Functionality by Device Platform

ZENworks® Mobile Management 2.5.x

September 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

The information in these tables describes functionality supported by each device platform for *ZENworks Mobile Management*, version 2.5.x.

Device platforms supported by *ZENworks Mobile Management* are Android, BlackBerry with *NotifySync*, iOS 4 or 5, Symbian S60 3rd edition, webOS, Windows Mobile 6, and Windows Phone 7. Supported device operating system versions are listed below.

Anrd	TD/A	NS/BB	iOS	S60	wOS	WM	WP7
Android devices OS v2.2 – 4.0	Android devices OS v2.0 - 4.0 with TouchDown v7.3.x	BlackBerry devices OS v4.5 – 7.1 with NotifySync v4.9 or greater	iOS 4 - 6 devices with multitasking capabilities	Symbian S60 3rd edition devices OS v 9.1	WebOS devices OS v1.4.3/1.4.5, 2.0.0/2.0.1, 2.1.2	Windows Mobile devices OS v6.1/6.5	Windows Phone devices OS v7 or 7.5

The ZENworks Mobile Management Device Application

Android, iOS, Symbian S60 3rd Edition, and Window Mobile devices use the *ZENworks Mobile Management* device application to provide additional functionality and enforce policies that are not handled by ActiveSync. The *NotifySync for BlackBerry* application, which interfaces with *ZENworks Mobile Management,* has an MDM component that enforces ActiveSync policies and provides additional functionality for BlackBerry devices. (Requires an additional *NotifySync* license.)

The device platforms listed above also require a native ActiveSync protocol or an application that uses the ActiveSync protocol, such as *NotifySync for BlackBerry* or *TouchDown for Android*.

- On Android OS 2.2 or greater devices, the ActiveSync protocol native to the device is sufficient; although the TouchDown application offers greater functionality. See Policy Rules: TouchDown
  For devices running OS versions 2.0 or 2.1, the *TouchDown* application (available from the Play Store) is required to handle the ActiveSync policies. On OS 2.0/2.1 devices, ActiveSync policies affect only the TouchDown account and data.
- On BlackBerry devices, *NotifySync for BlackBerry* v4.9.x or greater is the ActiveSync application required to handle the ActiveSync policies. The application has an MDM component that interfaces with *ZENworks Mobile Management* and provides additional functionality. (Requires an additional *NotifySync* license.)
- On iOS 4 - 6 devices with multitasking capabilities, the ActiveSync policies are enforced by using Apple configuration profiles.
- On Symbian S60 3rd Edition devices, *Mail for Exchange* is required to handle the ActiveSync policies.
- On Windows Mobile 6.1/6.5 devices, the ActiveSync protocol native to the device is sufficient.

Enrolling Android, iOS, Symbian, or Windows Mobile 6 devices without the *ZENworks Mobile Management* app is not recommended, because only ActiveSync policies supported by the device platform or model can be enforced. BlackBerry devices do not have native ActiveSync capabilities and are not supported without the *NotifySync* app.

ActiveSync Only Devices

webOS and Windows Phone 7 platforms, for which there are no *ZENworks Mobile Management* applications, are also supported. Because these devices utilize the native ActiveSync protocol alone, only ActiveSync policies supported by the device platform or model can be enforced.

Policy Rules: All Devices

ZENworks Mobile Management is a trademark of Novell, Inc. The abbreviation “ZMM” is not a Novell trademark, but is used in these tables because of space constraints.

● A red dot indicates **ActiveSync only -** Currently, there is no *ZENworks Mobile Management* app available for WP7 or wOS. Devices support the feature via the native ActiveSync app on the device. BlackBerry devices have no native ActiveSync app and are only supported with the NotifySync app

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
Application Control													
Allow unsigned applications	(ActiveSync) Determines whether the device allows the execution of unsigned applications that already exist on the device.										●	●	
Allow unsigned installation packages	(ActiveSync) Determines whether the device allows unsigned cabinet files (installers) to run, (that is, whether an unsigned application can be installed by using a cab file).										●	●	
Number of Whitelisted Applications	(ActiveSync) Applications expressly allowed to operate on a device. This can be used to make an exception for the unsigned applications policy or to make an exception to the blacklist for a specific build of an application. Requires ActiveSync protocol 12.1										●	●	

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
Number of Blacklisted Applications	(ActiveSync) Applications expressly blocked from operating on a device. This only applies to applications that are factory-installed on the device. Requires ActiveSync protocol 12.1										•	•	
Audit Tracking													
Archive Files on Device	Requires the device to periodically send a list of all folders and files stored on the device and the SD card to the server. Displayed on the server in the User Profile: *File Archive* *Symbian devices: S*ends most files, with the exception of those in the device's *X:\private* and *X:\sys* folders, which normally contain system files or sensitive application data. The administrator defines the frequency of the file archiving.	•		•	•			•					
Record Phone Log	Requires the device to send all telephone log information to the server. For BlackBerry devices with *NotifySync*, tracks only calls made after *ZENworks Mobile Management* enrollment.	•		•	•			•					
Record Text/Multimedia Message Log	Requires the device to send all Short Message Service (SMS) and Multimedia Messaging Service (MMS) information to server. *BlackBerry devices* with *NotifySync:* • Do not track MMS messages • Track only texts made after *ZENworks Mobile*	•		•	•			•					

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	Management enrollment • Some devices use only MMS, so text messaging is not tracked *Android devices:* Text and MMS logging functionality might vary based on the device manufacturer or carrier. (See the *SMS & MMS Capabilities* document.) *Symbian S60 3 and Windows Mobile devices:* Records only SMS messages.												
Record Location of Device (Latitude / Longitude)	Uses GPS or triangulation on the device to locate where a user's device is at all times. Information is displayed using Google Maps. The device reports longitude and latitude as two separate values.	•		•	•	•		•					
GPS Location Accuracy	Allows administrators to specify a level of location accuracy. Accuracy primarily depends on using a cell tower vs. GPS (satellite) location methods; additional factors may be involved depending on the device type. Because improved accuracy generally results in increased battery usage, the level can be adjusted to facilitate a more efficient use of a device battery. Set levels via the policy suite.	•		•	•	•							
Device Controls: Device Features													
Allow Bluetooth	(ActiveSync) Determines whether										•	•	

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	Bluetooth is allowed to operate on the device. There are three settings: 1. Don't allow Bluetooth 2. Allow only Bluetooth headsets 3. Allow all Bluetooth												
Allow Browser	(ActiveSync) Determines whether the use of the native Web browser is allowed on the device. This setting might also prevent the use of third-party browsers that use the native browser as a basis for operation.					●	●				●	●	
Allow Camera	(ActiveSync) Determines whether the use of the device camera is allowed. Disabling the camera might limit the functionality of third-party apps that use the camera such as: Photoshop. *For Android:* supported on devices with OS 4.0 and *ZENworks Mobile Management* device application.	●	●	●		●	●				●	●	
Allow Infrared	(ActiveSync) Determines whether infrared connections are allowed to and from the device.										●	●	
Allow Internet Sharing from the Device (Tethering)	(ActiveSync) Determines whether the device can be used as a modem for a desktop or a portable computer.										●	●	

