Functionality by Device Platform

ZENworks® Mobile Management 2.7.x

August 2013

Novell.

TABLE OF CONTENTS

►**Policy Rules: All Devices**

Audit Tracking

Device Control

- Device Features
- Email
- ActiveSync Synchronization

File Share Permissions

Mobile Apps Permissions

Restricted Apps Permissions

Resource Control

Security Settings

- Password
- Encryption
- Device Inactivity and Locking
- Emergency Calls

S/MIME Settings

►**Policy Rules: iOS Device**

- Device Features
- Applications
- Safari Browser
- Ratings
- Security
- iCloud
- iOS MDM
- Supervised Mode

►**Policy Rules: TouchDown**

- Installation
- General
- Signature
- Widgets
- Phone Book
- User Configurable Settings
- Suppression Rules

►**Security: All Devices**

- Security Commands
- Network Connection Security and Configuration

►**Device Statistics: All Devices**

- Device Statistics

►**Compliance Manager**

- Access Policies and Device Restrictions
- Non-Access Policy Based
- Event Based Alerts
- System Alerts

The information in these tables describes functionality supported by each device platform for *ZENworks Mobile Management*, version 2.7.x.

Device platforms supported by *ZENworks Mobile Management* are Android, BlackBerry (4.5-7.1) with *NotifySync*, BlackBerry (OS 10), iOS, Symbian S60 3rd edition, webOS, Windows Mobile 6, and Windows Phone. Supported device operating system versions are listed below.

Anrd	TD/A	BB10	NS/BB	iOS	TD/iOS	S60	wOS	WM	WP
Android devices OS v2.2 – 4.2.2	Android devices OS v2.2 - 4.2.2 with TouchDown v8.1.x	BlackBerry devices OS 10 (Z10)	BlackBerry devices OS v4.5 – 7.1 with NotifySync v4.9 or greater	iOS 5 – 6.1.3 multitasking devices	iOS 5 – 6.1.3 multitasking devices with TouchDown v1.3.8	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, 7.5, 8

End-of-Life Notice –*ZENworks Mobile Management* server v2.7.2 and *ZENworks Mobile Management for Android with TouchDown* app version 2.7.2.x were the last to support Android OS v2.0 - v2.1.
End-of-Life Notice –*ZENworks Mobile Management* server v2.7.2 and *ZENworks Mobile Management for iOS* app version 2.7.1.x were the last to support iOS devices not running iOS 5 or above.

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 4.5-7.1 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
- On BlackBerry devices (OS 4.5-7.1), *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 5 - 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

BlackBerry (OS 10), webOS and Windows Phone 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.

● Red text or dots indicate **ActiveSync only -** Currently, there is no *ZENworks Mobile Management* app available for BB10, WP or wOS. Devices support the feature via the native ActiveSync app on the device. BlackBerry 4.5-7.1 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	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
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: Sends 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 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	●		●	●					●				

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
	Mobile 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 Application Data Usage	Requires the device to send data usage statistics associated with device applications. Usage statistics are displayed in the Apps section of the User Profile.	●		●										
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 Bluetooth is allowed to operate on the device. There are three settings: Don't allow Bluetooth Allow only Bluetooth headsets Allow all Bluetooth											●	●	

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
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.											●	●	
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.								●			●	●	

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
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.			●	●		●					●	●	BB10
Maximum HTML email body truncation size (in KB) (ActiveSync)	Defines the maximum 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 plain text 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.			●	●		●					●	●	BB10 WP
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 device. Not supported with systems operating with ActiveSync protocol 2.5, such as Exchange 2003.			●	●	●	●	●	●			●	●	BB10 WP

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
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.	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
File and Application Management														
File Share Permissions	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 Permissions	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 device type. Sets permissions for access per policy suite. iOS Configurator devices: Recommended apps can only be made available by an administrator via force push.	●		●	●	●	●		●	●		●		
Restricted Apps Permissions	Create a list of strings that will filter either by blacklisting or whitelisting applications. Blacklist - When one or more blacklisted applications are installed on a device, the user's access to email, shared files, app lists, or other organization resources can be blocked. Whitelist – When one or more applications are installed on a device	●		●		●	●	●	●					

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
	that are not on the Whitelist, the user's access to email, shared files, app lists, or other organization resources can be blocked.													
Resource Control														
Allow ActiveSync	Determines whether users are permitted to make ActiveSync connections.	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
Allow File Share	Determines whether users are permitted to access the File Share.	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
Allow Mobile Apps	Determines whether users are permitted to access the Mobile Apps list.	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
Security: Password														
Require Password (ActiveSync)	Forces the device to require a lock password.	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
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,	●	●	●	●	●	●	●	●	●	●	●	●	WP

