

Functionality by Device Platform

ZENworks® Mobile Management 3.2.x

November 2015

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 \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

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

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

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

Novell Trademarks

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

Third-Party Materials

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

TABLE OF CONTENTS

Policy Rules: All Devices	6
Policy Rules: iOS Devices	19
Policy Rules: KNOX Devices	30
Policy Rules: TouchDown	36
Policy Rules: Windows Devices	48
User Self-Administration Portal (USAP)	51
Security Actions: All Devices	54
Device Statistics: All Devices	59
Compliance Manager	66

Expanded Table of Contents

► Policy Rules: All Devices

Audit Tracking

Device Control

- [Device Features](#)
- [Email](#)
- [ActiveSync Synchronization](#)
- [Applications](#)

File Share Permissions

Resource Control

Security Settings

- [Password](#)
- [Encryption](#)
- [Device Inactivity and Locking](#)
- [Emergency Calls](#)

S/MIME Settings

Whitelists/Blacklists Permissions

► Policy Rules: Samsung KNOX

- [Samsung KNOX Device Policies](#)
- [Samsung KNOX Workspace Policies](#)

► Policy Rules: iOS Device

- [Device Features](#)
- [Applications](#)
- [Safari Browser](#)
- [Ratings](#)
- [Security](#)
- [iCloud](#)
- [Management](#)
- [Supervised Mode](#)

► Policy Rules: TouchDown

- [Installation](#)
- [General](#)
- [Signature](#)
- [Widgets](#)
- [Phone Book](#)
- [User Configurable Settings](#)
- [Suppression Rules](#)

► Policy Rules: Windows Devices

- [Applications](#)
- [Device Features](#)
- [Management](#)
- [Passport for Work](#)

► User Self-Administration Portal (USAP)

- [iOS Security Actions](#)
- [Android Security Actions](#)
- [Device Statistics](#)
- [iOS Applications](#)
- [Android Applications](#)

Certificates

► 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 Alerts](#)
- [Event Based Alerts](#)
- [System Alerts](#)

The information in these tables describes functionality supported by each device platform for *ZENworks Mobile Management*, version 3.0.x.

Device platforms supported by *ZENworks Mobile Management* are Android, BlackBerry (4.5-7.1) with *GO!NotifySync*, BlackBerry (OS 10), iOS, webOS, Windows Devices 8.1+, and Windows Phone. Supported device operating system versions are listed below.

Anrd	TD/A	BB10	NS/BB	iOS	TD/iOS	Windows	wOS	WP
								
Android devices OS v2.2 – 5.1	Android devices OS v2.2 – 5.1 with TouchDown v8.4.x or 8.5.x	BlackBerry Devices OS 10	BlackBerry devices OS v4.5 – 7.1 with <i>GO!NotifySync</i> v4.9 or greater	iOS 6.0 – 9.1 multitasking devices	iOS 6.0 – 9.1 multitasking devices with latest TouchDown app version	Windows Devices OS 8.1 Windows PCs & tablets OS 10	WebOS devices OS v1.4.3/1.4.5, 2.0.0/2.0.1, 2.1.2	Windows Phone devices OS v7,7.5, 8

The ZENworks Mobile Management Device Application

Android and iOS devices use the *ZENworks Mobile Management* device application to provide additional functionality and enforce policies that are not handled by ActiveSync. The *GO!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 *GO!NotifySync* license.)

The device platforms listed above also require a native ActiveSync protocol or an application that uses the ActiveSync protocol, such as *GO!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), *GO!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 *GO!NotifySync* license.)
- On **iOS 6, 7, 8, 9** devices with multitasking capabilities, the ActiveSync policies are enforced by using Apple configuration profiles.
- Windows 8.1+ - phones and tablets with OS 8.1+ or tablets and PCs with OS 10.

Enrolling Android or iOS 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 ((OS 4.5-7.1) do not have native ActiveSync capabilities and are not supported without the *GO!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** functionality – The device does not have the ZENworks Mobile Management app and supports 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 GO!NotifySync app.

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Windows	Active- Sync only
Audit Tracking										
Archive Device File List	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 Device Profile: File Archive	•		•	•					
Record Phone Log	Requires the device to send all telephone log information to the server. For BlackBerry devices with GO!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 GO!NotifySync: Do not track MMS messages Track only texts made after ZENworks 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.)	•		•	•					
Record Installed Applications	Requires the device to send app information with data usage statistics for all applications installed on the device. Usage statistics are displayed in the Apps section of the Device Profile.	•		•						

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Windows	Active- Sync only
Record Managed Applications	Requires the device to send app information with data usage statistics for managed applications. Usage statistics are displayed in the Apps section of the Device Profile.	•		•						
Record Location of Device (Latitude / Longitude)	<p>When device GPS service is on, uses GPS or triangulation to locate a user's device. Information is displayed using Google Maps. The device reports longitude and latitude as two separate values.</p> <p>This setting will be automatically replicated in the user self-administration portal (USAP) permission, <i>Display Locate Device</i>.</p> <p>KNOX devices: If the device's GPS Service is off, enabling this will turn the GPS service on and return the device's current location to the server.</p> <p>iOS devices support this only when the MDM App is installed on the device. Instruct users to set <i>Settings > MDM > Privacy > Location Services > Allow Location Access</i> to "Always" on the device.</p> <p>Windows devices: Require Windows OS 10 or higher</p>	•		•	•	•	•	•		
GPS Location Accuracy	<p>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.</p> <p>iOS devices support this only when the MDM App is installed on the device.</p> <p>Windows devices: Require Windows OS 10 or higher</p>	•		•	•	•	•	•		
Device Controls: Device Features										
Allow Bluetooth (ActiveSync)	<p>Determines whether Bluetooth is allowed to operate on the device.</p> <p>There are three settings:</p> <p>Don't allow Bluetooth</p> <p>Allow only Bluetooth headsets</p> <p>Allow all Bluetooth</p> <p>Android devices: Requires KNOX compatibility. "Handsfree" functions the same as the "Allowed" option on KNOX devices.</p>	•		•				•		

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Windows	Active- Sync only
	Windows devices: When MDM proxy is not on, "Handsfree" functions the same as the "Allowed" option.									
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. Android devices: Enforced through the device app on select Android devices and those supporting KNOX.	•				•	•	•		
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 KNOX Standard compatible devices.	•	•	•		•	•	•	•	
Allow GPS	Determines whether the device will allow the use of GPS.								•	
Allow Infrared (ActiveSync)	Determines whether infrared connections are allowed to and from the device. This feature may only be supported by ActiveSync only devices using a third-party email client that supports it.									
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. This feature may only be supported by ActiveSync only devices using a third-party email client that supports it.								•	
Allow NFC	Determines whether the device will allow Near Field Communication.								•	
Allow Remote Desktop (ActiveSync)	Determines whether a remote desktop connection can be created from the device. This feature may only be supported by ActiveSync only devices using a third-party email client that supports it.									
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. This feature may only be supported by ActiveSync only devices using a third-party email client that supports it.									

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Windows	Active- Sync only
Allow Text Messaging (ActiveSync)	Determines whether the device can send or receive text messages. This feature may only be supported by ActiveSync only devices using a third-party email client that supports it.									
Allow USB	Determines whether the device will allow a USB connection.								•	
Allow Wi-Fi (ActiveSync)	Determines whether wireless Internet access is allowed on the device. Android devices: Requires KNOX compatibility. Windows devices: Require OS 8.1 or higher.	•						•	•	
Allow user to remove enrollment	Determines whether the user is permitted to remove the MDM user account from the device.	•		•		•	•		•	
Initiate Selective Wipe when user removes MDM app account	If the user removes the MDM account on the device, a selective wipe is executed. Selective Wipe functionality varies by device platform.	•		•		•	•	•		
Allow Screen Capture	Determines whether the device will allow the user to take screenshots. This policy can only be enforced when the MDM device agent is provisioned as a device owner or profile owner app. (Enable the <i>Provision Managed Profile</i> policy under <i>Resource Control</i> OR use NFC to provision the MDM device agent as the Device Owner.) Requires Android OS version 5.0+	•		•					•	
Disable Fingerprint	Determines whether the device will allow the user to use the finger print reader. Requires Android OS version 5.0+	•		•						
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.									