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
Allow Remote Desktop	(ActiveSync) Determines whether a remote desktop connection can be created from the device.										●	●	
Allow SD Card	(ActiveSync) Determines whether using an SD Card is allowed on the device. *For Android w/ TouchDown*: Allows or disallows SD card access for the TouchDown application only.			●							●	●	
Allow Synchronization from a Desktop	(ActiveSync) Determines whether the device can synchronize with a computer through a cable, Bluetooth, or IrDA connection.										●	●	
Allow Text Messaging	(ActiveSync) Determines whether the device can send or receive text messages.										●	●	
Allow Wi-Fi	(ActiveSync) Determines whether wireless Internet access is allowed on the device.										●	●	
Device Controls: Email													
Allow HTML formatted Email	(ActiveSync) Determines whether email synchronized to the device can be in HTML format. *Not supported with systems operating with ActiveSync protocol 2.5, such as Exchange 2003.*			●	●						●	●	
Maximum HTML email body	(ActiveSync) Defines the maximum				●						●	●	

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
truncation size (in KB)	HTML email body size of messages received on the device. Not supported with systems operating with ActiveSync protocol 2.5, such as Exchange 2003.												
Allow Consumer Email	(ActiveSync) Determines whether the user can use Windows Live services, such as Hotmail, Office, or Spaces.										●	●	
Allow POP/IMAP Email	(ActiveSync) Determines whether the device can access POP3 or IMAP4 email.										●	●	
Maximum email body truncation size (in KB)	(ActiveSync) Defines the maximum email body size of plain text messages received on the device.			●	●						●	●	
Device Control: ActiveSync Synchronization													
Maximum calendar age for synchronization	(ActiveSync) Defines the maximum look-back age of calendar events. Events older than the maximum age are automatically removed from the device. Not supported with systems operating with ActiveSync protocol 2.5, such as Exchange 2003.			●	●						●	●	●
Maximum email age for synchronization	(ActiveSync) Defines the maximum age of email on the device. Email older than the maximum age is automatically removed from the			●	●	●	●				●	●	●

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	device. Not supported with systems operating with ActiveSync protocol 2.5, such as Exchange 2003.												
Require manual sync when roaming	(ActiveSync) Enforces the use of manual synchronization on the device while roaming to avoid the higher data costs that are often incurred with automatic synchronization.			•	•	•	•				•	•	
Device Control: Multiple Devices													
Allow Multiple Devices	Determines whether users can enroll multiple devices against a single user account.	•	•	•	•	•	•	•	•	•	•	•	•
File and Application Management													
File Share	Creates a directory of folders and files to make accessible to users. Users access files directly through the *ZENworks Mobile Management* app. Sets permissions for access per policy suite.	•		•	•	•		•			•		
Mobile Apps	Creates a list of recommended apps. The list might consist of apps that users access directly through *ZENworks Mobile Management* or through links to the apps in device application stores. Available mobile applications are determined by	•		•	•	•		•			•		

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	device type. Sets permissions for access per policy suite.												
Security: Password													
Require Password	(ActiveSync) Forces the device to require a lock password.	●	●	●	●	●	●	●	●	●	●	●	●
Enable password recovery	(ActiveSync) This allows or disallows a user to use the device to issue a request for a temporary recovery password if they have forgotten their unlock password. The recovery password can be retrieved from the MDM *User Self Administration Portal* or the administrative dashboard. Requires ActiveSync protocol 12.0 or 12.1 *For Android w/TouchDown*, gives temporary unlock password only for the TouchDown application; does not provide temporary unlock password when the lock is imposed by the device's native OS.			●	●								
Allow Simple Password	(ActiveSync) Determines whether or not a password can consist of only repeating or sequential characters, such as "1111" or "abcd". *Not supported with systems operating with ActiveSync protocol 2.5, such*	●	●	●	●	●	●	●	●		●	●	●

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	as Exchange 2003.												
Require Minimum Password Length	(ActiveSync) Forces the device to require a password with a specified minimum length.	●	●	●	●	●	●	●	●	●	●	●	●
Minimum Password Length	(ActiveSync) Defines the minimum password length.	●	●	●	●	●	●	●	●	●	●	●	●
Require Alphanumeric Password	(ActiveSync) Forces the device to require a device password to contain both letters and numbers.	●	●	●	●	●	●	●	●	●	●	●	
Minimum Number of Complex Characters	(ActiveSync) Forces the device to require a minimum number of complex characters (symbols) in the password. If an alphanumeric password is not required, this is not enforced. *For Android (native):* Supported on devices with OS 3.0 and selected OS 2.x devices. *For BlackBerry w/ NotifySync:* Minimum number of each type of character required in an alphanumeric password. (Example: If minimum is 2, password must have 2 uppercase, 2 lowercase, 2 numeric, and 2 symbol characters.)	●	●	●	●	●	●				●	●	
Require Device Password Expiration	(ActiveSync) Forces the device to require users to update their passwords after a number of days. Not supported with systems	●	●	●	●	●	●				●	●	●

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	operating with ActiveSync protocol 2.5, such as Exchange 2003. *For Android:* Supported on devices with *ZENworks Mobile Management* device application and OS 3.0 (and selected devices with OS 2.x).												
Password expiration in days	(ActiveSync) Defines the number of days a password can be used before it expires. *For Android:* Supported on devices with *ZENworks Mobile Management* device application and OS 3.0 (and selected devices with OS 2.x).	●	●	●	●	●	●				●	●	●
Require Device Password History	(ActiveSync) Forces the device to disallow passwords that have been used in the recent past to be re-used. The number of stored past passwords is configurable. Not supported with systems operating with ActiveSync protocol 2.5, such as Exchange 2003. *For Android (native):* Supported on devices with OS 3.0 and selected OS 2.x devices. *For Android w/ TouchDown:* Applies to the password associated with the TouchDown application only.	●	●	●	●	●	●				●	●	●
Number of passwords stored	(ActiveSync) Defines the number of device passwords stored to prevent				●	●	●				●	●	●

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	users from reusing them too soon.												
Enable Password Echo	After the specified number of password entry attempts are made, the last password entered is unmasked to allow the user to see the error they are making.				•								
Begin password echo after attempts	Defines the number of unlock attempts before echoing begins.				•								
Security: Encryption													
Require Device Encryption	(ActiveSync) Determines whether the device encrypts stored data. Not supported with systems operating with ActiveSync protocol 2.5, such as Exchange 2003. iOS devices (3GS and 4) have hardware encryption that is always enabled. The ActiveSync policy is not used to enable/disable. *For Android w/ native ActiveSync account,* supported on the Motorola Droid Pro (OS 2.2) and devices with OS 3.0.0 or greater. For *Android w/ TouchDown*, only TouchDown data is encrypted (email, calendar, contacts, tasks). With *NotifySync for BlackBerry,* only	•	•	•	•	•	•				•	•	