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
	such as Exchange 2003.													
Require Minimum Password Length (ActiveSync)	Forces the device to require a password with a specified minimum length.	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
Minimum Password Length (ActiveSync)	Defines the minimum password length.	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
Require complex password	User must create a password containing at least a letter, a numerical digit, and a special symbol. Requires Android OS 3.0 or greater. If this requirement is set and a device does not support it, the next level of security, which is alphanumeric will be implemented.	●	●	●										
Require Alphanumeric Password (ActiveSync)	Forces the device to require a device password to contain both letters and numbers.	●	●	●	●	●	●	●	●	●	●	●	●	wOS
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 alphabetic password	User must create a password containing at least alphabetic (or other symbol) characters.	●	●	●										

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
Require numeric password	User must create a password containing at least numeric characters.	●	●	●										
Require biometric password	Allows for low-security biometric (face) recognition technology. Uses technologies that can recognize the identity of an individual to about a 3 digit PIN (false detection is less than 1 in 1,000). Requires Android OS 4.0 or greater.	●	●	●										
Require Device Password Expiration (ActiveSync)	Forces the device to require users to update their passwords after a number of days. Not supported with systems 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).	●	●	●	●	●	●	●	●			●	●	BB10 WP
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).	●	●	●	●	●	●	●	●			●	●	BB10 WP
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.	●	●	●	●	●	●	●	●			●	●	BB10 WP
Number of passwords stored	Defines the number of device passwords stored to prevent users from reusing				●	●	●	●	●			●	●	BB10 WP

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
(ActiveSync)	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 their entry error.				●									
Begin password echo after attempts	Defines the number of unlock attempts before echoing begins.				●									
Security: Encryption														
Require Encryption on the Device (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. Gives repeated reminders until the user initiates encryption. For Android w/ TouchDown, TouchDown data is encrypted (email, calendar, contacts, tasks). Use *Require TouchDown encryption* instead, to require encryption of TouchDown data only. Gives repeated reminders until the user initiates encryption. With NotifySync for BlackBerry, only NotifySync data is encrypted (email).	●	●	●	●	●	●	●	●			●	●	BB10
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).			●								●	●	BB10

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
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 re-entered."	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
Max Inactivity Timeout (in minutes) (ActiveSync)	Defines the maximum value a user can set for 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.	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
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 maximum value a user can set for 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.				●									
Enable 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 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-					●	●		●					

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
	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 Number of 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: 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. 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 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. BB10, webOS and WP or any device without *ZENworks Mobile Management* app: The device returns to factory	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
	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.	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
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 locked device: ambulance, fire, police, and one other emergency number.				●									
Allow dialing of any number	Gives the user an option to manually enter and call any number when the device is locked.				●									
S/MIME Settings														
Require signed SMIME messages	This setting forces the device to send digitally signed S/MIME messages.											●	●	WP
Require encrypted SMIME messages	This setting forces the device to send encrypted S/MIME messages.											●	●	WP
Require signed SMIME algorithm	This setting specifies the algorithm to be used for signing messages. Options are SHA1, MD5.											●	●	WP
Require encryption SMIME algorithm	This setting specifies the algorithm to be used for encrypting messages. Options are TripleDES, DES, RC2128bit, RC264bit, RC240bit.											●	●	WP
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.											●	●	WP

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
Allow SMIME soft certs	This setting enables/disables the device from using soft certificates to sign outgoing messages.											●	●	WP

POLICY RULES: IOS DEVICES

Policy Suite Rules: iOS	Description	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices
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. *Require Password* in Security Settings must be enabled as well.	●	●		●
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 Profanity Filter	Determines whether profanity is filtered on the device. Functional on devices in Supervised mode only. *Allow Siri* must be enabled in order to enable this policy.				●
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 higher.	●	●		●
Allow Game Center	Determines whether the Game Center is accessible. When disabled, the icon is removed from the Home screen. Functional on devices in Supervised mode only. Disabling this policy also disables *Allow Multiplayer Gaming* and *Allow Adding Game Center Friends*.				●
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.	●	●		●

Policy Suite Rules: iOS	Description	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices
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.	●	●		●
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 Passbook while device locked	Allows use of the Apple Passbook app when the device is locked, giving users access to their boarding passes, tickets, store cards, coupons, etc. Requires iOS 6.0 or higher.	●	●		●
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 Bookstore	When disabled, iBookstore is disable and users are prevented from accessing it from the iBooks app. Functional on devices in Supervised mode only. Disabling this policy also disables the non-supervised policy Allow Bookstore Erotica.				●
Allow Bookstore Erotica	Determines whether users can purchase books categorized as Erotica from iBookstore.				●
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.	●	●		●
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.	●	●		●