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Windows	Active- Sync only
	This feature may only be supported by ActiveSync only devices using a third-party email client that supports it.									
Allow POP/IMAP Email (ActiveSync)	Determines whether the device can access POP3 or IMAP4 email. This feature may only be supported by ActiveSync only devices using a third-party email client that supports it.									
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
Specific calendar age for synchronization	Determines a specific number of calendar days that can be synchronized. The value should be lower than the <i>Maximum calendar age for synchronization</i> .			•			•			
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
Specific Email age for synchronization	Determines a specific age for emails to synchronize. The value should be lower than the <i>Maximum Email age for synchronization</i> .			•			•			
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 Controls: Applications										
Allow Copy and Paste	Determines whether the users is able copy and paste across applications.								•	
Allow Unsigned Applications	Determines whether unsigned applications which already exist on the device are permitted to run.	•								

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Windows	Active- Sync only
Allow Unsigned Package Installation	Determines whether the device permits unsigned installers to install applications.	•								
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.	•		•	•	•	•	•		
Whitelists/Blacklists Permissions	<p>Create a list of strings that will filter either by blacklisting or whitelisting applications.</p> <p>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.</p> <p>Whitelist – When one or more applications are installed on a device that are not on the Whitelist, the user's access to email, shared files, app lists, or other organization resources can be blocked.</p> <p>Android KNOX and KNOX Workspace compatible devices: Blacklist/Whitelist restrictions will prevent apps that do not meet the criteria from being installed on the device. Workspace devices require KNOX v2.0 and prevent installation only in the container.</p>	•		•		•	•	•		
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.	•		•	•	•	•	•		
Allow Managed Apps	<p>Determines whether users are permitted to access the Managed Apps list.</p> <p>This setting will be automatically replicated in the user self-administration portal (USAP) permissions, <i>Display Managed Apps</i>.</p>	•		•	•	•	•	•		
Provision Managed Profile	Determines whether a Managed Profile is installed on Android devices. When a Managed Profile exists, all MDM managed apps are installed inside the profile. This allows an administrator to remove the profile and apps with a selective wipe if necessary. Applications installed outside of the	•		•						

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Windows	Active- Sync only
	Managed Profile will not be removed when the Managed Profile is removed. Notes: 1) Some device modes may not support managed profile installation. 2) Enabling managed profile installation will require full device encryption. 3) Managed Profile won't be activated if the TouchDown app is enrolled. Requires Android OS version 5.0+									
Remove Managed Profile	Determines whether the managed profile will be removed from the device when the <i>Provision Managed Profile</i> policy settings changes from Yes to No. When enabled, a selective wipe is also issued when the <i>Provision Managed Profile</i> policy changes from Yes to NO. Requires Android OS version 5.0	•		•						
Security: Password										
Require Device Password (ActiveSync)	Forces the device to require a password to unlock the device.	•	•	•	•	•	•	•	•	BB10 wOS WP
Require TouchDown PIN	Determines whether a PIN is required to access the TouchDown app. Can be used in addition to or in place of the <i>Require Device Password</i> option.			•			•			
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 as Exchange 2003.	•	•	•	•	•	•	•	•	WP
Require Minimum Password Length (ActiveSync)	Forces the device to require a password with a specified minimum length.	•	•	•	•	•	•	•	•	BB10 wOS WP

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Windows	Active- Sync only
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, selected OS 2.x devices, and KNOX Standard compatible devices. For BlackBerry w/ GO!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.	•	•	•						
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. Android: Supported on devices with OS 3.0, selected devices with OS 2.x, and KNOX Standard compatible devices. BlackBerry 10: Not supported on Q5 and Z30	•	•	•	•	•	•	•		BB10 WP

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Windows	Active- Sync only
Password expiration in days (ActiveSync)	<p>Defines the number of days a password can be used before it expires.</p> <p>Android: Supported on devices with OS 3.0, selected devices with OS 2.x, and KNOX Standard compatible devices.</p> <p>BlackBerry 10: Not supported on Q5 and Z30</p>	•	•	•	•	•	•	•	•	BB10 WP
Require Device Password History (ActiveSync)	<p>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.</p> <p>Android (native): Supported on devices with OS 3.0, selected OS 2.x devices, and KNOX Standard compatible devices.</p> <p>Android w/ TouchDown: Applies to the password associated with the TouchDown application only.</p> <p>BlackBerry 10: Not supported on Q5 and Z30</p>	•	•	•	•	•	•	•	•	BB10 WP
Number of passwords stored (ActiveSync)	<p>Defines the number of device passwords stored to prevent users from reusing them too soon.</p> <p>BlackBerry 10: Not supported on Q5 and Z30</p>				•	•	•	•		BB10 WP
Enable Password Echo	<p>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.</p>				•					
Begin password echo after attempts	<p>Defines the number of unlock attempts before echoing begins.</p>				•					
Require numeric complex password	<p>Determines whether the device will allow the user to enter a password that has repeating numeric sequences, such as 4444, 1234.</p> <p>Requires Android OS version 5.0+</p>	•		•						
Security: Encryption										
Require Encryption on the Device (ActiveSync)	<p>Determines whether the device encrypts stored data.</p> <p>Not supported with systems operating with ActiveSync protocol 2.5, such as Exchange 2003.</p> <p>iOS devices (iPhone and iPad) have hardware encryption that is always enabled. The ActiveSync policy is not used to enable/disable.</p>	•	•	•	•	•	•	•	•	BB10

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Windows	Active- Sync only
	<p>Android (native): Supported on the Motorola Droid Pro (OS 2.2), devices with OS 3.0.0 or greater, and KNOX Standard compatible devices. Gives repeated reminders until the user initiates encryption.</p> <p>Android w/ TouchDown, TouchDown data is encrypted (email, calendar, contacts, tasks). Use <i>Require TouchDown encryption</i> instead, to require encryption of TouchDown data only. Gives repeated reminders until the user initiates encryption.</p> <p>GO!NotifySync for BlackBerry: only GO!NotifySync data is encrypted (email).</p> <p>Windows 10 desktop: For encryption of a local or internal data drive, <i>BitLocker</i> must be enabled on a desktop computer. Follow the instructions at http://www.howtogeek.com/howto/6229/how-to-use-bitlocker-on-drives-without-tpm/</p>									
<p>Require Encryption on the Storage Card</p> <p>(ActiveSync)</p>	<p>Forces the device to encrypt the file system of a storage card.</p> <p>Android: Requires KNOX Standard compatibility. The device will not prompt the user to encrypt the SD card until a reboot of the device is performed.</p> <p>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).</p>	•		•						BB10
Security: Device Inactivity and Locking										
<p>Require Max Inactivity Time Device Lock</p> <p>(ActiveSync)</p>	<p>Forces the device to lock after a set number of minutes of user inactivity. This value serves as a maximum.</p> <p>This is also known as “Time without user input before password must be re-entered.”</p>	•	•	•	•	•	•	•	•	BB10 wOS WP
<p>Max Inactivity Timeout (in minutes)</p> <p>(ActiveSync)</p>	<p>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.</p>	•	•	•	•	•	•	•	•	BB10 wOS WP
<p>Require Device Challenge Timeout</p>	<p>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.</p>				•					

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Windows	Active- Sync only
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.				•	•	•	•		
Customizable lock message	Enter text to be displayed when device locks.				•	•	•	•		
Lock message phone number	Enter a contact phone number to be displayed when the device locks. A user can tap the displayed phone to initiate dialing. Requires iOS 7 or later.					•	•	•		
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-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. Android: Requires KNOX Standard compatibility. iOS: If Touch ID is enabled on the device, <i>Maximum grace period</i> is set to <i>Immediately</i> since the user can easily access the device with a fingerprint scan. An administrator can block the use of Touch ID by disabling <i>Allow fingerprint for unlock</i> .	•				•	•	•		
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 GO!NotifySync application and removes the GO!NotifySync account. Locks the device if Require	•	•	•	•	•	•	•		BB10 wOS WP

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Windows	Active- Sync only
	<p>Password is enabled. Erases GO!NotifySync data from the SD card, including saved attachments.</p> <p>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.</p> <p>BB10, webOS and WP or any device without <i>ZENworks Mobile Management</i> app: 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.</p>									
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 MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Windows	Active- Sync 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 Super- vised 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. <i>Require Password</i> 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 Global Background Fetch while 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 Screenshot	Determines if the device will allow screenshots and screen recordings.	•	•	•
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.	•	•	•
Enable Siri Profanity Filter	Determines whether profanity is filtered on the device. <i>Allow Siri</i> must be enabled in order to enable this policy. Functional on devices in Supervised mode only.			•
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 <i>Allow Multiplayer Gaming</i> and <i>Allow Adding Game Center Friends</i> .			•

Policy Suite Rules: iOS	Description	iOS	TD/ iOS	iOS Super- vised devices
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.	•	•	•
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.	•	•	•
Allow Over-the-Air PKI Updates	Determines if over-the-air if Public Key Infrastructure (PKI) updates are permitted. Requires iOS 7 or later.	•	•	•
Force Limited Ad Tracking	Determines if advertisers' tracking of a user's habits is limited. Enabling this does not eliminate ad tracking, but may reduce it to some degree. Requires iOS 7 or later.	•	•	•
Force Unmanaged Air Drop	Determines whether AirDrop is an unmanaged drop target. When enabled, sharing managed documents using AirDrop is not allowed. Requires iOS 9.0 or greater	•	•	•
Force Watch Wrist Detection	Determines whether Apple Watch will lock automatically when removed from the wrist. Requires iOS 8.2 or greater	•	•	•
Allow Fingerprint for Unlock	Determines whether the user's Touch ID can be used to unlock the device. iOS 7 or later required	•	•	•
Allow Lock Screen Control Center	Determines whether Control Center appears on the Lock screen. Control Center appears with a swipe up from any screen giving the user quick access to controls and apps. iOS 7 or later required	•	•	•
Allow Lock Screen Notification View	Determines whether the Notifications view in Notification Center can be accessed from the Lock screen.	•	•	•