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	NotifySync data is encrypted (email).												
Require Encryption on the Storage Card	(ActiveSync) Forces the device to encrypt the file system of a storage card. For *Android w/ TouchDown*, only TouchDown files are encrypted (email attachments that have been downloaded are encrypted by using AES (256); attachments are still unreadable if the card is moved to another device).			•							•	•	
Security: Duress													
Enable Duress Notification	A notification is sent to the specified email address if the user is forced to unlock the device under duress.				•								
Duress Notification Email	Defines the email address to which the duress notification is sent.				•								
Security: Device Inactivity and Locking													
Require Max Inactivity Time Device Lock	(ActiveSync) Forces the device to lock after a set number of minutes of user inactivity. This value serves as a maximum. This is also known as “Time without user input before password must be	•	•	•	•	•	•	•	•	•	•	•	•

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	re-entered."												
Max Inactivity Timeout (in minutes)	(ActiveSync) Defines the numbers of minutes of inactivity before the device locks. If the Challenge Timeout is being enforced, the Max Inactivity Timeout should be less than the Challenge Timeout.	•	•	•	•	•	•	•	•	•	•	•	•
Require Device Challenge Timeout	Forces the device to enable a challenge timeout. A lock is initiated regardless of activity and is intended to challenge the use of a lost or stolen device.				•								
Max Device Challenge Timeout	Defines the number of minutes before the device initiates a challenge lock. This lock is initiated regardless of activity and is intended to challenge the use of a lost or stolen device. If the Max Inactivity Timeout is being enforced, the Challenge Timeout should be greater than the Max Inactivity Timeout.				•								
Customizable Lock Message	Enable the lock message and enter the text to be displayed when device is locked.				•								
Audible Alert On Lock	This setting enables a device to constantly emit a loud noise when a server-initiated device lock has been issued. The intent is to draw				•						•		

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	attention to the missing device and the device thief. The noise continues while the device is powered on, until the device is unlocked.												
Maximum grace period (in minutes)	Determines how soon the device can be unlocked again after use, without re-prompting for the password. The administrator can also disallow a grace period by selecting *Immediately* or choose not to impose a limit by selecting *None*.					•							
Wipe device on Failed Unlock Attempts	(ActiveSync) After the specified number of password entry attempts are made, data is cleared from the device. Functionality varies by device. *Android or Android w/TouchDown (requires OS v2.2 or greater)*: The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Does not erase the SD card. *Android w/TouchDown (using OS v2.1 or older)*: Wipes only *ZENworks Mobile Management* information. *BlackBerry:* Removes all mail and PIM data associated with the *NotifySync* application and removes the *NotifySync* account. Locks the device if Require Password is enabled. Erases *NotifySync* data from the SD card, including saved	•	•	•	•	•	•	•	•	•	•	•	•

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	attachments. *iOS:* The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. *Symbian*: The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state in was in when purchased. Erases the SD card. *WM*: The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Erases SD card only on *Professional* devices. *webOS and WP7:* The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state in was in when purchased.												
Maximum number of unlock attempts	(ActiveSync) Defines the number of unlock attempts before the device-initiated wipe is performed.	•	•	•	•	•	•	•	•	•	•	•	•
Security: Emergency Calls													
Enable emergency calls when locked	Allows the device to make emergency calls in a locked state. Allows emergency numbers to be specified for allowed calls on a				•								

Policy Suite Rules: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	locked device: ambulance, fire, police, and one other emergency number.												
S/MIME Settings													
Require signed SMIME messages	This setting forces the device to send digitally signed S/MIME messages.										●	●	●
Require encrypted SMIME messages	This setting forces the device to send encrypted S/MIME messages.										●	●	●
Require signed SMIME algorithm	This setting specifies the algorithm to be used for signing messages. Options are SHA1, MD5.										●	●	●
Require encryption SMIME algorithm	This setting specifies the algorithm to be used for encrypting messages. Options are TripleDES, DES, RC2128bit, RC264bit, RC240bit.										●	●	●
Allow SMIME Encryption algorithm negotiation	This setting enables/disables the device from negotiating the encryption algorithm used for signing messages. Options are Do not negotiate, Negotiate only strong algorithms, Negotiate any algorithm.										●	●	●
Allow SMIME soft certs	This setting enables/disables the device from using soft certificates to sign outgoing messages.										●	●	●

Security: All Devices

Security: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
Security Commands													
Disable/Enable Device	Disables or enables device connection with the *ZENworks Mobile Management* server.	•	•	•	•	•	•	•	•	•	•	•	•
Selective Wipe	Administrators or end users can issue a selective wipe command. Functionality varies by device. *Android w/ native ActiveSync account (requires OS v2.2 or greater)*: Removes the *ZENworks Mobile Management* account information. *Android w/TouchDown (using any supported OS)*: Removes all mail and PIM (calendar, contact, tasks) data associated with the *TouchDown* application and returns *TouchDown* to a pre-registration state. Erases *TouchDown* data from the SD card. Removes the *ZENworks Mobile Management* account information. When the *Clean SD*	• •		•	•	•		•					

Security: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	card on Remote Wipe option in the TouchDown *Advanced Settings* is enabled, the SD card is completely erased. *BlackBerry:* Removes all mail and PIM data associated with the *NotifySync* application. Locks the device if *Require Password* is enabled. *iOS:* Removes all mail and PIM (calendar and contacts) data controlled by *ZENworks Mobile Management*. The command is applied immediately; however, the device is capable of postponing the action. *Symbian:* Removes the *ZENworks Mobile Management* account information.												
Wipe Storage Card	Administrators or end users can remotely wipe all data from the device's storage card.	•		•	•						•		
Full Wipe	Administrators or end users can issue a full wipe command. Functionality varies by device. *Android w/ native ActiveSync account (requires OS v2.2 or greater)*: The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Does not erase the SD card. *Android w/TouchDown (requires*	•	•	•	•	•	•	•	•	•	•	•	•

Security: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	OS v2.2 or greater): Device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Does not erase SD card. Note: When the *Clean SD card on Remote Wipe* option in the TouchDown *Advanced Settings* is enabled, the SD card is completely erased. *Android w/TouchDown using OS v2.0 or 2.1: Full Wipe* is not available – use the *Selective Wipe* option. *BlackBerry:* Removes all mail and PIM data associated with the *NotifySync* application and removes the *NotifySync* account. Locks the device if *Require Password* is enabled. Erases the entire SD card, including saved attachments. *iOS:* The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. *Symbian*: The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Some models (N95 and 6120c) wipe only *Mail for Exchange* data. Erases the SD card.												

