Functionality by Device Platform

*Functionality Overview for the **Notify Mobile Device Management System** by Device Platform*
for Version 1.8.0

Table of Contents

Summary of the categories contained in the charts:

Policy Rules: All Devices

Application Control

Audit Tracking

Device Control

- Device Features
- Email
- ActiveSync Synchronization

Files Share Permissions

Mobile Apps Permissions

Security Settings

- Password
- Encryption
- Duress
- Device Inactivity and Locking
- Emergency Calling

SMIME Settings

Device Statistics: All Devices

Security: All Devices

- Device Statistics
- Security Commands
- Network Connection Security and Configuration

Policy Rules: iOS Device Specific

- Device Features
- Applications
- Safari Browser
- Ratings
- Security

Policy Rules: TouchDown Specific

- Installation
- General
- Signature
- Widgets
- Phone Book
- Suppression Rules

The information in these charts conveys what is functional in the *Notify Mobile Device Management* or ***NotifyMDM*** (*NMDM*) system, version 1.8.0.

Device platforms supported are iOS 4, Android, BlackBerry, Symbian S60 3rd edition, webOS, Windows Mobile 6, and Windows Phone 7. *See key below for supported OS versions.*

Functionality on iOS 4, Android, BlackBerry, and Window Mobile platforms is implemented using a *NotifyMDM* application (app) that is installed on the device. These devices also require a native ActiveSync protocol or an application that uses the ActiveSync protocol, such as *NotifySync™ for BlackBerry* or *TouchDown™ for Android*.

- On **BlackBerry** devices, *NotifySync for BlackBerry v4.9.x* is required to handle the ActiveSync policies. It can be installed in tandem with the *NotifyMDM* application.
- On **Android** OS 2.2 or greater devices, the ActiveSync protocol native to the device is sufficient. For devices running OS versions 2.0 or 2.1, the *TouchDown* ActiveSync client, available from the Android Market, is required to handle the ActiveSync policies. (Note that ActiveSync policies will only affect the *TouchDown* application.)
- On **iOS4** devices with multitasking capabilities, the ActiveSync policies are enforced using Apple configuration profiles. Additional iOS MDM API functionality is available when an Apple Enterprise Developer Production Certificate is purchased and applied on the *NotifyMDM* server.
- On **Windows Mobile** 6.1/6.5 devices, the ActiveSync protocol native to the device is sufficient.

The *NotifyMDM* app implements additional functionality, beyond the ActiveSync policies, which is not available if iOS 4, Android, BlackBerry, and Windows Mobile devices register against the server without the *NotifyMDM* app.

Symbian S60 3, **webOS**, and **Windows Phone 7** devices utilize the ActiveSync protocol native to the device and only ActiveSync policies supported by the device platform/model can be enforced. Functionality is indicated by a **red dot** in the charts below.

KEY

Anrd = Android devices, v2.2 - 3.1

TD/A = *TouchDown* v6.5.x for Android, Android OS v2.0 – 3.1

NS/BB = *NotifySync for BlackBerry* v4.9, BlackBerry OS v4.5-6.0

iOS4 = iOS 4 devices with multitasking capabilities

iOS4 w/ MDM API = Requires Production Certificate generated with Apple Enterprise Developer account

S60 = Symbian S60 3rd edition devices, v9.1

WM = Windows Mobile, v6.1/6.5 devices

wOS = webOS devices, v1.4.3/1.4.5, 2.0.0/2.0.1, 2.1.2

WP7 = Windows Phone 7

● A red dot in the charts indicates **ActiveSync only -** Currently, there is no *NotifyMDM* app available for WP7, wOS, or S60. Devices support the feature via the native ActiveSync app on the device. *(Note: BlackBerry devices have no native ActiveSync app and are only supported with the NMDM app)*

Policy Rules: All Devices

● A red dot indicates **ActiveSync only -** Currently, there is no *NotifyMDM* app available for WP7, wOS, or S60. Devices support the feature via the native ActiveSync app on the device. *(Note: BlackBerry devices have no native ActiveSync app and are only supported with the NMDM app)*