Policy Suite Rules: iOS	Description	iOS	TD/ iOS	iOS Super- vised devices
	iOS 7 or later required			
Allow Lock Screen Today View	Determines whether the Today view in Notification Center can be accessed from the Lock screen. iOS 7 or later required	•	•	•
Applications				
Allow App Management	Determines whether an administrator has the ability to give user access to iOS apps or force push iOS apps to users in a particular policy suite. iOS Configurator devices: Apps can only be made available on the device by an administrator via force push.	•	•	•
Allow Activity Continuation	Determines whether the device will allow activity continuation.	•	•	•
Allow App Store	Determines whether an iOS device will allow users to install applications. When disabled, the App Store is disabled and the icon is removed from the device Home screen.	•	•	•
Allow Managed Application Installation	Determines whether iOS 7 or greater devices will allow users to install recommended or required applications even if the <i>Allow App Store</i> policy has been disabled.	•	•	•
Allow Bookstore	When disabled, iBookstore is disabled 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 Enterprise Books Backup	Determines whether the device will allow backups of Enterprise books.	•	•	•
Allow Enterprise Books Metadata Backup	Determines whether the device will allow backups of Enterprise books, notes and highlights.	•	•	•
Allow In App Purchases	Determines whether or not users can make in-app purchases.	•	•	•
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.	•	•	•
Allow Managed App Documents to Open in Unmanaged Apps	Determines if documents in managed apps and accounts will only open in other managed apps and accounts. Requires iOS 7 or later.	•	•	•
Allow Unmanaged App Documents to Open in Managed Apps	Determines if documents in unmanaged apps and accounts will only open in other unmanaged apps and accounts.	•	•	•

Policy Suite Rules: iOS	Description	iOS	TD/ iOS	iOS Super- vised devices
	<p><i>Note:</i> When disabled, this setting prevents users from attaching photos from the iPhone camera roll.</p> <p>Requires iOS 7 or later.</p>			
Record Installed Applications	Access and record applications installed on devices.	•	•	•
Force pairing password for outgoing AirPlay requests	<p>Determines whether a pairing password is requested from any device receiving AirPlay requests from an MDM device (an MDM device attempting to stream media to other AirPlay-enabled devices on the same Wi-Fi network.)</p> <p>Requires iOS 7.1 or later.</p>	•	•	•
Safari Browser				
Allow Safari	<p>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.</p> <p>Allow Browser in the Device Controls must also be enabled.</p>	•	•	•
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 from visiting Websites identified as being fraudulent or compromised.	•	•	•
Ratings				
Rating Region	Determines the media content rating scale used by a particular region. If rating restrictions are enabled, items that violate the restrictions cannot be downloaded over-the-air and those installed via iTunes are hidden. Items violating the restriction that existed on the device before rating restrictions were imposed will be hidden.	•	•	•
Application Ratings	Determines the maximum allowed ratings for apps. If rating restrictions are enabled, applications that violate the restrictions cannot be downloaded over-the-air and those installed via iTunes are hidden. Applications violating the restriction that existed on the device before rating restrictions were imposed will be hidden. Caution: If you choose the Don't Allow Apps option, the <i>ZENworks Mobile Management</i> app will be hidden on iOS devices.	•	•	•

Policy Suite Rules: iOS	Description	iOS	TD/ iOS	iOS Super- vised devices
	<p>Rating settings determine the highest rating permissible. For example a policy with the U.S. application rating of 9+ will allow the installation of applications with a rating of 4+ or 9+, but will block applications with a rating of 12+ or 17+.</p> <p>Note: Set to “Allow All” to allow users to install VPP apps without having to enter their Apple ID credentials.</p>			
Movie Ratings	<p>Determines the maximum allowed ratings for movies. If rating restrictions are enabled, movies that violate the restrictions cannot be downloaded over-the-air and those installed via iTunes are hidden. Movies violating the restriction that existed on the device before rating restrictions were imposed will be hidden.</p>	•	•	•
TV Show Ratings	<p>Determines the maximum allowed ratings for TV shows. If rating restrictions are enabled, TV shows that violate the restrictions cannot be downloaded over-the-air and those installed via iTunes are hidden. TV shows violating the restriction that existed on the device before rating restrictions were imposed will be hidden.</p>	•	•	•
Security				
Allow Untrusted TLS Prompt	<p>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.</p>	•	•	•
Allow Diagnostic Submission Text	<p>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.</p>	•	•	•
Managed Domains	<p>Managed mail domains list and the managed Safari domains list are enabled only when the managed domains policy is enabled.</p> <p>Requires iOS 8.0 or higher.</p>	•	•	•
Managed Email Domains	<p>Recipient email addresses from unmanaged domains entered in this list will be highlighted in the Mail app.</p> <p>Requires iOS 8.0 or higher.</p>	•	•	•
Managed Safari Domains	<p>Documents originating from managed domains entered in this list can only be opened within Safari.</p> <p>Requires iOS 8.0 or higher.</p>	•	•	•
iCloud				
Allow iCloud Backup	<p>Determines whether the device is permitted to back up to and restore from iCloud.</p>	•	•	•

Policy Suite Rules: iOS	Description	iOS	TD/ iOS	iOS Super- vised devices
Allow iCloud Keychain Sync	Determines if iCloud Keychain sync is permitted. Stores 256-bit AES encrypted user passwords in iCloud so they can be synced across trusted devices. Helps users create strong passwords. Requires iOS 7 or later.	•	•	•
Allow iCloud Photo Library	Determines whether photos in iCloud can be accessed on the device. Requires iOS 9.0 or greater	•	•	•
Allow Document Sync	Determines whether the device allows document synchronization to iCloud. When this option is enabled, users can store documents in iCloud.	•	•	•
Allow managed apps cloud sync	Determines whether the device allows cloud sync for managed apps.	•	•	•
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.	•	•	•
Management				
Allow Management of Settings	Determines whether the voice roaming, data roaming, and personal hotspot settings can be managed. When disabled, users can configure these settings on the device. Requires iOS 7 or higher.	•	•	•
Allow Voice Roaming	Determines whether the device will allow voice calls and SMS messages while roaming. If <i>Allow Management of Settings</i> is disabled, user determines the setting. If <i>Allow Management of Settings</i> is enabled, a user might still be able to configure this setting on the device (depending on OS version), but it will revert back to the configuration sent from the server each time the device synchronizes. Requires iOS 7 or higher.	•	•	•
Allow Data Roaming	Determines whether the device will allow data or video while roaming.	•	•	•

Policy Suite Rules: iOS	Description	iOS	TD/ iOS	iOS Super- vised devices
	<p>If <i>Allow Management of Settings</i> is disabled, user determines the setting. If <i>Allow Management of Settings</i> is enabled, a user might still be able to configure this setting on the device (depending on OS version), but it will revert back to the configuration sent from the server each time the device synchronizes.</p> <p>Requires iOS 7 or higher.</p>			
Enable personal hotspot	<p>Enables the personal hotspot feature on user devices, which allows the user to connect computers and other devices to the Internet using the device's cellular data connection.</p> <p>If <i>Allow Management of Settings</i> is disabled, user determines the setting. If <i>Allow Management of Settings</i> is enabled, a user might still be able to configure this setting on the device (depending on OS version), but it will revert back to the configuration sent from the server each time the device synchronizes.</p> <p>Requires iOS 7 or later.</p>	•	•	•
Supervised Mode				
Allow Account Modification	<p>Determines whether the user can modify the iTunes & App Stores account.</p> <p>Requires iOS 7 or later.</p>			•
Allow Activation Lock	<p>Determines whether a user will be able to lock the activation of the device (also known as bricking the device) via the <i>Find My Phone</i> app.</p> <p>Requires iOS 7 or later.</p>			•
Allow AirDrop	<p>Determines whether AirDrop is enabled or disabled. AirDrop allows users to easily share, via Wi-Fi or Bluetooth, photos, videos, contacts or anything else from any app with a Share button.</p> <p>iOS 7 or later required</p>			•
Allow App Cellular Data Modification	<p>Determines whether changes to cellular data usage settings for apps are permitted.</p> <p>Requires iOS 7 or later.</p>			•
Allow App Removal	<p>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.</p>			•

