prompt to appear for mirroring the password in TouchDown, even though TouchDown was not installed. [9245]

Version: 2.5.3.0

Description: Initial Public Release

Date: 2012.07.16

Key Features

1. Management of policies on the device.
2. Reporting of device statistics to the *ZENworks Mobile Management* server.
3. Rooted device detection.
4. Use of the TouchDown API for enrollment of the TouchDown account and control of policies and suppressions.
5. Handling for the device log request that can be issued by the administrator in the *ZENworks Mobile Management* dashboard.
6. Support for Mobile Apps from the *ZENworks Mobile Management* server.
7. Support for File Share from the *ZENworks Mobile Management* server.