Policy Suite Rules: iOS	Description	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices
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. 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.	●	●		●
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. Requires iOS 6.0 or higher.	●	●		●
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.	●	●		●
Allow Shared Photo Streams	Determines whether an administrator has the ability to manage apps for users in a particular policy suite. Requires iOS 6.0 or higher.	●	●		●

Policy Suite Rules: iOS	Description	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices
iOS MDM					
Record Installed Applications	Accesses and records applications installed on devices.	●	●		●
Manage Mobile Apps	Determines whether an administrator can manage apps for users in a particular policy suite.	●	●		●
Apply Managed Settings	Determines whether the voice and data roaming settings can be managed. Applies only to iPhone 4 devices.	●	●		●
Allow Voice Roaming	Determines if the device will allow voice calls and SMS messages while roaming. Applies only to iPhone 4 devices.	●	●		●
Allow Data Roaming	Determines if the device will allow data or video while roaming. Applies only to iPhone 4 devices.	●	●		●
Supervised Mode					
Allow App Removal	Determines whether users can remove apps from the device. This does not include apps that are included with iOS, such as App Store and iTunes. Functional on devices in Supervised mode only. If this is disabled, it does not prevent managed apps from being removed via the MDM API.				●
Allow Configuration Profile Installation	Determines whether users can install additional configuration profiles onto the device. Functional on devices in Supervised mode only. If this is disabled, it does not prevent the MDM API from installing configuration profiles on the device.				●
Allow iMessage	Determines whether users can send or receive messages using iMessage. It does not prevent messaging through third party apps. If the device does not support text messaging, disabling this policy will remove the Messages icon from the Home screen. Functional on devices in Supervised mode only.				●
Global HTTP Proxy Payload.	This payload allows the administrator to specify global HTTP proxy settings: Proxy Type, Proxy Server, Proxy Server Port, Proxy Username, and Proxy Password. Configuring the settings incorrectly can prevent the Apple API from functioning altogether on the device. There can only be one of this payload at any time and it can only be installed on supervised devices.				●
Single App Mode	This payload allows administrators to specify an app to which supervised devices will be locked. The device is locked to a single application until the payload is removed. The Home button is disabled and the device returns to the specified application automatically upon wake or reboot.				●

Policy Suite Rules: iOS	Description	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices
	There can only be one of this payload at any time and it can only be installed on supervised devices.				
	Requires iOS 6.0 or higher.				

POLICY RULES: TOUCHDOWN

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o ZMM	TD/iOS	TD/iOS 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 enrollment	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.	●			
Require TouchDown encryption	Allows an organization to require the encryption of TouchDown data only on the device. Enable this option and disable the *Require encryption on the device* option, under Security Settings, so that the entire device is not encrypted. Gives repeated reminders until the user initiates encryption.	●			
Push TD enterprise license to device	The TouchDown license entered for the organization will be pushed to Android devices using TouchDown.	●			
General					
Allow copy/paste in emails	Determines whether users can copy text from a received email and paste it elsewhere.	●		●	
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 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.	●			

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o ZMM	TD/iOS	TD/iOS w/o ZMM
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: Android devices: 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. iOS devices: 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.	●		●	
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.	●		●	
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.	●		●	
Disable Printing	Disables printing from TouchDown.	●			
Forced SMIME Pin Timeout	The timeout interval before a user is required to re-enter an SMIME certificate PIN, when the certificate has been configured to require a PIN for signing or encrypting/decrypting messages.	●		●	
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.	●		●	

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o ZMM	TD/iOS	TD/iOS w/o ZMM
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.	●			
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.	●		●	
User Configurable Settings: Calendar	*About User Configurable Settings: Users can configure these policies according to preference. Administrators choose the setting for initial device configuration. Changes to these settings do affect existing TouchDown users.*				
Show All-day events in the Calendar Widget	Determines whether all-day events display in the TouchDown Calendar Widget.	●			
Show upcoming events only	Determines whether the only appointments displayed in the current day's Agenda are those that have not passed.	●			
Enable meeting resource field	Determines whether a field is enabled for specifying resources such as conference rooms or equipment when creating a new meeting.	●			
Show calendar tasks in the Agenda	Determines whether calendar tasks display in the Agenda view.	●		●	
Show overdue tasks in the Agenda	Determines whether overdue tasks display in the Agenda view.	●			