Security: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	WM: The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Erases the SD card only on *Professional* devices. *webOS and WP7:* The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased.												
Lock Device	Administrators or end users can remotely lock the device, requiring an unlock password to be entered before the device can be used. *Android or Android w/TouchDown:* requires OS v2.2 or greater.	•		•	•	•					•		
Clear Passcode	The passcode is cleared. If a passcode is required by the user's policy, the user will be prompted to enter a new passcode.					•							
Network Connection Security and Configuration													
SCEP (Simple Certification Enrollment Protocol	Sets up SCEP settings for devices.					•							
VPN (Virtual Private Network)	Sets up VPNs for devices. Current Functionality: IPSec (Cisco protocol)					•							

Security: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
Wi-Fi	Sets up Wi-Fi settings, using various levels of security including WEP, WPA, and WPA2.					•							

Device Statistics: All Devices

Device Statistics: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
ZENworks Sync	The date and time of the last successful synchronization with the *ZENworks Mobile Management* server.	•		•	•	•		•			•		
ActiveSync Sync	The date and time of the last successful synchronization with the ActiveSync server.	•	•	•	•	•	•	•	•	•	•	•	•
iOS APN Sync	The date and time of the last successful synchronization with the Apple Push Notification server.					•							
Last Boot Time	The date and time of the last device boot.	•			•	•					•		

Device Statistics: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
Device Time Zone	The time zone setting on the device.	•			•	•					•		
Device GMT Offset	The time difference between the device's time zone and Greenwich Mean Time.	•			•	•					•		
AS User Agent	The device's native ActiveSync application version, which corresponds to the device's operating system version.	•	•	•	•	•	•	•	•	•	•	•	•
AS Version	ActiveSync protocol version used by the device.	•	•	•	•	•	•	•	•	•	•	•	•
Battery Level	Displays the percentage of battery life left for the device.	•		•	•	•		•			•		
Battery Status	Displays whether the device battery is charging or unplugged.	•		•	•	•		•			•		
ZENworks Application Language	Name of the language the *ZENworks Mobile Management* device application is using.	•		•	•	•		•			•		
ZENworks Application Version	Displays the version number of the *ZENworks Mobile Management* device application.	•		•	•	•		•			•		
Downloaded Data (any network)	Data usage statistics for data going out from the device over the network since the last device boot time. The sum-total of all networks.	•		•	•	•		•					

Device Statistics: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
	BlackBerry with NotifySync: Limited to GSM devices.												
Downloaded Data (cellular network)	Data usage statistics for data coming in to the device over the network since the last device boot time. The subtotal for the cellular network alone.	•		•		•		•					
Downloaded Data (Wi-Fi)	Data usage statistics for data coming in to the device over the network since the last device boot time. The subtotal for Wi-Fi alone.	•		•		•		•					
Uploaded Data (any network)	Data usage statistics for data going out from the device over the network since the last device boot time. The sum-total of all networks. *BlackBerry with NotifySync*: Limited to GSM devices.	•		•	•	•		•					
Uploaded Data (cellular network)	Data usage statistics for data going out from the device over the network since the last device boot time. The subtotal for the cellular network alone.	•		•		•		•					
Uploaded Data (Wi-Fi)	Data usage statistics for data going out from the device over the network since the last device boot time. The subtotal for Wi-Fi alone.	•		•		•		•					

Device Statistics: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
Jailbroken	Whether or not an iOS or Android device has been jailbroken/rooted.	•		•		•							
Device IMEI	The International Mobile Equipment Identify number. See http://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity *BlackBerry with NotifySync:* Limited to GSM devices.	•		•	•	•		•			•		
Device Model	Displays the device model.	•		•	•	•		•			•		
Device UID	Displays the device UID. *Symbian*: The device UID is the same as the device IMEI.				•			•			•		
Device Type	Displays the device type as reported by the device.	•		•	•	•		•			•		
Device Memory Capacity	Displays the total of the used and unused memory on the device.	•		•	•	•		•			•		
Device Free Memory	Displays the amount of free memory left on the device. (Labeled *Available Device Capacity* for iOS devices.)	•		•	•	•		•			•		
Network Type	Displays the network type the device is using.	•		•	•	•		•			•		
OS Language	Name of the language the device OS is using.	•		•	•			•			•		
OS Version	Displays the device OS version.	•		•	•	•		•			•		

Device Statistics: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
Phone Number	Displays device phone number.	•		•	•	•					•		
Device Ownership	Tracks whether the device is a company device or personal device.	•		•	•	•		•			•		
Phone Usage	Displays the phone minutes used in the last 30 days. This is calculated from phone logs.	•		•	•			•			•		
Roaming	Displays a simple yes or no if the device is roaming.	•		•	•	•		•			•		
SD Card Status	Displays if there is an SD card in the device. iOS devices do not have SD card capability.	•		•	•			•			•		
SD Card Free Memory	Displays the amount of free memory left on the device's storage card. iOS devices do not have SD card capability.	•		•	•			•			•		
SD Card Total Memory	Displays the total of the used and unused memory on the device storage card.	•		•	•			•			•		
Signal Level	Displays the signal strength using a percentage value.	•		•	•			•			•		
Device Encrypted	Whether the data stored in the device's local memory is encrypted.	•	•	•	•	•	•				•		

Device Statistics: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
SD Card Encrypted	Whether the data stored on the device's storage card is encrypted.			•							•		
TouchDown Registered	Whether the TouchDown application is registered on an Android device.	•		•									
SD Card IMSI Number	The ID number of the SD card: International Mobile Subscriber Identity.	•		•	•						•		
Device Name	The name given via iTunes.					•							
Build Version	iOS build number.					•							
Model Name	Name of the device model.					•							
Model	The device's internal model number.					•							
Product Name	The model code for the device.					•							
Serial Number	The device's serial number.					•							
Cellular Technology	Cellular technology 0 = none 1 = GSM 2 = CDMA					•							
MEID	The device's MEID (CDMA).					•							
Modem Firmware Version	The baseband firmware version.					•							
ICCID	The ICC identifier for the installed SIM card (if applicable).					•							

Device Statistics: All Devices	**Description**	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
Bluetooth MAC	Bluetooth MAC address.					•							
Wi-Fi MAC	Wi-Fi MAC address.					•							
Current Carrier Network	Name of current carrier network.					•							
SIM Carrier Network	Name of the home carrier network. (Note: Applies to CDMA in spite of its name.)					•							
Carrier Settings Version	Version of currently installed carrier settings file.					•							
Voice Roaming Enabled	Current setting for Voice Roaming.					•							
Data Roaming Enabled	Current setting for Data Roaming.					•							
Subscriber MCC	Home Mobile Country Code					•							
Subscriber MNC	Home Mobile Network Code					•							
Current MCC	Current Mobile Country Code					•							
Current MNC	Current Mobile Network Code					•							