Policy Suite Rules: iOS	Description	iOS	TD/ iOS	iOS Super- vised devices
Allow Assistant User Generated Content	Determines whether Siri can query web sources, such as Bing, Wikipedia, and Twitter, to answer user questions. iOS 7 or later required			•
Allow Auto Correction	Determines whether the device allows auto correction of keyboard entries.			•
Allow Automatic App Downloads	Determines whether the device is permitted to download apps automatically.			•
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 Definition Lookup	Determines whether the use of word definition features are permitted.			•
Allow Device Name Modification	Determines whether a user can change the device name.			•
Allow Enterprise App Trust	Determines whether the device is permitted to trust enterprise apps.			•
Allow Find My Friends Modification	Determines whether changes to Find My Friends settings are permitted. Allows users to locate friends and family that also have the Find My Friends app. Requires iOS 7 or later.			•
Allow Full Wipe via Device	Determines whether the device enables the <i>Erase All Content and Settings</i> under <i>Reset UI</i> on the device.			•
Allow Host Pairing	Determines whether host pairing, other than the supervision host, is disabled. If a supervision host has not been configured, all pairing is disabled. Requires iOS 7 or later.			•
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.			•
Allow Keyboard Shortcuts	Determines whether the device permits the use of keyboard shortcuts for onscreen menus.			•
Allow Paired Watch	Determines whether a device can pair with an Apple Watch.			•
Allow Passcode Modification	Determines whether a user can change the device passcode.			•
Allow Predictive Keyboard	Determines whether the use of Predictive Keyboard is permitted.			•

Policy Suite Rules: iOS	Description	iOS	TD/ iOS	iOS Super- vised devices
Allow Spell Check	Determines whether the device permits the use of spell check.			•
Allow Spotlight Results	Determines whether <i>Spotlight</i> will return Internet search results.			•
Allow user to change restrictions	Determines whether the device enables the <i>Enable Restrictions</i> option under <i>Restrictions UI</i> in the device Settings.			•
Allow Wallpaper Modification	Determines whether the user can change the device wallpaper.			•
Global HTTP Proxy	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.			•
Content Filter	Web content filter policies (<i>Auto Filter</i> , <i>Permitted URLs</i> , and <i>Blacklisted URLs</i>) for iOS 8+ devices are enabled only when <i>Content Filter</i> is enabled. Requires iOS 8.0 or later.			•
Filter Type	Choose <i>Blacklisted/Permitted URLs</i> and enter URLs to be blocked or choose <i>Whitelisted Bookmarks</i> and enter bookmarks for the URLs to which the device is limited.			•
Auto Filter Inappropriate Web Sites	When <i>Filter Type</i> is Blacklisted/ Permitted URLs , this determines whether web sites with content inappropriate for children are blocked. Requires iOS 8.0 or later.			•
Permitted URLs	When <i>Filter Type</i> is Blacklisted/ Permitted URLs : Permitted URLs can only be entered when Auto Filter is enabled. Specified URLs are accessible whether the automatic filter allows access or not. Requires iOS 8.0 or later.			•
Blacklisted URLs	When <i>Filter Type</i> is Blacklisted/ Permitted URLs , access to the specified URLs is blocked. Requires iOS 8.0 or later.			•
Whitelisted Bookmarks	When <i>Filter Type</i> is Whitelisted Bookmarks , URLs entered here are added to the browser's bookmarks, and the user is not allowed to visit any sites other than these.			•
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 Super- vised 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.			
Single App Mode: Disable Touch Screen	Determines if the touch screen is operational. Requires iOS 7 or later.			•
Single App Mode: Disable Device Rotation	Determines if device rotation sensing is operational. Requires iOS 7 or later.			•
Single App Mode: Disable Volume Buttons	Determines if volume buttons are operational. Requires iOS 7 or later.			•
Single App Mode: Disable Ringer Switch	Determines if the ringer switch is operational. Requires iOS 7 or later.			•
Single App Mode: Disable Sleep/Wake Button	Determines if the sleep/wake button is operational. Requires iOS 7 or later.			•
Single App Mode: Disable AutoLock	Determines if the device will automatically go to sleep after an idle period. Requires iOS 7 or later.			•
Single App Mode: Enable VoiceOver	Determines if VoiceOver, a feature that audibly assists a user in navigating the touch screen, is on or off. VoiceOver enables a blind or low vision user to touch the screen to hear what is under their finger, then gesture to control the device. Works with apps that come with the iOS device. Requires iOS 7 or later.			•
Single App Mode: Allow VoiceOver Adjustments	Determines if the user is permitted to adjust VoiceOver settings. Enable Voice Over must be on. Requires iOS 7 or later.			•
Single App Mode: Enable Zoom	Determines if Zoom, an assistive built in magnifier is turned on or off. A double tap with three fingers instantly zooms 100-500 percent. Requires iOS 7 or later.			•
Single App Mode: Allow Zoom Adjustments	Determines if the user is permitted to adjust Zoom settings. Enable Zoom must be on. Requires iOS 7 or later.			•

Policy Suite Rules: iOS	Description	iOS	TD/ iOS	iOS Super- vised devices
Single App Mode: Enable Invert Colors	Determines if Invert Colors, an assistive feature that inverts colors for a higher contrast, is turned on or off. Once colors are set, the settings apply systemwide, even to video. Requires iOS 7 or later.			•
Single App Mode: Allow Invert Colors Adjustments	Determines if the user is permitted to adjust Invert Colors settings. Enable Invert Colors must be on. Requires iOS 7 or later.			•
Single App Mode: Enable AssistiveTouch	Determines if the AssistiveTouch, a feature that provides alternatives to the standard navigation gestures, is turned on or off. Alternatives or customization can be created for gestures such as pinch, pressing the Home button, rotate, or shake. Requires iOS 7 or later.			•
Single App Mode: Allow AssistiveTouch Adjustments	Determines if the user is permitted to adjust AssistiveTouch. Enable AssistiveTouch must be on. Requires iOS 7 or later.			•
Single App Mode: Enable Speak Selection	Determines if Speak Selection, an assistive feature that reads text, is turned on or off. Speak Selection allows a user to highlight text in any application and tap Speak to have the selection read aloud. Requires iOS 7 or later.			•
Single App Mode: Enable Mono Audio	Determines if Mono Audio, an assistive feature that plays left and right audio channels in both headphone earbuds, is turned on or off. Requires iOS 7 or later.			•

POLICY RULES: KNOX DEVICES

Policy Suite Rules: Samsung KNOX Specific	Description	Anrd	Anrd w/o MDM App	TD/A
Samsung KNOX Device Policies: Alternative Home Screen				
Enable Alternative Home Screen	<p>When enabled, restricts devices to Managed Apps and allows administrators to define which navigation functions are available to users.</p> <p><i>The Allow user to remove enrollment</i> option (Device Control > Device Features) should be disabled to prevent users from deleting the MDM account in order to revert back to the original Home screen.</p> <p><i>Note: Alternative Home Screen cannot coexist with Kiosk Mode or KNOX Workspace. Only one of these features can be enabled at any given time.</i></p>	•		•
Allow Hardware Keys	Enables/disables device hardware keys that control device power, volume, and navigation.	•		•
Allow Back Button	Determines whether the Back button is functional on the device.	•		•
Allow Home Button	Determines whether the Home button is functional on the device.	•		•
Allow Menu Button	Determines whether the Menu button is functional on the device.	•		•
Allow Power Button	Determines whether the on /off power button is functional on the device.	•		•
Allow Volume Button	Determines whether the up/down Volume buttons are functional on the device.	•		•
Allow Multi Window Mode	Determines whether a tab that allows users to enter a mode where multiple tasks can be completed on one screen is visible or hidden.	•		•
Allow Navigation Bar	Determines whether the Navigation Bar is hidden on the Home screen of devices that lack hardware navigation.	•		•
Allow Status Bar	Determines whether the Status Bar is hidden on the device Home screen.	•		•
Allow System Bar	Determines whether the Status Bar, System Bar (at the bottom of tablet screens), or Navigation Bar (on the Home screen of devices that lack hardware navigation) are hidden on the device.	•		•
Allow Task Manager	Determines whether the Task Manager and Home button operation to display recently used applications are blocked.	•		•

Policy Suite Rules: Samsung KNOX Specific	Description	Anrd	Anrd w/o MDM App	TD/A
Samsung KNOX Device Policies: Applications				
Allow Google Play	Determines whether the user is able to install Play Store applications. If disabled, any managed Play Store app that is recommended or forced will not push to the device. Enterprise apps will be pushed to the device.	•		•
Allow Settings	Determines whether the user has access to the device settings.	•		•
Allow YouTube	Determines whether the user is able to use YouTube. If disabled, the YouTube icon is removed from the device Home screen.	•		•
Samsung KNOX Device Policies: Browser Policy				
HTTP Proxy	Allows an administrator to specify HTTP proxy settings. Enter the proxy server address and port number.	•		•
Samsung KNOX Device Policies: Device Features				
Allow Access to Clipboard	Determines whether user has access to the device clipboard.	•		•
Allow Sharing Clipboard Between Applications	Determines whether user can copy/paste data between applications. "Allow access to clipboard" must be enabled.	•		•
Allow Audio Recording	Determines whether a user can make audio recordings using the device.	•		•
Allow Cellular Data	Determines if the cellular network can be used for internet access.	•		•
Allow developers mode	Allows or disallows access to developer testing options on the device.	•		•
Allow background process limit	Allows or disallows access to the developer option which can be used to reduce the number of processes running in the background.	•		•
Allow killing activities on leave	Allows or disallows access to the developer option that deletes an app from the activity stack, thereby closing the app, when a user leaves the app or uses the back button.	•		•
Allow USB debugging	Allows or disallows the device to be connected to a computer running a diagnostic program in order to access higher level information about the device.	•		•
Allow using mock location	Allows or disallows access to an option that puts Location Services into a mock mode so that location data can be sent to the device for testing location-aware apps.	•		•
Allow Factory Reset	Determines whether a factory reset can be performed on the device, wiping data and firmware settings.	•		•
Allow installation of applications from sources other than Google Play	Determines whether the user can install apps from sources other than Google Play. This includes enterprise apps.	•		•