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o ZMM	TD/iOS	TD/iOS w/o ZMM
Customize the start and end days for the week	Determines whether user has the ability to define the first and last days of the week to display in the calendar Week view.	●		●	
First day of a week to show in Calendar	Define the first day of the week to display in the calendar Week view.	●		●	
Last day of a week to show in Calendar	Define the last day of the week to display in the calendar Week view.	●		●	
Start time of the work day	Times that fall between the work day's start time and end time display in a different color on Day and Week calendar views.	●		●	
End time of the work day	Times that fall between the work day's start time and end time display in a different color on Day and Week calendar views.	●		●	
Default reminder for each new event	Defines the default reminder time to assign to each new event unless otherwise specified for the event.	●		●	
Default privacy status for each new event	Defines the default privacy status to assign to each new event unless otherwise specified for the event.	●		●	
Default availability status for each new event	Defines the default availability status to assign to each new event unless otherwise specified for the event.	●		●	
Calendar zoom size	Shows the Day and Week calendar views in a larger text size.	●		●	
User Configurable Settings: Device Control					
Show a compact PIN screen (NEW 7.1)	Determines whether a compact PIN screen is shown, fitting the PIN buttons over half of the available screen space.	●			
Default theme (NEW 7.1)	Defines a default display theme for the TouchDown User Interface.	●			
User Configurable Settings: Email					
Enable email selectors	Adds a radio button beside each item in the email list, enabling the user to select multiple emails for various actions, such as delete, mark as read, move, etc.	●			
Show email summary	Determines whether part of the body of each email displays in the email list.	●			
Highlight email senders	Determines whether the sender of any email displays in a larger and bolder type than the subject field.	●		●	

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o ZMM	TD/iOS	TD/iOS w/o ZMM
Enable search as you type	Determines whether the search tool used in the email list begins to filter messages as the user types a string, as opposed to the user having to initiate the search after typing.	●			
Automatically download embedded images	Determines whether embedded images automatically download for an HTML email.	●		●	
Enable move to any folder option	Determines whether a user can move email messages to folders that have not been selected for synchronization, as opposed to only being able to move email to folders that have already synchronized.	●		●	
Highlight unread messages	When enabled, Email list displays read email in grey and unread email fully lit and in bold.	●			
Enable preview attachments option	When enabled, a thumbnail view of downloaded attachments displays before they are opened.	●			
Always expand folders	When enabled, the folder tree automatically expands when *Choose Folders* is used or when the user switches folders.	●			
Enable confirm deletes prompt	Determines whether a confirmation prompt displays when the user deletes an email.	●		●	
Enable confirm move prompt	Determines whether a confirmation prompt displays when the user moves an email.	●		●	
Toolbar mode	Determines whether the tool bar that appears when viewing an email will display, be hidden, or can be toggled on and off.	●			
After delete go to	Defines what is displayed after an email is deleted.	●		●	
Enable email alerts at non-peak times	Determines whether email notifications are sent when email arrives during non-peak times.	●			
Confirm move to Junk prompt	Determines whether a confirmation prompt displays when the user moves an email to the Junk folder.	●		●	

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o ZMM	TD/iOS	TD/iOS w/o ZMM
User Configurable Settings: Synchronization					
Enable push email mode	When enabled, switches the device from checking email at scheduled frequencies to a Push Email mode in which the device connects with the server for sustained intervals to retrieve email.	●		●	
Off-peak polling interval	Defines the polling interval for retrieving new mail during non-peak times.	●			
Suppressions	*About Suppressions: An enabled suppression gives the user control of the setting.* *A disabled suppression removes the setting from user devices. When the suppression has a control setting the administrator can configure it. When a control setting is not provided, the setting is locked as it was previously set on the device.*				
Suppression configuration	Choose which options to hide or expose to TouchDown users. Select *All* to enable all suppressions, giving users control. Select *None* to disable all suppressions or *Custom* to set each suppression individually.	●		●	
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 　　Enable appointment 　　reminders at non-peak times	Enables users to allow appointment reminders during periods when the device is not synchronizing. Control setting determines whether appointment reminders display during non-peak times.	●		●	
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 categories.	●		●	
Allow copy to phone format options 　　Name format for contacts 　　copied to phone	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. Control setting defines the format in which contacts are copied to the phone from TouchDown Exchange contacts. First MI Last, Last First MI, or File as is	●		●	