Policy Rules: iOS Device

Policy Suite Rules: iOS	**Description**	**iOS**	**iOS w/o ZMM**
Device Features			
Allow FaceTime	Determines whether the user can receive or place video calls. *Allow Camera* in the *Device Controls* must be enabled as well.	•	
Allow Voice Dialing	Determines whether the user can dial their phone using voice commands.	•	
Allow Screenshot	Determines whether or not the user can save a screenshot of the device display.	•	
Allow Explicit Content	Determines whether or not explicit music or video content purchased from the iTunes store is hidden.	•	
Allow Automatic Sync When Roaming	When disabled, devices that are roaming synchronize only when an account is accessed by the user.	•	
Allow Siri	Determines whether iPhone 4S devices allow the Siri speech recognition personal assistant.	•	
Allow Siri while device locked	Determines whether Siri is disabled when the device is locked with a password. Enabling *Allow Siri* is a prerequisite for enabling this option. Requires iOS 5.1 or greater.	•	
Enable Siri Profanity Filter	Filters out profanity from Siri, preventing it from recognizing or interpreting profanity. Enabling *Allow Siri* is a prerequisite for enabling this option.	•	

Policy Suite Rules: iOS	**Description**	iOS	iOS w/o ZMM
	Requires iOS 5.1 or greater.		
Allow Multiplayer Gaming	Determines whether the device will allow multiplayer gaming between iOS devices via Bluetooth or Wi-Fi. When this option is disabled, users cannot play multiplayer games in the Game Center.	•	
Allow Adding Game Center Friends	Determines whether the device allows adding friends or building a social gaming network associated with the Game Center app.	•	
Force iTunes Store Password Entry	Determines whether the device will require a password to access the iTunes store. Requires users to enter their Apple ID before making any purchase. Normally, there is a brief grace period after a purchase is made before users must authenticate for subsequent purchases. (Requires iOS 5.0 or higher.)	•	
Force Encrypted Backup	When disabled, users can choose whether or not device backups performed in iTunes, are stored in encrypted format on the computer.	•	
Allow Location Services	Determines whether Location Services can be enabled on the device. Requires iOS 5.1 or greater.	•	
Applications			
Allow Application Installation	When disabled, the App Store is disabled and the icon is removed from the device Home screen. In addition, users are prevented from installing applications made available through the *ZENworks* Mobile Apps list.	•	
Allow In App Purchases	Determines whether or not users can make in-app purchases.	•	
Allow YouTube	Determines whether the use of YouTube is allowed on the device. If disabled, the icon is removed from the Home screen.	•	
Allow iTunes	Determines whether the use of iTunes is allowed on the device. If disabled, the icon is removed from the Home screen and users cannot preview, purchase, or download content.	•	

Policy Suite Rules: iOS	**Description**	**iOS**	**iOS w/o ZMM**
Safari Browser			
Allow Safari	Determines whether use of the Safari Web browser is allowed on the device. If disabled, the Safari icon is removed from the Home screen and it prevents users from opening Web clips. Disabling Safari might also prevent the use of third-party browsers. *Allow Browser* in the *Device Controls* must also be enabled.	•	
Accept Cookies	Determines the Safari cookie policy – Whether the device accepts all cookies, no cookies, or only cookies from sites that were directly accessed.	•	
Allow Auto-fill	Determines whether Safari remembers what users enter in Web forms.	•	
Allow JavaScript	Determines whether Safari ignores JavaScript on Websites.	•	
Block Pop-ups	Determines whether Safari's pop-up blocking feature is enabled.	•	
Force Fraud Warning	Determines whether Safari attempts to prevent the user form visiting Websites identified as being fraudulent of compromised.	•	
Ratings			
Rating Region	Determines the media content rating scale used by a particular region.	•	
Application Ratings	Determines the maximum allowed ratings for apps.	•	
Movie Ratings	Determines the maximum allowed ratings for movies.	•	
TV Show Ratings	Determines the maximum allowed ratings for TV shows.	•	
Security			
Allow Profile Removal	Determines whether an iOS user can delete the *ZENworks Mobile Management* configuration profile from the device.	•	

Policy Suite Rules: iOS	Description	iOS	iOS w/o ZMM
	Includes an option to allow deletion with the use of a password.		
Profile Removal Password	Defines the password with which a user can remove the profile.	•	
Allow Untrusted TLS Prompt	Determines whether users are asked if they want to trust certifications that cannot be verified. This setting applies to Safari and to Mail, Contacts, and Calendar accounts. (Requires iOS 5.0 or higher.)	•	
Allow Diagnostic Submission Text	Determines whether the device sends iOS diagnostic data to Apple. When this option is disabled, iOS diagnostic information is not sent to Apple.	•	
iCloud			
Allow iCloud Backup	Determines whether the device is permitted to back up to and restore from iCloud.	•	
Allow Document Sync	Determines whether the device allows document synchronization to iCloud. When this option is enabled, users can store documents in iCloud.	•	
Allow Photo Stream	Determines whether the device allows Photo Stream. If enabled, iCloud automatically pushes (via Wi-Fi) a copy of any photo taken on or imported to an iOS device, to the user's other iOS devices, iPhoto or Aperture on a Mac, Pictures Library on a PC, and Apple TV. When this option is disabled, installing a configuration profile with this restriction erases Photo Stream photos from the user's device and prevents photos from the Camera Roll from being sent to Photo Stream. If there are no other copies of these photos, they might be lost.	•	
iOS MDM			
Record Installed Applications	Accesses and records applications installed on devices.	•	

Policy Suite Rules: iOS	**Description**	**iOS**	**iOS w/o ZMM**
Manage Mobile Apps	Determines whether an administrator can manage apps for users in a particular policy suite.	•	
Apply Managed Settings	Determines whether an administrator can enable the *Allow Voice Roaming* and *Allow Data Roaming* policies.	•	
Allow Voice Roaming	Determines whether users can make calls while roaming. This option only affects iOS 5 devices. Availability depends on carrier.	•	
Allow Data Roaming	Determines whether users can use the data features of their smart device while roaming. When data roaming is allowed, voice roaming is automatically allowed as well.	•	

Policy Rules: TouchDown

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o ZMM	Anrd	Anrd w/o ZMM
Installation					
Allow any server certificate	Currently, ZENworks Mobile Management requires a CA signed certificate and does not support self-signed certificates. For the present, this option should be disabled.	•			
Initiate registration	At the completion of the *ZENworks Mobile Management* enrollment, the user is prompted to configure TouchDown. When the user confirms, this automatically registers TouchDown and creates an ActiveSync account with the user credentials provided during *ZENworks Mobile Management* enrollment. If disabled, the user is not prompted and must initiate the TouchDown configuration by opening the *ZENworks Mobile Management* app and selecting *Settings* > *TouchDown Settings*.	•			
General					
Allow copy/paste in emails	Determines whether users can copy/paste text when composing an email.	•			
Allow easy PIN recovery	Allows users to reset the TouchDown PIN (password) by using their Exchange account password. With Exchange 2007 or 2010, this does not function when *Security Settings* > *Enable Password Recovery* is enabled. The ActiveSync password recovery method is used instead.	•			
Allow speak notification option	When enabled, users can choose to have the device issue spoken email and appointment notifications. When disabled, the	•			