Policy Suite Rules:	Description	Anrd	Anrd w/o MDM App	TD/A
Samsung KNOX Specific				
Allow installation of non-trusted apps	Determines whether user can install an unsigned application. <i>Note:</i> This currently allows the installation of any app regardless it is enabled or disabled. This is an issue with the KNOX device API that needs to be addressed by Samsung.	•		•
Allow Microphone	Determines if a user is permitted to use the device microphone.	•		•
Allow MTP	Determines if the device can use the “Media Device (MTP)” option to connect to a computer for media file transfers.	•		•
Allow NFC	Determines if short range or Near Field Communication is permitted between the device and other compatible devices. Supported with KNOX 2.0 devices.	•		•
Allow OTA Upgrade	Determines whether the device operating system can be updated over-the-air.	•		•
Allow Safe Mode	Determines whether a device can use Safe mode to diagnose whether a third party app is causing issues with the device.	•		•
Allow Screen Capture	Determines whether the user can capture a screen shot with the device.	•		•
Allow SD Card	Determines if a user can access contents of the storage card.	•		•
Allow Tethering	Determines whether the user can use the device to connect a laptop or tablet to the internet.	•		•
Allow USB-Host-Storage	Determines if the device can connect to a USB drive and browse its contents. Requires Android OS 3.1+	•		•
Allow Video Recording	Determines whether a user can make video recordings using the device.	•		•
Samsung KNOX Device Policies: Email Policy				
Allow Account Addition	Determines if users can create mail accounts in addition to the mail account created by MDM.	•		•
Samsung KNOX Device Policies				
Kiosk Mode	Allows administrators to specify a single application to which KNOX devices will be locked. The device returns to the specified app upon wake or reboot and blocks device features that permit navigation and task management. There can only be one kiosk app named at a time. Since device navigation buttons are disabled, the kiosk app should be one that is completely navigable from within the app. <i>Note: Kiosk Mode cannot coexist with Alternative Home Screen or KNOX Workspace. Only one of these features can be enabled at any given time.</i>	•		•

Policy Suite Rules:	Description	Anrd	Anrd w/o MDM App	TD/A
Samsung KNOX Specific				
Samsung KNOX Device Policies: Password				
Maximum character sequence length	The number of repeated (aaa) or sequential (abc) alphabetic characters in a password.	•		•
Maximum occurrences of a character in a password	The number of times a character may be used in a password.	•		•
Minimum character change length	The number of changed characters a password must have when compared to the previous password. Rearranging existing characters is not an acceptable change.	•		•
Maximum numeric sequence length	The number of repeated (333) or sequential (123) digits in a password.	•		•
Minimum number of complex characters	The number of numeric or symbol characters required in a password.	•		•
Set forbidden string permissions	Define strings that users may not use when creating a password.	•		•
Allow occurrence of username in password	Determines whether username can be part of the password.	•		•
Allow occurrence of email in password	Determines whether email address can be part of the password.	•		•
Forbidden password strings	Define the strings users are not permitted to use in passwords.	•		•
Enable password visibility	Determines whether user will see the password elements as they are entered.	•		•
Enable password pattern visibility	Determines whether user will see the 9-point pattern unlock as it is used to access the device.	•		•
Define password pattern	Define the regular expression pattern that must be used to create a password.	•		•
Require password change timeout	Repeatedly prompts a user to change the password when it is not compliant with one or more of the password policies.	•		•
Maximum password change timeout (in minutes)	Defines the interval between the repeated prompt that alerts a user his/her password does not meet requirements.	•		•
Disable device on failed password attempts	Prevents the user from entering a password after a specific number of attempts have been made. A disabled device can be recovered by issuing the <i>Unblock Password Entry</i> command or a selective wipe from the dashboard.	•		•
Maximum number of attempts	Define the number of unlock attempts before the device blocks the user from entering a password.	•		•
Samsung KNOX Device Policies: Roaming				
Allow Data while roaming	Determines whether the device can use cellular data while roaming.	•		•
Allow Push while roaming	Determine whether the device can use a cellular connection to synchronize user's mail accounts at periodic intervals while roaming.	•		•

Policy Suite Rules:	Description	Anrd	Anrd w/o MDM App	TD/A
Samsung KNOX Specific				
Allow Sync while roaming	Determines whether the device can use a cellular connection to auto-synchronize user's mail accounts while roaming.	•		•
Allow Voice calls while roaming	Determines if the device can be used for cellular voice calls while roaming.	•		•
Samsung KNOX Workspace Policies				
Create KNOX Workspace Container	<p>When enabled, pushes license to supported devices and prompts users to install the KNOX Workspace Container app. License must be uploaded on the ZMM server first.</p> <p>When this policy is enabled in a user's policy suite, their native ActiveSync account on the device will be migrated to the secure Workspace container.</p> <p><i>Note: KNOX Workspace cannot coexist with Alternative Home Screen or KNOX Kiosk Mode. Only one of these features can be enabled at any given time.</i></p>	•		•
Samsung KNOX Workspace Policies: Email Policy				
Allow Account Addition	Determines if users can create mail accounts in addition to the mail account created by MDM.	•		•
Samsung KNOX Workspace Policies: Password				
Minimum password length	Determines the password length if a minimum length is set. Password is always required when a KNOX Workspace container exists.	•		•
Maximum character sequence length	The number of repeated (aaa) or sequential (abc) alphabetic characters in a password.	•		•
Maximum occurrences of a character in a password	The number of times a character may be used in a password.	•		•
Minimum character change length	The number of changed characters a password must have when compared to the previous password. Rearranging existing characters is not an acceptable change.	•		•
Maximum numeric sequence length	The number of repeated (333) or sequential (123) digits in a password.	•		•
Minimum number of complex characters	The number of numeric or symbol characters required in a password.	•		•
Set forbidden string permissions	Define strings that users may not use when creating a password.	•		•
Allow occurrence of username in password	Determines whether username can be part of the password.	•		•
Allow occurrence of email in password	Determines whether email address can be part of the password.	•		•
Forbidden password strings	Define the strings users are not permitted to use in passwords.	•		•
Enable password visibility	Determines whether user will see the password elements as they are entered.	•		•

Policy Suite Rules: Samsung KNOX Specific	Description	Anrd	Anrd w/o MDM App	TD/A
Enable password pattern visibility	Determines whether user will see the 9-point pattern unlock as it is used to access the device.	•		•
Define password pattern	Define the regular expression pattern that must be used to create a password.	•		•
Require password change timeout	Repeatedly prompts a user to change the password when it is not compliant with one or more of the password policies.	•		•
Maximum password change timeout (in minutes)	Defines the interval between the repeated prompt that alerts a user his/her password does not meet requirements.	•		•
Disable device on failed password attempts	Prevents the user from entering a password after a specific number of attempts have been made. A disabled device can be recovered by issuing the <i>Unblock Password Entry</i> command or a selective wipe from the dashboard.	•		•
Maximum number of attempts	Define the number of unlock attempts before the device blocks the user from entering a password.	•		•
Require device password expiration	Forces the device to require users to update their passwords after a number of days.	•		•
Password expiration in days	Defines the number of days a password can be used before it expires.	•		•
Require device password history	Forces the device to disallow the entry of passwords that have been used in the recent past. The number of stored past passwords is configurable.	•		•
Number of passwords stored	Defines the number of device passwords stored to prevent users from reusing them too soon.	•		•
Samsung KNOX Workspace Policies: Restrictions				
Allow Camera	Determines if the use of a camera is allowed on the device (this may affect 3rd party apps that utilize the camera). Note: The <i>Allow Camera</i> setting under <i>Device Control</i> will control the device camera both inside and outside the Workspace container.	•		•
Allow Share List	Administrator can disable the display of the Share Via List. The option is available in certain applications that share data with other applications.	•		•
Use Secure Keypad	When enabled, characters, digits, and symbols associated with device keys do not display when pressed.	•		•

POLICY RULES: TOUCHDOWN

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o MDM App	TD/iOS	TD/iOS w/o MDM App
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 <i>Require encryption on the device</i> option, under Security Settings, so that the entire device is not encrypted. Gives repeated reminders until the user initiates encryption. iOS devices (iPhone and iPad) have hardware encryption that is always enabled. The policy is not used to enable/disable.	•		•	
Push TD volume license key 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.	•			

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o MDM App	TD/iOS	TD/iOS w/o MDM App
	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.				
Require TouchDown PIN (Link)	Links to the <i>Require TouchDown PIN</i> option in Security Settings > Password, which determines whether a PIN is required to access the TouchDown app. Can be used in addition to or in place of the <i>Require Device Password</i> option.	•		•	
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.	•		•	
Set signature (Corporate / Individual)	Allows the entry of a signature determined by the administrator.	•		•	