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o ZMM	TD/iOS	TD/iOS w/o ZMM
Allow enable appointment reminders option Enable appointment reminders	Allows users to enable appointment reminders. Control setting determines whether a notification displays when an appointment has a reminder.	●		●	
Allow include phone contacts in picklist option Include phone contacts in picklist	Enables users to determine whether the contact list displayed when composing email or SMS includes contacts from the Android Phone Book. Control setting determines whether contacts from the Android phone book are included in the contact picklist that can be accessed while composing email.	●			
Allow normalize phone numbers option Normalize phone numbers	Enables users to determine how contact phone numbers retrieved from the server are formatted. Control setting defines the format of contact phone numbers retrieved from the server as follows: X/x/ext (extension) becomes ; P/p (pause) becomes ; W/w (tone wait) becomes ,	●		●	
Allow reminders configuration Set reminders (in min)	Enables users to configure repeating reminders for calendar events. Use the control setting to configure the repeating reminders. 0 = No repeats; X<0 = reminders start at set reminder time and continue every X minutes until event starts; X>0 = reminders repeat every X minutes after event starts	●		●	
Allow update contact changes to phone option Update contact changes to phone	Enables users to determine whether updates made to contacts in TouchDown also update the phone book database. For iOS devices, updates occur when the user manually synchronizes contacts. Choosing all or some of the fields in the Phone Book > Phone book fields to copy rule is a prerequisite. Determine whether updates made to contacts in TouchDown also update the phone book database. For iOS devices, updates occur when the user manually synchronizes contacts.	●		●	
Suppressions: Device Control					
Allow ActiveSync device type string field ActiveSync device type string	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. Use the control setting to set the ActiveSync device type string to the	●		●	

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o ZMM	TD/iOS	TD/iOS w/o ZMM
field	TouchDown option.				
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.	●			
Allow disable tablet mode (tablet devices only) option	Allows tablet users to disable the automatic switch to tablet mode.	●		●	
Disable tablet mode (tablet devices only)	Use the control setting to disable the automatic switch to Tablet Mode for tablet users.				
Allow exclude attachments from gallery option	Enables users to determine whether Android Gallery scans the SD card for TouchDown media files.	●			
Exclude attachments from gallery	Control setting determines whether or not Android Gallery scans the SD card for TouchDown media files.				
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	Enables users to filter tasks shown on the Home screen and on the Task Widget just as they are on the TouchDown Tasks screen.	●			
Display tasks on home screen and widgets	Control setting determines whether 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.	●		●	
Show email list on startup	Control setting determines whether TouchDown will open to the Email list instead of TouchDown's main screen.				

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o ZMM	TD/iOS	TD/iOS w/o ZMM
Allow use system background data setting option Use system background data setting	Determines whether TouchDown honors how the user has configured the Android *Background Data* setting, which controls whether the app updates in the background or only on demand. When control setting is disabled, TouchDown synchronizes in the background regardless of how the Android *Background Data* setting is configured.	●			
Suppressions: Email					
Allow always BCC myself option Enable always BCC myself option	Enables the user to send a copy of all outgoing emails to his or her own email address. Control setting determines whether a copy of all outgoing email is sent to the user's own email address.	●		●	
Allow choose folders	Enables users to select the folders TouchDown synchronizes 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 Disable SmartReplies and SmartForwards	Enables users to turn off SmartReplies and SmartForwards. Control setting disables the SmartReplies/SmartForwards functionality. This should only be disabled if the server does not support Smart Replies/Forwards.	●		●	
Allow don't delete emails on server option Do not delete email on server	Enables users to prevent email they delete on the device from being deleted on the server. Control setting determines whether email on the server will be deleted when email is deleted on the device.	●		●	
Allow don't mark read on server Do not mark email read on server	Enables users to prevent email, marked read/unread on the device, from being marked as read/unread on the server. Control setting determines whether email marked read/unread on the device will be marked as read/unread on the server.	●		●	
Allow email alerts configuration	Enables users to customize the alerts displayed for new email.	●		●	
Allow email body style options Email body style (Corporate/Individual)	Enables users to choose font, size, color, and style of the HTML email they compose. Use control setting to define the font, size, color, and style of text used for composing HTML email.	●		●	
Allow email checking frequency options Email checking frequency (in	Enables users to determine how often the device checks for new email.	●		●	

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o ZMM	TD/iOS	TD/iOS w/o ZMM
minutes)	When Push Email is not enabled, this control setting defines the frequency at which the device checks the server for new mail. The recommended value is 15 minutes, as more frequent checks can increase battery drain.				
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 Email text size	Enables users to select the text size of email they view. Use the control setting to define the text size for viewing emails.	●		●	
Allow emails to synchronize options	Enables users to set how many days of email to keep on the device.	●		●	
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 Send new mail notifications	Enables users to determine whether a notification displays when new email arrives. Control setting determines whether a notification displays when new mail 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 Clean SD card on remote wipe	Enables users to determine whether all files on the SD card are deleted when a remote Wipe is issued. Control setting determines whether all files on the SD card are deleted when a remote Wipe is issued.	●			
Allow client certs configuration	Enables users to import a client certificate, which TouchDown uses to authenticate with the server.	●			

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o ZMM	TD/iOS	TD/iOS w/o ZMM
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.	●		●	
Remote kill code	Define the designated code that will initiate a 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)	Enables users to choose a device option to erase all TouchDown data and return TouchDown to a pre-registration state.	●		●	
Suppressions: Synchronization					
Allow defer server updates option	Enables users to determine whether TouchDown updates will synchronize to the server in batches or as they occur. Batches are sent only when the next scheduled sync occurs, an item arrives via direct push, or the user initiates a manual sync.	●		●	
Enable defer server updates	When control setting is enabled, TouchDown updates synchronize to the server in batches instead of as they occur. Batches are sent only when 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	Enables users to determine whether a notification displays if synchronization fails due to a user password issue.	●		●	
Send password failure notifications	Control setting determines whether a notification displays if synchronization fails due to a user password issue.				
Allow notify on polling failure option	Enables users to determine whether a notification displays if synchronization has failed.	●		●	
Send failed polling notifications	Control setting determines whether a notification displays if synchronization has failed.				