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
Application Control												
Allow unsigned applications	(ActiveSync) Determines whether the device allows the execution of unsigned applications which already exist on the device.							●	●			
Allow unsigned installation packages	(ActiveSync) Determines whether the device allows unsigned cabinet files (installers) to run, (i.e. whether an unsigned application can be installed using a cab file).							●	●			
Number of Whitelisted Applications	(ActiveSync) Applications expressly allowed to operate on a device. This can be used to make an exception for the unsigned applications policy or to make an exception to the blacklist for a specific build of an application. *Note: Requires ActiveSync protocol 12.1*							●	●			
Number of Blacklisted Applications	(ActiveSync) Applications expressly blocked from operating on a device. This only applies to applications that are							●	●			

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
	factory-installed on the device. *Note: Requires ActiveSync protocol 12.1*											
Audit Tracking												
Record Files on Device	Requires device to periodically send a list of all folders and files stored on the device and the SD card to the server. Displayed on the server in the User Profile: *File Archive*	•		•	•							
Record Phone Log	Requires the device to send all telephone log related information to the server. For BlackBerry devices, tracks only calls made after NotifyMDM registration. Future development may include call times and lengths; whether the call was roaming, incoming, or outgoing; usage tracking for work related calls verses personal, defined by a list of approved work numbers on the server.	•		•	•			•				
Record Text/Multimedia Message Log	Requires the device to send all Short Message Service (SMS) and Multimedia Messaging Service (MMS) related information to server. *BlackBerry devices:* • Do not track MMS messages • Track only texts made after NotifyMDM registration • Some devices use only MMS, so text messaging is not tracked *Android devices:* Text and MMS logging functionality may vary based on device manufacturer or carrier. (See *SMS & MMS Capabilities* document) *Windows Mobile devices:* Record only SMS messages.	•		•	•			•				

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
Record Location of Device (Latitude / Longitude)	Uses GPS or triangulation on the device to be able to locate where a user's device is at all times. Information is displayed using Google maps implementation. The device reports longitude and latitude as two separate values.	•		•	•	•		•				
GPS Location Accuracy	Allows administrators to specify a level of location accuracy. Accuracy primarily depends on use of cell tower vs. GPS (satellite) location methods; additional factors may be involved depending on the device type. Since improved accuracy generally results in increased battery usage, the level can be adjusted to facilitate a more efficient use of device battery. Set levels via the Policy Suite.	•		•	•	•		•				
Device Controls: Device Features												
Allow Bluetooth	(ActiveSync) Determines whether Bluetooth is allowed to operate on the device. There are three settings: 1. Don't allow Bluetooth 2. Allow only Bluetooth headsets 3. Allow all Bluetooth							•	•			
Allow Browser	(ActiveSync) Determines whether the use of the native web browser is allowed on the device. This setting may also prevent the use of third-party browsers that use the native browser as a basis for operation.					•	•	•	•			

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
Allow Camera	(ActiveSync) Determines whether the use of the device camera is allowed. Disabling the camera may limit the functionality of 3rd party apps that use the camera (Ex: Photoshop)					•	•	•	•			
Allow Infrared	(ActiveSync) Determines whether infrared connections are allowed to and from the device.							•	•			
Allow Internet Sharing from the Device (Tethering)	(ActiveSync) Determines whether the device can be used as a modem for a desktop or a portable computer.							•	•			
Allow Remote Desktop	(ActiveSync) Determines whether a remote desktop connection can be created from the device.							•	•			
Allow SD Card	(ActiveSync) Determines whether the use of an SD Card is allowed on the device.			•				•	•			
Allow Synchronization from a Desktop	(ActiveSync) Determines whether the device can synchronize with a computer through a cable, Bluetooth, or IrDA connection.							•	•			
Allow Text Messaging	(ActiveSync) Determines whether the device can send or receive text messages.							•	•			
Allow Wi-Fi	(ActiveSync) Determines whether wireless Internet access is allowed on the device.							•	•			

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
Device Controls: Email												
Allow HTML formatted Email	(ActiveSync) Determines whether email synchronized to the device can be in HTML format. *Not supported with systems operating with ActiveSync protocol 2.5, such as Exchange 2003.*			•	•			•	•			
Maximum HTML email body 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 may use Windows Live services, such as Hotmail, Office, Spaces, etc.							•	•			
Allow POP/IMAP Email	(ActiveSync) Determines whether the device can access POP3 or IMAP4 email on the device.							•	•			
Maximum email body truncation size (in KB)	(ActiveSync) Defines the maximum email body size of plaintext 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 max age are automatically removed from the device.			•	•			•	•	•		