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o MDM App	TD/iOS	TD/iOS w/o MDM App
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 MDM App	TD/iOS	TD/iOS w/o MDM App
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. Choose from: 150%, 200%, 250%, 300%, 400%, or 500%	•		•	
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 MDM App	TD/iOS	TD/iOS w/o MDM App
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 <i>Choose Folders</i> 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 MDM App	TD/iOS	TD/iOS w/o MDM App
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: <i>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.</i>				
Suppression configuration	Choose which options to hide or expose to TouchDown users. Select <i>All</i> to enable all suppressions, giving users control. Select <i>None</i> to disable all suppressions or <i>Custom</i> 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	Enables users to allow appointment reminders during periods when the device is not synchronizing.	•		•	
Enable appointment reminders at non-peak times	Control setting determines whether appointment reminders display during non-peak times.				
Allow appointment synchronization options	Enables users to choose how many days worth of appointments to keep on the device. From Device Control options, an administrator can set a maximum or allow users to choose a specific number of days.	•		•	
Allow category configuration	Enables users to select colors for contact, event, and task 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.	•		•	
Name format for contacts copied to phone	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 MDM App	TD/iOS	TD/iOS w/o MDM App
Allow enable appointment reminders option	Allows users to enable appointment reminders.				
Enable appointment reminders	Control setting determines whether a notification displays when an appointment has a reminder.	•		•	
Allow include phone contacts in picklist option	Enables users to determine whether the contact list displayed when composing email or SMS includes contacts from the Android Phone Book.				
Include phone contacts in picklist	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	Enables users to determine how contact phone numbers retrieved from the server are formatted.				
Normalize phone numbers	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	Enables users to configure repeating reminders for calendar events.				
Set reminders (in min)	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	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.				
Update contact changes to phone	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.	•		•	

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o MDM App	TD/iOS	TD/iOS w/o MDM App
Suppressions: Device Control					
Allow ActiveSync device type string field ActiveSync device type string field	Enables users to modify the ActiveSync device type the device reports to the <i>ZENworks Mobile Management</i> 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 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 Disable tablet mode (tablet devices only)	Allows tablet users to disable the automatic switch to tablet mode. Use the control setting to disable the automatic switch to Tablet Mode for tablet users.	•		•	
Allow exclude attachments from gallery option Exclude attachments from gallery	Enables users to determine whether Android Gallery scans the SD card for TouchDown media files. 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 Display tasks on home screen and widgets	Enables users to filter tasks shown on the Home screen and on the Task Widget just as they are on the TouchDown Tasks screen. 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.	•			

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o MDM App	TD/iOS	TD/iOS w/o MDM App
Allow server name fields	Displays the address of the <i>ZENworks Mobile Management</i> 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 Show email list on startup	Enables users to open TouchDown to the email list instead of the main display pane. Control setting determines whether TouchDown will open to the Email list instead of TouchDown's main screen.	•		•	
Allow use system background data setting option Use system background data setting	Determines whether TouchDown honors how the user has configured the Android <i>Background Data</i> 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 <i>Background Data</i> 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 <i>Choose Folders</i> , this also controls the following device options: <i>Selected Email Folders</i> and <i>Refresh Folders</i> .	•		•	
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.	•		•	

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o MDM App	TD/iOS	TD/iOS w/o MDM App
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 minutes)	Enables users to determine how often the device checks for new email. 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 email synchronization options	Enables users to set the age of email to be synchronized to the device. From Device Control options, an administrator can set a maximum or allow users to choose a specific age.	•		•	
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.	•		•	

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o MDM App	TD/iOS	TD/iOS w/o MDM App
Suppressions: Security					
Allow clean SD card on remote wipe option	Enables users to determine whether all files on the SD card are deleted when a remote Wipe is issued.				
Clean SD card on remote wipe	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.	•			
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.	•		•	

Policy Suite Rules: TouchDown Specific	Description	TD/A	TD/A w/o MDM App	TD/iOS	TD/iOS w/o MDM App
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 Send failed polling notifications	Enables users to determine whether a notification displays if synchronization has failed. Control setting determines whether a notification displays if synchronization has failed.	•		•	
Allow notify on successful polling option Send successful polling notifications	Enables users to determine whether a notification displays when synchronization is successful. 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 Enable polling at off-peak times	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. 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.	•		•	

POLICY RULES: WINDOWS DEVICES

Policy Suite Rules: Windows Device Specific	Description	Windows
Applications		
Allow Email Setup	Determines whether the device will allow an Email account to be set up.	•
Allow IE Browser	Determines whether the device will allow the use of Internet Explorer.	•
Allow Windows App Store	Determines whether Windows App Store access is enabled on the device.	•
Allow Windows Store Auto Update	Determines if the option in Windows Store to automatically update apps is enabled. Requires Windows OS 10 or higher.	•
Restrict App Installation to System Volume	Determines whether the installation of applications is restricted to the system drive. Requires Windows OS 10 or higher.	•
Device Features		
Allow Action Center Notifications	Determines if notifications can be viewed in a phone's action center when the screen is locked. Requires Windows OS 8.1 or higher. Not supported on PCs.	•
Allow Bluetooth Discovery	Determines whether other devices are able to discover the Windows device via Bluetooth. Supported for Windows 10 Desktop or higher.	•
Allow Cortana	Determines whether Cortana, the voice based digital assistant, is enabled on the device. Requires Windows OS 8.1 or higher. PCs require OS 10 or higher.	•
Allow Developer Unlock	Determines whether a user can unlock a device in order to side load apps that are not available in Windows Store. Requires Windows OS 8.1 or higher. PCs require OS 10 or higher.	•

Policy Suite Rules: Windows Device Specific	Description	Windows
Allow Microsoft Account Connection	Determines whether the user is allowed to use outlook.com, hotmail.com, or other Microsoft accounts for non-email related authentication. Requires Windows OS 8.1 or higher. PCs require OS 10 or higher.	•
Allow Sync My Settings	Determines whether settings associated with a Microsoft account are synchronized to all devices associated with the account. If enabled, changes made on one device will synchronize to all. Requires Windows OS 8.1 or higher. PCs require OS 10 or higher.	•
Allow Task Switcher	Determines whether the visual Task Switcher can be used on the device. Disabling it does not affect the back button action. Requires Windows OS 8.1 or higher. PCs require OS 10 or higher.	•
Allow Toasts	Determines whether toast notifications (auto-expiring, pop-up information) can be viewed on a device when the screen is locked. Requires Windows OS 10 or higher.	•
Allow Voice Recording	Determines whether voice recording features is enabled on the device. Requires Windows OS 8.1 or higher. PCs require OS 10 or higher.	•
Management		
Allow Data Roaming	Determines whether the data network is enabled when the device is roaming.	•
Allow Phone Reset	Determines whether the user is able to factory reset the device.	•
Allow VPN Over Cellular	Determines whether a VPN connection can be made over a cellular network. Requires Windows OS 8.1 or higher. PCs require OS 10 or higher.	•
Allow VPN Over Cellular Roaming	Determines whether a VPN connection can be made when a device is using cellular roaming service. Requires Windows OS 8.1 or higher. PCs require OS 10 or higher.	•
Passport for Work		
Use Passport for Work	Determines if Passport for Work is configured on the device. Disabling the setting disallows configuration, but does not remove Passport on devices already configured. Requires Windows OS 10 desktop.	•

Policy Suite Rules: Windows Device Specific	Description	Windows
Require Security Device	Determines if the device is required to have a Trusted Platform Module (TPM) in order to use Passport with the defined Active Directory tenant. Requires Windows OS 10 desktop.	•
Minimum PIN Length	Defines the minimum length for any Passport PIN used with the defined Active Directory tenant. Requires Windows OS 10 desktop.	•
Require Uppercase Letters	Determines if uppercase letters are required in the Passport PIN used with the defined Active Directory tenant. If this setting is off, uppercase letters are disabled. Requires Windows OS 10 desktop.	•
Require Lowercase Letters	Determines if lowercase letters are required in the Passport PIN used with the defined Active Directory tenant. If this setting is off, lowercase letters are disabled. Requires Windows OS 10 desktop.	•
Require Special Characters	Determines if symbol characters are required in the Passport PIN used with the defined Active Directory tenant. If this setting is off, symbols are disabled. Requires Windows OS 10 desktop.	•
Require Numbers	Determines if numbers are required in the Passport PIN used with the defined Active Directory tenant. If this setting is off, numbers are still allowed. Requires Windows OS 10 desktop.	•
Allow Biometrics	Determines if Passport may use biometric unlock methods. Requires Windows OS 10 desktop.	•

USER SELF-ADMINISTRATION PORTAL (USAP)