Policy Suite Rules: TouchDown Specific	**Description**	TD/A	TD/A w/o ZMM	Anrd	Anrd w/o ZMM
	option is not visible and the function is disabled. At least one of two suppression rules must be enabled in order for this to function: *Allow appointment alert configuration* or *Allow email alert configuration*.				
Show TouchDown PIN	This setting is dependent upon the ActiveSync *Require Password* policy. When *Require Password* is disabled, this setting has no effect and neither the device nor the TouchDown app locks or requires a password. When *Require Password* is enabled, behavior varies by Android OS version. *For Android OS 2.2 or greater* – The device locks and requires a password. The *Show TouchDown PIN* setting determines whether the TouchDown app locks/requires a password as well. When enabled, TouchDown locks. When disabled, TouchDown does not lock. *For Android OS 2.1 or less* – When the *Show TouchDown PIN* setting is enabled, the device does not lock, but TouchDown does. When it is disabled, neither the device nor the TouchDown app locks; however, the user is still prompted to create a PIN/password.	•			
Show calendar info on notification bar	Determines whether appointment subjects are displayed in the device notification bar when reminders are shown. To successfully display notifications, the following TouchDown settings must also be configured on the device: In the Advanced TouchDown Settings, enable the *Appointment reminders at non-peak times* options and configure *Appointment Alerts* to *Use system settings.*	•			

Policy Suite Rules: TouchDown Specific	**Description**	TD/A	TD/A w/o ZMM	Anrd	Anrd w/o ZMM
Show email info on notification bar	Determines whether the email sender and subject are displayed in the device notification bar when email notifications are shown. To successfully display notifications, the following TouchDown settings must also be configured on the device: In the Advanced TouchDown Settings, enable the *Notify on new mail* option and configure *Email Alerts* to *Use system settings.*	•			
Show task info on notification bar	Determines whether task subjects are displayed in the device notification bar when task notifications are shown. To successfully display notifications, the following TouchDown settings must also be configured on the device: In the Advanced TouchDown Settings, enable the *Appointment reminders at non-peak times* options and configure *Appointment Alerts* to *Use system settings.*	•			
Signature					
Allow change signature on device	When enabled, allows user to change the signature which accompanies email sent from the device. This option does not function unless the *Suppression > Allow signature line* field is enabled.	•			
Set signature (Corporate / Individual)	Allows the entry of a signature determined by the administrator.	•			
Widgets					
Allow export to third party widgets	Determines whether or not TouchDown data can be communicated to third-party widgets that request it.	•			
Allow TouchDown calendar widget	Determines whether or not the TouchDown calendar widget shows data.	•			
Allow TouchDown email widget	Determines whether or not the TouchDown email widget shows data.	•			

Policy Suite Rules: TouchDown Specific	**Description**	TD/A	TD/A w/o ZMM	Anrd	Anrd w/o ZMM
Allow TouchDown task widget	Determines whether or not the TouchDown task widget shows data.	•			
Allow TouchDown universal widget	Determines whether or not the TouchDown universal widget shows email, calendar and task data.	•			
Show widget data when TouchDown is locked	Determines whether widget data is locked when TouchDown is locked. This option does not function unless *Security Settings >Require Password*; *TouchDown-General > Show TouchDown PIN*; and at least one widget (calendar, email, third-party, task, or universal) are enabled.	•			
Phone Book					
Phone book fields to copy	Choose which fields of a contact synchronize when users copy contacts to the device phone book. Choosing all or some of the fields is a prerequisite for the suppression rules: *Allow copy phone format options* and *Allow update contact changes to phone options.*	•			
Suppressions					
Suppression configuration	Choose which options to hide or expose to TouchDown users. Disabling an option suppresses or hides it on the device and locks how it was previously set on the device. Enabling an option allows the user to access and change it on the device.	•			
Suppressions: Calendar, Contacts, Tasks					
Allow appointment alert configuration	Enables users to customize the alerts displayed for appointment reminders.	•			
Allow appointment reminders at non-peak times option	Enables users to allow appointment reminders during periods when the device is not synchronizing.	•			
Allow appointment synchronization option	Enables users to set how many days of appointments to keep on the device.	•			
Allow category configuration	Enables users to select colors for contact, event, and task	•			

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o ZMM	Anrd	Anrd w/o ZMM
	categories.				
Allow copy to phone format options	Enables users to select the format of contacts (First or Last Name placed first) copied from TouchDown to the Android phone book. Choosing all or some of the fields in the *Phone Book > Phone book fields to copy* rule is a prerequisite.	•			
Allow enable appointment reminders option	Allows users to enable appointment reminders.	•			
Allow include phone contacts in picklist option	When enabled, the contact list displayed when composing email or SMS includes contacts from the Android Phone Book.	•			
Allow normalize phone numbers option	When enabled, contact phone numbers retrieved from the server are changed to the following format: X/x/ext (extension) becomes ; P/p (pause) becomes ; W/w (tone wait) becomes ,	•			
Allow reminders configuration	Enables users to configure calendar event reminders.	•			
Allow update contact changes to phone option	When enabled, updates made to contacts via TouchDown also update the Android phone book database. Choosing all or some of the fields in the *Phone Book > Phone book fields to copy* rule is a prerequisite.	•			
Suppressions: Device Control					
Allow ActiveSync device type string field	Enables users to modify the ActiveSync device type the device reports to the *ZENworks Mobile Management* server. In order for the server to maintain accurate information, this should be disabled.	•			
Allow backup database (menu option)	Enables users to back up the TouchDown database to the SD card.	•			
Allow backup settings	Enables users to back up the TouchDown settings to the SD card.	•			