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
	Not supported with systems operating with ActiveSync protocol 2.5, such as Exchange 2003.											
Maximum email age for synchronization	(ActiveSync) Defines the maximum age of email on the device. Email older than the max age are automatically removed from the device. *Not supported with systems operating with ActiveSync protocol 2.5, such as Exchange 2003.*			•	•	•	•	•	•	•		
Require manual sync when roaming	(ActiveSync) Enforces the use of manual synchronization on the device while roaming to avoid the often higher data costs incurred with automatic synchronization.			•	•	•	•	•	•			
File and Application Management												
File Share	Create a directory of folders and files to make accessible to users. Users access files directly through the NotifyMDM app. Set permissions for access per Policy Suite.	•		•	•	•		•				
Mobile Apps	Create a list of recommended apps. The list may consist of apps which users access directly through *NotifyMDM* or through links to the apps in device application stores. Available mobile applications are determined by device type. Set permissions for access per Policy Suite. (*NMDM for Windows Mobile* app will	•		•	•	•						

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
	support this in a future release.)											
Security: Password												
Require Password	(ActiveSync) Forces the device to require a lock password.	●	●	●	●	●	●	●	●	●	●	●
Enable password recovery	(ActiveSync) This allows or disallows a user to issue, from the device, 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. Note: Requires ActiveSync protocol 12.0 or 12.1			●	●							
Allow Simple Password	(ActiveSync) Determines whether or not a password may 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.*			●	●	●	●	●	●	●		●
Require Minimum Password Length	(ActiveSync) Forces the device to require a password with a specified minimum length.	●	●	●	●	●	●	●	●	●	●	●
Minimum Password Length	(ActiveSync) Defines the minimum password length.	●	●	●	●	●	●	●	●	●	●	●
Require Alphanumeric Password	(ActiveSync) Forces the device to require a device password to contain both letters and numbers.	●	●	●	●	●	●	●	●		●	●
Minimum Number of Complex Characters	(ActiveSync) Forces the device to require a minimum number of complex characters			●	●	●	●	●	●			

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
	(symbols) in the password. If alphanumeric password is not required then this is not enforced.											
Require 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.*			•	•	•	•	•	•	•		
Password expiration in days	(ActiveSync) Defines the number of days a password may be used before it expires.			•	•	•	•	•	•	•		
Require Device Password History	(ActiveSync) Forces the device to disallow passwords that have been used in the recent past to be re-used. The number of stored past passwords is configurable. *Not supported with systems operating with ActiveSync protocol 2.5, such as Exchange 2003.*			•	•	•	•	•	•	•		
Number of passwords stored	(ActiveSync) Defines the number of device passwords stored to prevent users from reusing them too soon.				•	•	•	•	•	•		
Enable Password Echo	After the specified number of password entry attempts are made, the last password entered will be unmasked to allow the user to see the error they are making.				•							
Begin password echo after attempts	Define the number of unlock attempts before echoing begins.				•							

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
Security: Encryption												
Require Device Encryption	(ActiveSync) Determines whether the device encrypts stored data. *Not supported with systems operating with ActiveSync protocol 2.5, such as Exchange 2003.* Note that iOS4 devices (3GS and 4) have hardware encryption that is always enabled. The ActiveSync policy is not used to enable/disable. *For Android w/ native ActiveSync account,* supported on the Motorola Droid Pro(OS 2.2) and devices with OS 3.0.0 or greater. For *Android w/ TouchDown*, only TouchDown data is encrypted (email, calendar, contacts, tasks). With *NotifySync for BlackBerry* only *NotifySync* data is encrypted (email).	•	•	•	•	•	•	•	•			
Require Encryption on the Storage Card	(ActiveSync) Forces the device to encrypt the file system of a storage card. For *Android w/ TouchDown*, only TouchDown files are encrypted (email attachments that have been downloaded are encrypted using TDES; attachments are still unreadable if card is moved to another device).			•				•	•			

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
Security: Duress												
Enable Duress Notification	A notification is sent to the specified email address if the user is forced to unlock the device under duress.				•							
Duress Notification Email	Defines the email address to which the duress notification is sent.				•							
Security: Device Inactivity and Locking												
Require Max Inactivity Time Device Lock	(ActiveSync) Forces the device to lock after a set number of minutes of user inactivity. This value serves as a maximum. This is also known as "Time without user input before password must be re-entered."	•	•	•	•	•	•	•	•	•	•	•
Max Inactivity Timeout (in minutes)	(ActiveSync) Define the numbers of minutes of inactivity before the device locks. If Challenge Timeout is being enforced, the Max Inactivity Timeout should be less than Challenge Timeout.	•	•	•	•	•	•	•	•	•	•	•
Require Device Challenge Timeout	Forces the device to enable a challenge timeout. A lock is initiated regardless of activity and is intended to challenge the use of a lost or stolen device.				•							
Max Device Challenge Timeout	Define 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 Max Inactivity Timeout is being enforced, the Challenge Timeout				•							