User Self Administration Portal (USAP) Permissions	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS or TD/iOS	iOS Supervised devices	Active-Sync Only
iOS Security Actions								
Display Selective Wipe	Determines whether the Selective Wipe action is visible in the User Self-Administration Portal (USAP).					•	•	
Display Locate Device	Determines whether the Locate Device action is visible in the USAP. <i>When Audit Tracking > Location Tracking > Record Location of Device is disabled, this option cannot be edited.</i>					•	•	
Display Lock Device	Determines whether the Lock Device action is visible in the USAP.					•	•	
Display Full Wipe	Determines whether the Full Wipe action is visible in the USAP.					•	•	
Display Clear Passcode	Determines whether the Clear Passcode action is visible in the USAP.							
Android Security Actions								
Display Selective Wipe	Determines whether Selective Wipe action is visible in the User Self-Administration Portal (USAP).	•		•				
Display Locate Device	Determines whether the Locate Device action is visible in the USAP. <i>When Audit Tracking > Location Tracking > Record Location of Device is disabled, this option cannot be edited.</i>	•		•				
Display Lock Device	Determines whether the Lock action is visible in the USAP.	•		•				
Display Wipe Storage Card	Determines whether the Wipe Storage action is visible in the USAP.	•		•				

User Self Administration Portal (USAP) Permissions	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS or TD/iOS	iOS Supervised devices	Active-Sync Only
Display Full Wipe	Determines whether the Full Wipe action is visible in the USAP.	•		•				
Display Reboot Device	Determines whether the Reboot Device action is visible in the USAP.	•		•				
Display Power Off	Determines whether the Power Off action is visible in the USAP.	•		•				
Display Unblock Password Entry	Determines whether the Unblock action is visible in USAP.	•		•				
Device Statistics								
Display Connections	Determines whether Connections are visible in the User Self-Administration Portal (USAP).							
Display Basic Statistics	Determines whether Basic statistics are visible in the USAP.							
Display Advanced Statistics	Determines whether Advanced statistics are visible in the USAP.							
iOS Applications								
Display Managed Apps	Determines whether Managed Applications are visible in the USAP. When <i>Display Managed Apps</i> for both iOS and Android are enabled or both are disabled, the setting is replicated in <i>Resource Control > Allow Managed Apps</i> .					•	•	
Display Blacklists	Determines whether Blacklists are visible in the USAP.					•	•	
Display Whitelists	Determines whether Whitelists are visible in the USAP.					•	•	
Android Applications								
Display Managed Apps	Determines whether Managed Applications are visible in the USAP. When <i>Display Managed Apps</i> for both Android and iOS are enabled or both are disabled, the setting is replicated in <i>Resource Control > Allow Managed Apps</i> .	•		•				

User Self Administration Portal (USAP) Permissions	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS or TD/iOS	iOS Supervised devices	Active-Sync Only
Display Blacklists	Determines whether Blacklists are visible in the USAP.	•		•				
Display Whitelists	Determines whether Whitelists are visible in the USAP.	•		•				
Certificates								
Display Add Certificates	Determines if Certificates section is visible in USAP. If either Corporate or Individual is enabled, certificates will display on both Corporate and Individual devices.	•		•	•	•	•	

SECURITY ACTIONS: ALL DEVICES

Security: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS or TD/iOS	iOS Supervised devices	Windows	Active-Sync 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, Managed Apps, and File Share options and must enter a password to gain full functionality when suspension is lifted.	•	•	•	•	•	•		BB10 wOS WP
Selective Wipe	<p>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 <i>ZENworks Mobile Management</i> account; and deletes the device from the grid. Functionality varies by device platform.</p> <p>Android (native): Devices with native mail app only wipe the <i>ZENworks</i> account. Mail/PIM is not wiped.</p> <p>Android (native) KNOX devices: Native mail accounts that have been set up automatically through the KNOX API wipe the <i>ZENworks Mobile Management</i> account and mail/PIM data associated with the native mail app.</p> <p>Android (TouchDown): Returns TouchDown to a pre-registration state. Erases only the TouchDown data from the SD card. If the <i>Clean SD Card on Remote Wipe</i> option in the TouchDown <i>Advanced Settings</i> is enabled, then the SD card is completely erased.</p>	•		•	•	•	•	•	

Security: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS or TD/iOS	iOS Supervised devices	Windows	Active-Sync only
	<p>BlackBerry (OS 4.5-7.1): Removes mail and PIM data associated with the GO!NotifySync application. Locks the device if Require Password is enabled.</p> <p>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.)</p> <p>iOS 7.0.3+ devices enrolled in the Volume Purchase Program : VPP licenses are reclaimed and the user is retired from the program when it is the last iOS 7.0.3+ device associated with the user.</p> <p>BB10, webOS and WP or any device without the <i>ZENworks</i> app: The only action performed is to remove device from the <i>ZENworks</i> server and dashboard grid.</p> <p>Windows 8.1+: device is unenrolled and configured policies, apps, etc. are automatically removed.</p>								
Remove User	<p>Stops managing all devices associated with the user and subsequently removes the user from the <i>ZENworks Mobile Management</i> server and dashboard grid.</p> <p><i>Note:</i> Shared Users can only be removed when status is <i>Not Enrolled</i> or all devices enrolled with the shared user credentials have been wiped. Any DEP devices assigned to the shared user will be unassigned when the shared user is removed.</p> <p>iOS 7.0.3+ devices enrolled in the Volume Purchase Program : VPP licenses are reclaimed and the user is retired from the program.</p>	•	•	•	•	•	•		BB10 wOS WP
Wipe Storage Card	<p>Administrators or end users can remotely wipe all data from the device's storage card.</p> <p>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.</p>	•		•	•				
Full Wipe	<p>Administrators or end users can issue a full wipe command. Once the wipe is completed, the device is removed from the</p>	•	•	•	•	•	•	•	BB10 wOS

Security: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS or TD/iOS	iOS Super- vised devices	Windows	Active- Sync only
	<p>dashboard Device Grid. Functionality varies by device platform.</p> <p>(Once the device has been wiped, the administrator might also want to issue the <i>Disable</i> or <i>Suspend Device</i> command to temporarily block the device.)</p> <p>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. KNOX Standard compatible devices wipe both internal and external memory.</p> <p>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.</p> <p>BlackBerry: Removes all mail and PIM data associated with the GO!NotifySync application and removes the GO!NotifySync account. Locks the device if Require Password is enabled. Erases the entire SD card, including saved attachments.</p> <p>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.</p> <p>iOS 7.0.3+ devices enrolled in the Volume Purchase Program : VPP licenses are reclaimed and the user is retired from the program when it is the last iOS 7.0.3+ device associated with the user.</p> <p>BB10, webOS and WP or any device without <i>ZENworks Mobile Management</i> 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.</p> <p>Windows 8.1+: the device is unenrolled and returns to factory settings removing all internally stored data and device settings.</p>								WP
Lock Device	Administrators or end users can remotely lock the device, requiring an unlock password to be entered before the device can be used.	•		•	•	•	•	•	

Security: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS or TD/iOS	iOS Supervised devices	Windows	Active-Sync only
	<p>Windows 8.1+: Lock is initiated only if the device has a device security password enabled and only when device syncs with the server; Not supported in Windows 10 Desktop.</p> <p>Windows 10 Phones: Locking the phone generates a new unlock PIN and gives the administrator an opportunity to email it to the user. See also, <i>Email Unlock PIN</i> below. Not supported for Windows 10 Desktop or tablets.</p>								
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.					•			
Reboot	<p>Rebooting a device is a troubleshooting measure that will power off your device and restart it. In the process it returns device software to a known state and often corrects what is causing the issue.</p> <p>Applicable for Samsung KNOX device only.</p>	•		•					
Power Off	<p>Power off your device to conserve its charge.</p> <p>Applicable for Samsung KNOX device only.</p>	•		•					
Unlock Password Entry	<p>If the password entry field to unlock your device has been blocked due to a password violation, you can remove the block by sending this command. This does not reset the password.</p> <p>Applicable for Samsung KNOX device only.</p>	•		•					
Remote Ring	This action will audibly ring the device to assist in location, even if it is set to vibrate or silent.							•	
Reset PIN	<p>Resets the PIN that unlocks a device and transmits a new PIN to the server. The new PIN can be viewed on the server via the Desktop User Self-Administration Portal.</p> <p>Only supported for Windows 8.1/10 phones.</p>							•	
Email Unlock PIN	<p>Sends an email to the user with the unlock PIN from the most recent lock action.</p> <p>Only supported for Windows 10 phones.</p>							•	
Network Connection Security and Configuration									
SCEP (Simple Certification Enrollment Protocol)	Sets up SCEP settings for devices.					•			

Security: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS or TD/iOS	iOS Super- vised devices	Windows	Active- Sync only
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

Device Statistics: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS or TD/iOS	iOS Super- vised devices	Windows	Active- Sync 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.			•					
Status: Device Memory									
Capacity	Displays the total of the used and unused memory on the device.	•		•	•	•	•		

Device Statistics: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS or TD/iOS	iOS Super- vised devices	Windows	Active- Sync only
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. iOS devices support this only when the MDM App is installed on the device.	•		•		•			
Status: TouchDown									
TouchDown Enrolled	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.					•	•		
Data Roaming Enabled	Current setting for Data Roaming.					•	•		
Status: Supervised									
Is Supervised	Whether or not the device is in Supervised mode. Requires iOS 6 or later.					•	•		