Policy Suite Rules: TouchDown Specific	**Description**	TD/A	TD/A w/o ZMM	Anrd	Anrd w/o ZMM
Allow disable tablet mode (tablet devices only) option	Allows tablet users to disable the automatic switch to tablet mode.	•			
Allow exclude attachments from gallery option	When enabled, prevents the Android Gallery application from scanning media attachments downloaded to the SD card.	•			
Allow export settings	Enables users to do an SD card export for a .pcf configuration file with the settings required to connect to the server.	•			
Allow filtered tasks on home screen and widgets option	When enabled, the tasks shown on the Home screen and on the Task Widget are filtered just as they are on the TouchDown Tasks screen.	•			
Allow login ID, email address, domain fields	Displays the user's ActiveSync account information and allows user to edit.	•			
Allow quick configuration	Enables users to use the Quick Configuration option to create the ActiveSync account.	•			
Allow restore database (menu option)	Enables users to restore a backup of the TouchDown database from the SD card.	•			
Allow restore settings	Enables users to restore TouchDown settings they have backed up to the SD card.	•			
Allow server name fields	Displays the address of the ZENworks Mobile Management server and allows the user to edit it. This option also controls the following device options: *Uses SSL* and *Fetch and Trust Certificate*.	•			
Allow show emails on startup option	Enables users to open TouchDown to the email list instead of the main display pane.	•			
Allow use system background data setting option	When enabled, TouchDown honors the Android Background Data setting, which controls whether apps update in the background or only on demand.	•			

Policy Suite Rules: TouchDown Specific	**Description**	TD/A	TD/A w/o ZMM	Anrd	Anrd w/o ZMM
Suppressions: Email					
Allow always BCC myself option	Enables a user to have his or her own email address added to the BCC of every email sent from the device.	•			
Allow choose folders	Allows selection of the folders TouchDown will synchronize with the server. In addition to *Choose Folders*, this also controls the following device options: *Selected Email Folders* and *Refresh Folders*.	•			
Allow disable SmartReplies and SmartForwards option	Enables users to turn off Smart Reply and Smart Forward functionality.	•			
Allow don't delete emails on server option	Enables users to delete email on the device, but prevents it from being deleted on the server.	•			
Allow don't mark read on server	Enables users to prevent email, read or unread on the device, from being marked as read or unread on the server.	•			
Allow email alerts configuration	Enables users to customize the alerts displayed for new email.	•			
Allow email body style options	Enables users to choose font, size, color, and style of the HTML email they compose.	•			
Allow email checking frequency options	Enables users to determine how often the device checks for new email.	•			
Allow email download size options	Enables users to determine the size of downloaded email messages. An email larger than this value displays an option to download the remainder. (Zimbra users - value must be no greater than 10 KB.)	•			
Allow email view text size options	Enables users to select the text size of email they view.	•			
Allow emails to synchronize options	Enables users to set how many days of email to keep on the device.	•			

Policy Suite Rules: TouchDown Specific	**Description**	TD/A	TD/A w/o ZMM	Anrd	Anrd w/o ZMM
Allow enable HTML email options	TouchDown attempts to download and display email in HTML format. Mail servers other than Exchange should leave this disabled.	•			
Allow folder language options	Enables users to choose the language used for folder labeling.	•			
Allow manage rules option	Enables users to create and manage rules for incoming email.	•			
Allow notify on new mail option	Determines whether a notification appears when new email arrives.	•			
Allow out of office configuration	Enables users to configure automatic Out of Office replies.	•			
Allow signature line field	Enables users to enter their own signature for email sent from the device.	•			
Suppressions: Security					
Allow clean SD card on remote wipe option	Determines whether a remote wipe removes attachments downloaded to the SD card.	•			
Allow client certs configuration	Enables users to import a client certificate, which TouchDown uses to authenticate with the server.	•			
Allow remote kill configuration	Enables users to configure the device to allow a remote wipe of TouchDown data. An email sent to the device with a designated code in the subject field initiates the wipe.	•			
Allow security policy display	Displays the security policies imposed by the server, which are governing the device.	•			
Allow S/MIME settings configuration	Enables users to adjust the settings of the S/MIME options for their device.	•			
Allow wipe data (menu option)	When enabled, users can choose a device option to erase all TouchDown data and return TouchDown to a pre-registration state.	•			

Policy Suite Rules: TouchDown Specific	**Description**	TD/A	TD/A w/o ZMM	Anrd	Anrd w/o ZMM
Suppressions: Synchronization					
Allow defer server updates option	When enabled, TouchDown updates do not sync to the server until the next scheduled sync occurs, an item arrives via direct push, or the user initiates a manual sync.	•			
Allow enable SMS syncing (Exchange 2010 Only) option	Enables users to synchronize SMS messages to Outlook.	•			
Allow manual sync when roaming option	When enabled, automatic synchronization stops when the device is roaming, but users can initiate a manual sync.	•			
Allow notify on password failure option	When enabled, the user is notified if synchronization fails because of a user password issue.	•			
Allow notify on polling failure option	When enabled, the user is notified if synchronization fails.	•			
Allow notify on successful polling option	When enabled, the user is notified when synchronization is successful.	•			
Allow peak time configuration	Enables users to set the hours during which TouchDown synchronizes with the server.	•			
Allow poll during off-peak times option	During off peak times (times outside the peak schedule), TouchDown pulls down updates from the server when a user sends an email, reply, or forward from the device.	•			

Compliance Manager

Compliance Manager	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
Access Restriction													
Restrict on ActiveSync authorization failures	A device passes invalid credentials for the ActiveSync account of a known user to the server a number of times that exceeds the set limit.	●	●	●	●	●	●	●	●	●	●	●	●
Restrict ActiveSync protocol	A device cannot support sufficient ActiveSync policies, because of ActiveSync version support limitations with the device or server.	●	●	●	●	●	●	●	●	●	●	●	●
Restrict cellular connection	A device is using a cellular network connection and is in violation of the enabled *Restrict Cellular Connection* access policy.				●								
Restrict Liability	A device enrolls with a liability status specifically restricted by the *Restrict Liability* access policy.	●	●	●	●	●	●	●	●	●	●	●	●

Compliance Manager	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
Restrict on ZENworks authorization failures	A device passes invalid credentials for the *ZENworks Mobile Management* account of a known user to the server a number of times that exceeds the set limit.	●	NA	●	●	●	NA	●	NA	NA	●	NA	NA
Restrict BlackBerrys without NotifySync	A BlackBerry device that does not have the *NotifySync* application has enrolled.	NA	NA	NA	●	NA	NA	NA	NA	NA	NA	NA	NA
Restrict if roaming detected	A device is roaming and is in violation of the *Restrict if Roaming Detected* access policy.	●		●	●	●		●			●		
Restrict if SIM Card removed or changed	A user has removed or changed the SIM card in a device and is in violation of the *Restrict if SIM Card is Removed or Changed* access policy.	●		●	●	●					●		
Restrict TouchDown for Android	TouchDown is required and either an Android device does not have the TouchDown application or the TouchDown version does not meet the minimum requirement.	●	●	●	NA	NA	NA	NA	NA	NA	NA	NA	NA
Restrict user ActiveSync connections	A device's *Last ActiveSync Sync* time stamp has not updated within the set interval.	●	●	●	●	●	●	●	●	●	●	●	●
Restrict Wi-Fi connection	A device is using a Wi-Fi connection and is in violation of the enabled *Restrict Wi-Fi Connection* access policy.				●								
Single Devices	A specific device, identified by phone number or UID number, has been denied access.	●		●	●	●		●					
Single Users	A specific user, identified by User Name, has been denied access.	●	●	●	●	●	●	●	●	●	●	●	●