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
	should be greater than Max Inactivity Timeout.											
Customizable Lock Message	Enable the lock message and enter the text to be displayed when device is locked.				•							
Audible Alert On Lock	When enabled, this setting will cause 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 if applicable the device thief. The noise will continue 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. Administrator can also disallow a grace period by selecting "*Immediately*" or choose not to impose a limit by selecting "*None*."					•						
Wipe device on Failed Unlock Attempts	(ActiveSync) After the specified number of password entry attempts are made, data is cleared from the device. Functionality varies by device. *Android or Android w/TouchDown (requires OS v2.2 or greater)*: 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. *Android w/TouchDown (using OS v2.1 or*	•	•	•	•	•	•	•	•	•	•	•

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
	older): Wipes only *NotifyMDM* information. *BlackBerry:* Removes all mail and PIM data associated with the *NotifySync* / *NotifyMDM* application, and locks the device if Require Password is enabled. Erases *NotifySync* data from SD card. *iOS:* 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. *WM*: Device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Erases SD card only on *Professional* devices. *S60, webOS, and WP7:* Device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state in was in when purchased. Erases SD card on Symbian devices.											
Maximum number of unlock attempts	(ActiveSync) Defines the number of unlock attempts before the device-initiated wipe is performed.	•	•	•	•	•	•	•	•	•	•	•
Security: Emergency Calls												
Enable emergency calls when locked	Allows the device to make emergency calls in a locked state. Allows emergency numbers to be specified for allowed calls on a locked device: ambulance, fire, police, and one other emergency number.				•							

Policy Suite Rules: All Devices	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
S/MIME Settings												
Require signed SMIME messages	When enabled, this setting forces the device to send digitally signed S/MIME messages.							•	•	•		
Require encrypted SMIME messages	When enabled, this setting forces the device to send encrypted S/MIME messages.							•	•	•		
Require signed SMIME algorithm	This setting specifies the algorithm to be used for signing messages. Options are: SHA1, MD5.							•	•	•		
Require encryption SMIME algorithm	This setting specifies the algorithm to be used for encrypting messages. Options are: TripleDES, DES, RC2128bit, RC264bit, RC240bit.							•	•	•		
Allow SMIME Encryption algorithm negotiation	This setting enables/disables the device from negotiating the encryption algorithm used for signing messages. Options are: Do not negotiate, Negotiate only strong algorithms, Negotiate any algorithm.							•	•	•		
Allow SMIME soft certs	This setting enables/disables the device from using soft certificates to sign outgoing messages.							•	•	•		

Security: All Devices

Security	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS4	iOS4 w/MDM API	iOS4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
Security Commands													
Disable/Enable Device	Disables or enables device connection with the *NotifyMDM* server.	•	•	•	•	•	•	•	•	•	•	•	•
Selective Wipe	Administrators or end users can issue a selective wipe command. Functionality varies by device. *Android w/ native ActiveSync account (requires OS v2.2 or greater)*: Removes the *NotifyMDM* account information. *Android w/TouchDown (using any supported OS)*: Removes all mail and PIM (calendar, contact, tasks) data associated with the *TouchDown* application and returns *TouchDown* to a pre-registration state. Erases *TouchDown* data from the SD Card. Removes the *NotifyMDM* account information. Note: When the *Clean SD card on Remote Wipe* option in the TouchDown *Advanced Settings* is enabled, SD card is completely erased. *BlackBerry:* Removes all mail and PIM data associated with the *NotifySync*	•		•	•		•							