Device Statistics: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS or TD/iOS	iOS Super- vised devices	Windows	Active- Sync only
Status: Device Locator Service									
Device Locator Service Enabled	Whether the device has a device locator service (such as Find My iPhone) enabled. Requires iOS 7 or later.					•	•		
Status: Do Not Disturb									
Is Do Not Disturbed in Effect	Whether the device's <i>Do Not Disturb</i> option is enabled, silencing calls, alerts, and notifications. Requires iOS 7 or later.					•	•		
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 GO!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 GO!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.	•		•		•			

Device Statistics: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS or TD/iOS	iOS Super- vised devices	Windows	Active- Sync only
Network: Network Details									
Network Type	Displays the network type the device is using.	•		•	•	•	•		
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. <i>Android devices: Requires KNOX Standard compatibility</i>	•				•	•	•	
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.					•	•		
Ethernet MACs	Ethernet MAC addresses. <i>Requires iOS 7 or later.</i>					•	•		
Network: Hotspot									
Personal Hotspot Enabled	Whether the device connected to the Internet over a cellular data network is sharing the Internet connection with a computer or other iOS device connected to it via Wi-Fi or a computer connected to it via Bluetooth or USB. <i>Requires iOS 7 or later.</i>					•	•		
About: Shared Devices									
Last Signed Out	Date/time stamp of the most recent sign out of a shared device by an individual user.	•		•		•	•		
Last Signed In	Date/time stamp of the most recent sign in to a shared device by an individual user.	•		•		•	•		
Signed In By	The individual user who is currently signed in to the shared device.	•		•		•	•		
Shared User	The Shared User credentials with which a device was originally enrolled.	•		•		•	•		

Device Statistics: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS or TD/iOS	iOS Super- vised devices	Windows	Active- Sync only
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
Device ID	A device identifier string reported to Exchange ActiveSync. Requires iOS 7 or later.					•	•		
About: Operating System									
Operating System: Language	Name of the language the device OS is using.	•		•	•			•	
Operating System: Version	Displays the device OS version. iOS supervised devices: If OS is older than the current version, administrator can issue a command, from the <i>Device Information</i> page, to update.	•		•	•	•	•	•	
Operating System: Build Number	Detects and displays the Android OS build number.	•		•					
Operating System: OS	The base operating system used for the device platform. Android devices: Requires KNOX Standard compatibility.	•						•	
Operating System: Kernel Version	The version of the kernel portion of the device platform's base operating system. Android devices: Requires KNOX Standard compatibility.	•							
About: Device									
Model	Device's internal model number.	•				•	•	•	

Device Statistics: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS or TD/iOS	iOS Super- vised devices	Windows	Active- Sync only
	Android devices: Requires KNOX Standard compatibility.								
Model Name	Name of the device model. Android devices: Requires KNOX Standard compatibility.	•				•	•		
Device Name	The name of the device. iOS devices: Given via iTunes Android devices: Given via KNOX Standard API; Requires KNOX Standard compatibility.	•				•	•	•	
Maker	The device manufacturer. Android devices: Requires KNOX Standard compatibility.	•						•	
Ownership	Tracks whether the device is a company device or personal device.	•		•	•	•	•		
Platform	Displays the device platform type as reported by the device.	•		•	•	•	•		BB10
Platform Version Name	The name of the device platform version. Android devices: Requires KNOX Standard compatibility.	•							
UID	Displays the device UID.				•		•	•	
IMEI	The International Mobile Equipment Identify number. See http://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity BlackBerry with GO!NotifySync: Limited to GSM devices.	•		•	•	•	•	•	WP
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	Device's serial number.	•		•	•	•	•		
Device Local Time	Local time set on the device.							•	
Device Processor Architecture	Processor family identifying the processor in the device and applications that can run on it.							•	
Modem Firmware Version	The baseband firmware version. Android devices: Requires KNOX Standard compatibility.	•				•	•		

Device Statistics: All Devices	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS or TD/iOS	iOS Super- vised devices	Windows	Active- Sync only
MEID	The device's MEID (CDMA).					•			
ICCID	The ICC identifier for the installed SIM card (if applicable).					•	•		
WiFi IP	IP address of the network to which the device is currently connecting.							•	
Bluetooth MAC	Bluetooth MAC address. Android devices: Requires KNOX Standard compatibility.	•				•	•		
Wi-Fi MAC	Wi-Fi MAC address.	•		•		•	•		
Activation Lock	Whether the Activation Lock can be used via the Find My Phone app.						•		
Subscriber MCC	Home Mobile Country Code					•	•		
Subscriber MNC	Home Mobile Network Code					•	•		
Current MCC	Current Mobile Country Code					•	•		
Current MNC	Current Mobile Network Code					•	•		
About: iTunes									
iTunes Account Active	Whether the device is currently using an iTunes account. Requires iOS 7 or later.					•	•		
iTunes Account Hash Value	Returns a hash of the iTunes store account currently logged in. This string is identical to the itsIdHash returned by the VPP App Assignment web service. Requires iOS 8.0 or later.					•	•		
About: iCloud									
Cloud Backup Enabled	Whether the device has iCloud backup enabled. Requires iOS 7.1 or later.					•	•		
Last Cloud Backup	The date and time of the device's last iCloud backup. Requires iOS 8.0 or later.					•	•		

COMPLIANCE MANAGER

Compliance Manager	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/iOS	iOS Supervised devices	Active-Sync 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 if Android user disables Device Administrators	An Android user has not granted device administration privileges to the <i>ZENworks Mobile Management</i> app.	•		•					
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
Restrict BlackBerrys without GO!NotifySync	A BlackBerry device that does not have the GO!NotifySync application has enrolled.	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.	•		•	•	•	•		
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

Compliance Manager	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/iOS	iOS Supervised devices	Active-Sync only
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 GO!NotifySync app is not enrolled	A BlackBerry device that does not have the <i>GO!NotifySync</i> application has enrolled. Devices that have the <i>GO!NotifySync</i> app, but not the <i>ZENworks Mobile Management</i> app will also trigger this 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. iOS devices support this only when the MDM App is installed on the device.	•		•	•	•	•		
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 server.	•		•	NA	NA	NA	NA	NA
Restrict jailbroken devices	A jailbroken iOS device connects to the server.	NA	NA	NA	NA	•	•		NA

Compliance Manager	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Active- Sync only
	iOS devices support this only when the MDM App is installed on the device.								
Restrict if passcode not initiated on device	The user's policy suite requires a password, but the device does not have a passcode initiated.	•		•		•	•	•	
Restrict if passcode is not compliant with requirements	The user's policy suite requires a password, but the device does not have a passcode compliant with the requirements.	•		•		•	•	•	
Restrict if passcode is not compliant with data protection	The device does not have a passcode and thus is not compliant with "data protection," which enhances the built-in hardware encryption by protecting the hardware encryption keys with the passcode.	•		•		•	•	•	
Restrict if data usage statistics reset by user	The user of an Android or iOS device on which the data plan is being tracked, has manually reset the data usage statistics.	•		•		•	•	•	
Restrict if iOS unmanaged configuration profile is on device	An iOS device has an unmanaged configuration profile.	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
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
Non-Access Policy Based Alerts									
Android passcode not initiated	The user's Policy Suite requires a password, but the Android device does not have a passcode initiated.	•		•					
Android passcode not compliant with data protection	The Android device does not have a passcode and thus is not compliant with "data protection," which enhances the built-in hardware encryption by protecting the hardware encryption keys with the passcode.	•		•					
Location not updated	A device's location has not updated within the defined interval.	•		•	•	•	•		
Low application availability	A managed application purchased in bulk is close to its availability limit (download limit or number of available licenses/redemption codes).	•		•		•	•		
Low battery detection	A device's battery level has fallen below a specified warning level.	•		•	•	•	•		

Compliance Manager	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/iOS	iOS Supervised devices	Active-Sync only
Low memory detection	A device's memory level has fallen below the greater of the two specified levels.	•		•	•	•	•		
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
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
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
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
Reset for Enrollment	An administrator has issued a <i>Reset for Enrollment</i> 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
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 to their device.	•	•	•	•	•	•		BB10 wOS 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

Compliance Manager	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Active- Sync only
									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 from 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 Managed Apps when these resources have been blocked.	•	•	•	•	•	•		BB10 wOS WP
Stop managing device issued by Admin	An administrator has issued a <i>Stop Managing Device</i> command from the dashboard to a device.	•		•	•	•	•	•	BB10 wOS WP
Stop managing device issued by user	A user has issued a <i>Stop Managing Device</i> command from the User Self Administration Portal to a device.	•		•	•	•	•		BB10 wOS WP
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
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	
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	NA	NA	NA	NA	•	•	•	NA

Compliance Manager	Description	Anrd	Anrd w/o MDM App	TD/A	NS/BB	iOS	TD/ iOS	iOS Super- vised devices	Active- Sync only
	reminder 30 days prior to the expiration and repeat it every day.								