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o ZMM	TD/iOS	TD/iOS w/o ZMM
Allow notify on successful polling option	Enables users to determine whether a notification displays when synchronization is successful.	●		●	
Send successful polling notifications	Control setting determines whether a notification displays 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	Enables users to determine whether TouchDown synchronizes with the server during non-peak times when email is sent, replied to, or forwarded from the device.	●		●	
Enable polling at off-peak times	Control setting determines whether TouchDown synchronizes with the server during non-peak times when the user sends an email, a reply, or forward from the device.				

SECURITY: ALL DEVICES

Security: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS or TD/iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
Security Commands													
Disable/Enable Device	Device is unmanaged while disabled and thus blocked from all communication with the server. It does not occupy a license seat in this state.	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
Suspend/Resume Device	Device is managed (it can be wiped and continues to send statistics) while suspended, but blocked from corporate resources. User cannot access the application's Config, Mobile Apps, and File Share options and must enter a password to gain full functionality when suspension is lifted.	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
Stop Managing Device	Un-enrolls the device. Un-enrollment selectively wipes the device, removing mail/PIM associated with the mail application, along with any managed apps or profiles; clears the *ZENworks Mobile Management* account; and deletes the device from the grid. Functionality varies by device platform. Android (native): Devices with native mail app only wipe the *ZENworks* account. Mail/PIM is not wiped. Android (TouchDown): Returns TouchDown to a pre-registration state. Erases only the TouchDown data from the SD card. If the *Clean SD Card on Remote Wipe* option in the	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP

Security: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS or TD/iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
	TouchDown *Advanced Settings* is enabled, then the SD card is completely erased. BlackBerry (OS 4.5-7.1): Removes mail and PIM data associated with the NotifySync application. Locks the device if Require Password is enabled. iOS: Removes managed iOS profiles, thus removing corporate resources and managed apps designated to be removed when the APN profile is removed. (Manually created mail profiles and user-installed apps are not removed.) Symbian and WM: Wipes only the *ZENworks* account. Mail/PIM is not wiped. BB10, webOS and WP or any device without the *ZENworks* app: The only action performed is to remove device from the *ZENworks* server and dashboard grid.												
Remove User	Stops managing all devices associated with the user and subsequently removes the user from the *ZENworks Mobile Management* server and dashboard grid.	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
Wipe Storage Card	Administrators or end users can remotely wipe all data from the device's storage card. Android w/native ActiveSync account and Android w/ TouchDown using OS 3.2-4.1.2: Wipes the internal storage card, but does not wipe the external storage card – an OS limitation.	●		●	●						●		

Security: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS or TD/iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
Full Wipe	Administrators or end users can issue a full wipe command. The device remains on the User Grid. Functionality varies by device platform. (Once the device has been wiped, the administrator might also want to issue the *Disable* or *Suspend Device* command to temporarily block the device.) Android w/ native ActiveSync account: 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: 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. 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	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP

Security: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS or TD/iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
	it was in when purchased. Some models (N95 and 6120c) wipe only Mail for Exchange data. 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 the SD card only on Professional devices. BB10, webOS and WP or any device without *ZENworks Mobile Management* app: 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.	●		●	●	●		●			●		
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)					●		●					
Wi-Fi	Sets up Wi-Fi settings, using various levels of security including WEP, WPA, and WPA2.					●		●					

Device Statistics: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS or TD/iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
Status: Last Connections													
Device App	The date and time of the last successful synchronization with the ZENworks Mobile Management server.	●		●	●	●			●		●		
ActiveSync	The date and time of the last successful synchronization with the ActiveSync server.	●	●	●	●	●	●		●	●	●	●	BB10 wOS WP
iOS APN Sent	The last date and time an APN was sent from the Apple Push Notification server.					●		●					
iOS APN Check-In	The last date and time the device acknowledged an APN from the Apple Push Notification server.					●		●					
Status: Battery													
Level	Displays the percentage of battery life left for the device.	●		●	●	●		●	●		●		
Status	Displays whether the device battery is charging or unplugged.	●		●	●	●		●	●		●		
Last Boot Time	The date and time of the last device boot.	●		●	●	●					●		
Status: Encryption													
Device Encrypted	Whether the data stored in the device's local memory is encrypted.	●	●	●	●	●	●				●		
Storage Card Encrypted	Whether the data stored on the device's storage card is encrypted. iOS devices do not have SD card capability.			●							●	●	