Security	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS4	iOS4 w/MDM API	iOS4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
	application, and locks the device if *Require Password* is enabled. *iOS4 with (APNs) Enterprise Developers Certificate:* Removes all mail and PIM (calendar and contacts) data controlled by *NotifyMDM*. iOS MDM API functionality allows for *Selective Wipe* to be applied immediately* to iOS 4 devices. * *Command is applied immediately, however, device is capable of postponing the action.*												
Wipe Storage Card	Administrators or end users can remotely wipe all data from the device's storage card.	•		•	•				•				
Full Wipe	Administrators or end users can issue a full wipe command. Functionality varies by device. *Android w/ native ActiveSync account (requires OS v2.2 or greater)*: 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. *Android w/TouchDown (requires OS v2.2 or greater)*: Device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Does not erase SD card. Note: When the *Clean SD card on Remote Wipe* option in the TouchDown *Advanced Settings* is enabled, SD card is completely erased. *Android w/TouchDown using OS v2.0 or 2.1: Full Wipe* not available – use *Selective Wipe* option.	•	•	•	•	•	•	•	•	•	•	•	•

Security	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS4	iOS4 w/MDM API	iOS4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
	BlackBerry: Removes all mail and PIM data associated with the *NotifySync* application and removes the *NotifySync* / *NotifyMDM* accounts. Locks the device if *Require Password* is enabled. Erases the entire SD card. *iOS:* 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. *iOS4 with (APNs) Enterprise Developers Certificate:* iOS MDM API functionality allows for *Full Wipe* to be applied immediately to iOS 4 devices. *WM*: Device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Erases SD card only on *Professional* devices. *S60, webOS, and WP7:* Device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Erases SD card on Symbian devices.												
Lock Device	Administrators or end users can remotely lock the device, requiring an unlock password to be entered before the device can be used. *Android or Android w/TouchDown:* requires OS v2.2 or greater. *iOS4 with (APNs) Enterprise Developers*	•		•	•		•		•				

Security	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS4	iOS4 w/MDM API	iOS4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
	Certificate: iOS MDM API functionality allows for *Lock Device* to be applied immediately to iOS 4 devices.												
Clear Passcode	Passcode will be cleared. If passcode is required by the user's policy, the user will be prompted to enter a new passcode.						•						
Network Connection Security and Configuration													
SCEP (Simple Certification Enrollment Protocol	Setup SCEP settings for devices.					•	•						
VPN (Virtual Private Network)	Setup VPN's for devices. Current Functionality: IPSec (Cisco protocol)					•	•						
Wi-Fi	Setup WiFi settings using various levels of security including WEP, WPA, and WPA2.					•	•						

Device Statistics: All Devices

Device Statistics	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS4 w/MDM API	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
Last Sync	The date and time of the last successful synchronization with the server.	•		•	•	•	•		•				
Battery Level	Displays the percentage of battery life left for the device.	•		•	•	•	•		•				
Battery Status	Displays whether the device battery is charging or unplugged.	•		•	•	•	•		•				
NotifyMDM Application Language	Name of the language the NotifyMDM device application is using.	•		•	•	•	•		•				
NotifyMDM Application Version	Displays the version number of the NotifyMDM device application.	•		•	•	•	•		•				
Data Usage *(Downloaded Data, Uploaded Data)*	Displays the amount of data being used by the device over the network since the last time the device booted. Data usage is not recorded when devices uses WiFi. BlackBerry: *Limited to GSM devices. Usage statistics for incoming and outgoing data are sum-totals of all networks.* Android: *Usage Statistics for incoming and outgoing data are sum-totals of all networks, as well as a subtotal for the*	•		•	•								

Device Statistics	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS4 w/MDM API	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
	cellular network alone.												
Device IMEI	The International Mobile Equipment Identify number. See http://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity *BlackBerry:* Limited to GSM devices.	•		•	•		•		•				
Device Model	Displays the device model.	•		•	•	•	•		•				
Device UID	Displays the device UID.				•				•				
Device Type	Displays the device type as reported by the device.	•		•	•	•	•		•				
Device Memory Capacity	Displays the total of the used and unused memory on the device.	•		•	•	•	•		•				
Device Free Memory	Displays the amount of free memory left on the device. *(Labeled "Available Device Capacity" for iOS4 w/MDM API devices.)*	•		•	•		•		•				
Network Type	Displays the network type the device is using.	•		•	•	•	•		•				
OS Language	Name of the language the device OS is using.	•		•	•				•				
OS Version	Displays the device OS version.	•		•	•	•	•		•				
Phone Number	Displays the device's phone number.	•		•	•		•		•				
Device Ownership	Tracks who owns on the device: Company or Personal	•		•	•	•	•		•				
Phone Usage	Displays the phone minutes used in the	•		•	•		•		•				