Compliance Manager	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
Device Platform Restriction													
Restrict if ZENworks app is not enrolled	A device enrolls via the native ActiveSync agent alone and without the *ZENworks Mobile Management* application.	●	●	●	●	●	●	●	●	●	●		
Restrict if location not updated	A device's location has not updated within the defined interval.	●		●	●	●		●			●		
Restrict user ZENworks connections	A device's *Last ZENworks Sync* time stamp has not updated within the set interval.	●		●	●	●		●			●		
Restrict if policy out of date	A policy has been updated on the server, but a device has not updated within the set grace period.	●	●	●	●	●	●	●	●	●	●	●	●
Restrict rooted devices	A rooted Android device connects to the server.	●		●	NA	NA	NA	NA	NA	NA	NA	NA	NA
Restrict jailbroken devices	A jailbroken iOS device connects to the server.	NA	NA	NA	NA	●		NA	NA	NA	NA	NA	NA
Restrict if iOS passcode not initiated	The user's policy suite requires a password, but the iOS device does not have a passcode initiated.	NA	NA	NA	NA	●		NA	NA	NA	NA	NA	NA
Restrict if iOS passcode is not compliant with requirements	The user's policy suite requires a password, but the iOS device does not have a passcode compliant with the requirements.	NA	NA	NA	NA	●		NA	NA	NA	NA	NA	NA
Restrict if iOS passcode is not compliant with data protection	The iOS device does not have a passcode and thus is not compliant with iOS "data protection," which enhances the built-in hardware encryption by protecting the hardware encryption keys with the passcode.	NA	NA	NA	NA	●		NA	NA	NA	NA	NA	NA

Compliance Manager	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
Restrict if iOS unmanaged configuration profile is on device	An iOS device has an unmanaged configuration profile.	NA	NA	NA	NA	●		NA	NA	NA	NA	NA	NA
Restrict if iOS APN profiles are not enrolled	An iOS device has not loaded the iOS APN configuration profile and has never synchronized through the Apple MDM API.	NA	NA	NA	NA	●		NA	NA	NA	NA	NA	NA
Restrict if no iOS APN connectivity	A device's *Last iOS APN Sync* time stamp has not updated within the set interval.	NA	NA	NA	NA	●		NA	NA	NA	NA	NA	NA
Non-Access Policy Based Alerts													
Low battery detection	A device's battery level has fallen below a specified warning level.	●		●	●	●		●			●		
Low memory detection	A device's memory level has fallen below the greater of the two specified levels.	●		●	●	●		●			●		
Low on redemption codes	The number of redemption codes (for iOS devices installing an app obtained through the Apple Volume Purchase Program) available on the server has fallen below a specified amount.	NA	NA	NA	NA	●		NA	NA	NA	NA	NA	NA
ZENworks app is not enrolled	A device of any platform type connects to the server via ActiveSync and does not have the *ZENworks Mobile Management* application enrolled.	●	●	●	●	●	●	●	●	●	●	●	●
Organization-wide ActiveSync connectivity	The *Last ActiveSync Sync* time stamp has not updated for any users within the set interval.	●	●	●	●	●	●	●	●	●	●	●	●
Organization-wide ZENworks connectivity	The *Last ZENworks Sync* time stamp has not updated for any users within the set interval.	●		●	●	●		●			●		

Compliance Manager	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
Watch List	A user or policy suite on the Watch List grid has exceeded the time for which it was being monitored.	●	●	●	●	●	●	●	●	●	●	●	●
User's e-mail not set	A user's email address has not been set. Because a user's email address cannot always be determined during Hands-Off provisioning, this alerts the administrator that an email address for the user should be manually set.	●	●	●	●	●	●	●	●	●	●	●	●
Event Based Alerts													
ActiveSync Account Already Enrolled	An iOS profile included an ActiveSync payload that could not be installed because an identical ActiveSync account was already enrolled.	NA	NA	NA	NA	●		NA	NA	NA	NA	NA	NA
Clear device enrollment	An administrator has issued a *Clear Device Enrollment* command from the dashboard to a device.	●	●	●	●	●	●	●	●	●	●	●	●
Clear passcode issued by Admin	An administrator has issued a *Clear Passcode* from the dashboard to an iOS device.	NA	NA	NA	NA	●		NA	NA	NA	NA	NA	NA
Full wipe issued by Admin	An administrator has issued a *Full Wipe* command from the dashboard to a device.	●	●	●	●	●	●	●	●	●	●	●	●
Full wipe issued by user	A user has issued a *Full Wipe* command from the User Self Administration Portal to their device.	●	●	●	●	●	●	●	●	●	●	●	●
Lock device issued by Admin	An administrator has issued a *Lock Device* command from the dashboard to a device.	●		●	●	●		●			●		
Lock device issued by user	A user has issued a *Lock Device* command from the User Self Administration Portal to their device.	●		●	●	●					●		

Compliance Manager	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
New Hands-Off Provisioned device	Any time a new device uses Hands-Off enrollment to connect to the system.	•	•	•	•	•	•	•	•	•	•	•	•
New Hands-Off Provisioned user	Any time a new user uses Hands-Off enrollment to connect to the system.	•	•	•	•	•	•	•	•	•	•	•	•
Recovery password requested by device	A user requests a temporary recovery password form a device's locked screen.			•	•								
Recovery Password viewed by Admin	An administrator has attempted to view a temporary recovery password issued for a user from the dashboard.			•	•								
Recovery Password viewed by user	A user has attempted to view a temporary recovery password from the User Self Administration Portal. (This does not detect when the recovery password has been viewed through OWA.)			•	•								
Restricted device attempts to connect	A restricted device tries to access ActiveSync, File Share, or Mobile Apps when these resources have been blocked.	•	•	•	•	•	•	•	•	•	•	•	•
Selective wipe issued by Admin	An administrator has issued a *Selective Wipe* command from the dashboard to a device.	•		•	•	•		•			•		
Selective wipe issued by user	A user has issued a *Selective Wipe* command from the User Self Administration Portal to a device.	•		•	•	•		•			•		
TouchDown policy override detection	The system issues a warning if it detects that a user has overridden the TouchDown settings governed by *ZENworks Mobile Management*.	NA	NA	•	NA	NA	NA	NA	NA	NA	NA	NA	NA

Compliance Manager	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	iOS w/o ZMM	S60	S60 w/o ZMM	wOS	WM	WM w/o ZMM	WP7
User restricted	A user becomes restricted for any reason.	●	●	●	●	●	●	●	●	●	●	●	●
Wipe storage card	An administrator has issued a *Wipe Storage Card* command from the dashboard to a device.	●		●	●	NA	NA				●		