Device Statistics: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS or TD/iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
Status: Device Memory													
Capacity	Displays the total of the used and unused memory on the device.	●		●	●	●		●	●		●		
Available	Displays the amount of free memory left on the device. (Labeled Available Device Capacity for iOS devices.)	●		●	●	●		●	●		●		
Percent Free	Displays the percentage of free memory left on the device.	●		●	●	●		●	●		●		
Status: External Storage Card													
Capacity	Displays the total of the used and unused memory on the device storage card. iOS devices do not have SD card capability.	●		●	●				●		●		
Available	Displays the amount of free memory left on the device's storage card. iOS devices do not have SD card capability.	●		●	●				●		●		
Percent Free	Displays the percentage of free memory left on the device's storage card. iOS devices do not have SD card capability.	●		●	●				●		●		
Status: Jailbroken													
Jailbroken	Whether or not an iOS or Android device has been jailbroken/rooted.	●		●		●							
Status: TouchDown													
TouchDown Registered	Whether the TouchDown application is registered on an Android device.	●		●									
Status: Roaming													
Currently Roaming	Displays a simple yes or no if the device is roaming.	●		●	●	●		●	●		●		
Voice Roaming Enabled	Current setting for Voice Roaming.					●		●					

Device Statistics: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS or TD/iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
Data Roaming Enabled	Current setting for Data Roaming.					●		●					
Network: Downloaded Data													
Any	Data usage statistics for data coming in to the device over the network since the last device boot time. The sum-total of all networks. BlackBerry with NotifySync: Limited to GSM devices.	●		●	●	●				●			
Cellular	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.	●		●		●				●			
Network: Uploaded Data													
Any	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.	●		●	●	●				●			
Cellular	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.	●		●		●				●			
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.	●		●		●				●			
Network: Network Details													
Network Type	Displays the network type the device is using.	●		●	●	●		●	●		●		

Device Statistics: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS or TD/iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
Signal Strength	Displays the signal strength using a percentage value.	●		●	●				●		●		
SIM Card IMSI Number	The ID number of the SIM card: International Mobile Subscriber Identity.	●		●	●						●		
Cellular Technology	Cellular technology 0 = none 1 = GSM 2 = CDMA					●		●					
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.					●		●					
About: Device Application													
Device Application Version	Displays the version number of the ZENworks Mobile Management device application.	●		●	●	●			●		●		
Device Application Language	Name of the language the ZENworks Mobile Management device application is using.	●		●	●	●			●		●		
About: ActiveSync													
ActiveSync: Version	ActiveSync protocol version used by the device.	●	●	●	●	●	●		●	●	●	●	BB10 wOS WP
ActiveSync: User Agent	The device's native ActiveSync application version, which corresponds to the device's operating system version.	●	●	●	●	●	●		●	●	●	●	BB10 wOS WP
About: Operating System													
Operating System: Language	Name of the language the device OS is using.	●		●	●				●		●		

Device Statistics: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS or TD/iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
Operating System: Version	Displays the device OS version.	●		●	●	●		●	●		●		
About: Device													
Model	Device's internal model number.					●		●					
Model Name	Name of the device model.					●		●					
Device Name	The name given via iTunes.					●		●					
Ownership	Tracks whether the device is a company device or personal device.	●		●	●	●		●	●		●		
Platform	Displays the device platform type as reported by the device.	●		●	●	●		●	●		●		BB10
UID	Displays the device UID. Symbian: The device UID is the same as the device IMEI.				●			●	●		●		
IMEI	The International Mobile Equipment Identify number. See http://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity BlackBerry with NotifySync: Limited to GSM devices.	●		●	●	●		●	●		●		
Phone Number	Displays device phone number.	●		●	●	●		●			●		
Time Zone	The time zone setting on the device.	●		●	●	●					●		
GMT Offset	The time difference between the device's time zone and Greenwich Mean Time.	●		●	●	●					●		
Build Version	iOS build number.					●		●					
Product Name	The model code for the device.					●		●					
Serial Number	The device's serial number.					●		●					
Modem Firmware Version	The baseband firmware version.					●		●					
MEID	The device's MEID (CDMA).					●							
ICCID	The ICC identifier for the installed SIM card (if applicable).					●		●					
Bluetooth MAC	Bluetooth MAC address.					●		●					
Wi-Fi MAC	Wi-Fi MAC address.					●		●					

Device Statistics: All Devices	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS or TD/iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
Subscriber MCC	Home Mobile Country Code					●		●					
Subscriber MNC	Home Mobile Network Code					●		●					
Current MCC	Current Mobile Country Code					●		●					
Current MNC	Current Mobile Network Code					●		●					

COMPLIANCE MANAGER

Compliance Manager	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
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.	●	●	●	●	●	●	●		●	●	●	●	BB10 wOS WP
Restrict ActiveSync protocol	A device cannot support sufficient ActiveSync policies, because of ActiveSync version support limitations with the device or server.	●	●	●	●	●	●	●		●	●	●	●	BB10 wOS WP
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.	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
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	BB10
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.	●		●	●	●	●					●		

Compliance Manager	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
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	NA
Restrict user ActiveSync connections	A device's Last ActiveSync Sync time stamp has not updated within the set interval.	●	●	●	●	●	●	●		●	●	●	●	BB10 wOS WP
Restrict when Blacklist App detected	A device has a blacklisted application installed.	●		●		●	●	●	●					
Restrict when non-Whitelist App detected	A device has an application that does not match the whitelist criteria.	●		●		●	●	●	●					
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.	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
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.	●	●	●	●	●	●	●	●	●	●	●		BB10 wOS WP
Restrict if location services are off	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.	●		●	●	●	●		NA	●		●		
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.	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
Restrict rooted devices	A rooted Android device connects to the	●		●	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA

Compliance Manager	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
	server.													
Restrict jailbroken devices	A jailbroken iOS device connects to the server.	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
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
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
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
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
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
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	NA	NA	NA	NA	●	●			NA	NA	NA	NA	NA

Compliance Manager	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
	fallen below a specified amount.													
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.	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
Organization-wide ActiveSync connectivity	The Last ActiveSync Sync time stamp has not updated for any users within the set interval.	●	●	●	●	●	●	●		●	●	●	●	BB10 wOS WP
Organization-wide ZENworks connectivity	The Last ZENworks Sync time stamp has not updated for any users within the set interval.	●		●	●	●	●			●		●		BB10
Watch List	A user or policy suite on the Watch List grid has exceeded the time for which it was being monitored.	●	●	●	●	●	●	●		●	●	●	●	BB10 wOS WP
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.	●	●	●	●	●	●	●		●	●	●	●	BB10 wOS WP
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
Reset for Enrollment	An administrator has issued a *Reset for Enrollment* command from the dashboard to a device.	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
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
Full wipe issued by Admin	An administrator has issued a Full Wipe command from the dashboard to a device.	●	●	●	●	●	●	●	●	●	●	●	●	BB10 wOS WP
Full wipe issued by user	A user has issued a Full Wipe command from the User Self Administration Portal	●	●	●	●	●	●	●		●	●	●	●	BB10 wOS

Compliance Manager	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
	to their device.													WP
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.	●		●	●	●	●					●		
New Hands-Off Enrolled device	Any time a new device uses Hands-Off enrollment to connect to the system.	●	●	●	●	●	●	●		●	●	●	●	BB10 wOS WP
New Hands-Off Enrolled user	Any time a new user uses Hands-Off enrollment to connect to the system.	●	●	●	●	●	●	●		●	●	●	●	BB10 wOS WP
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.	●	●	●	●	●	●	●		●	●	●	●	BB10 wOS WP
Stop managing device issued by Admin	An administrator has issued a *Stop Managing Device* command from the dashboard to a device.	●		●	●	●	●		●	●		●		BB10 wOS WP
Stop managing device issued by user	A user has issued a *Stop Managing Device* command from the User Self Administration Portal to a device.	●		●	●	●	●			●		●		BB10 wOS WP
TouchDown policy override	The system issues a warning if it detects	NA	NA	●	NA	NA		NA	NA	NA	NA	NA	NA	NA

Compliance Manager	Description	Anrd	Anrd w/o ZMM	TD/A	NS/BB	iOS	TD/ iOS	iOS w/o ZMM	iOS Config Devices	S60	S60 w/o ZMM	WM	WM w/o ZMM	AS Only
detection	that a user has overridden the TouchDown settings governed by ZENworks Mobile Management.													
User restricted	A user becomes restricted for any reason.	●	●	●	●	●		●	●	●	●	●	●	BB10 wOS WP
Wipe storage card	An administrator has issued a Wipe Storage Card command from the dashboard to a device.	●		●	●	NA		NA	NA			●		
System Alerts														
Apple Push Notification (APNs) Certificate Expiration	Enable and set parameters to keep track of the APNs certificate expiration. Default settings are to issue the reminder 30 days prior to the expiration and repeat it every day.	NA	NA	NA	NA	●	●	●	●	NA	NA	NA	NA	NA