Device Statistics	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS4 w/MDM API	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
	last 30 days. This is calculated from Phone logs.												
Roaming	Displays a simple yes or no if the device is roaming.	•		•	•		•		•				
SD Card Status	Displays if there is an SD card in the device. Note: iOS4 devices do not have SD Card capability.	•		•	•				•				
SD Card Free Memory	Displays the amount of free memory left on the device's storage card. *Note that iOS4 devices do not have SD Card capability.*	•		•	•				•				
SD Card Total Memory	Displays the total of the used and unused memory on the device storage card.	•		•	•				•				
Signal Level	Displays the signal strength using a percentage value.	•		•	•				•				
Device Name	The name given via iTunes.						•						
Build Version	iOS build number.						•						
Model Name	Name of device model.						•						
Model	Device's internal model number.						•						
Product Name	The model code for the device.						•						
Serial Number	Device's serial number.						•						
Cellular Technology	Cellular technology 0 = none 1 = GSM						•						

Device Statistics	Description	Anrd	Anrd w/o NMDM	TD/A	NS/BB	iOS 4	iOS4 w/MDM API	iOS 4 w/o NMDM	WM	WM w/o NMDM	WP7	wOS	S60
	2 = CDMA												
MEID	The device's MEID (CDMA)						•						
Modem Firmware Version	The baseband firmware version.						•						
ICCID	The ICC identifier for the installed SIM card (if applicable)						•						
Bluetooth MAC	Bluetooth MAC address.						•						
WiFi MAC	WiFi MAC address.						•						
Current Carrier Network	Name of current carrier network.						•						
SIM Carrier Network	Name of home carrier network. (Note: Applies to CDMA in spite of its name.)						•						
Carrier Settings Version	Version if currently installed carrier settings file.						•						
Data Roaming Enabled	Current setting of the Data Roaming setting.						•						
Subscriber MCC	Home Mobile Country Code						•						
Subscriber MNC	Home Mobile Network Code						•						
Current MCC	Current Mobile Country Code						•						
Current MNC	Current Mobile Network Code						•						

Policy Rules: iOS Device Specific

Policy Suite Rules: iOS Specific	**Description**	iOS 4	iOS 4 w/o NMDM	iOS4 w/MDM API
Device Features				
Allow Video Conferencing	Determines whether the user may receive or place video calls. *"Allow Camera" in the "Device Controls" must be enabled as well.*	•		•
Allow Voice Dialing	Determines whether the user may dial their phone using voice commands.	•		•
Allow Screenshot	Determines whether or not the user may save a screenshot of the device display.	•		•
Allow Explicit Content	Determines whether or not explicit music or video content purchased from the iTunes store is hidden.	•		•
Allow Automatic Sync When Roaming	When disabled, devices that are roaming will sync only when an account is accessed by the user.	•		•
Force Encrypted Backup	When disabled, users can choose whether or not device backups, performed in iTunes, are stored in encrypted format on their computer.	•		•
Applications				
Allow Application Installation	When disabled, App Store is disabled and the icon is removed from the device Home screen. In addition, users are prevented from installing applications made available through the	•		•

Policy Suite Rules: iOS Specific	**Description**	**iOS 4**	**iOS 4 w/o NMDM**	**iOS4 w/MDM API**
	NotifyMDM Mobile Apps list.			
Allow In App Purchases	Determines whether or not users can make in-app purchases.	•		•
Allow YouTube	Determines whether the use of YouTube is allowed on the device. If disabled, icon is removed from the Home screen.	•		•
Allow iTunes	Determines whether the use of iTunes is allowed on the device. If disabled, icon is removed from the Home screen and users cannot preview, purchase, or download content.	•		•
Safari Browser				
Allow Safari	Determines whether use of the Safari web browser is allowed on the device. If disabled, the Safari icon is removed from the Home screen and it prevents users from opening web clips. Disabling Safari may also prevent the use of third-party browsers. *"Allow Browser" in the "Device Controls" must also be enabled.*	•		•
Accept Cookies	Determines the Safari cookie policy – Whether the device accepts all cookies, no cookies, or only cookies from sites that were directly accessed.	•		•
Allow Auto-fill	Determines whether or not Safari remembers what users enter in web forms.	•		•
Allow JavaScript	Determines whether or not Safari ignores JavaScript on websites.	•		•
Allow Pop-ups	Determines whether or not Safari's pop-up blocking feature is enabled.	•		•
Force Fraud Warning	Determines whether or not Safari attempts to prevent the user form visiting websites identified as being fraudulent of compromised.	•		•

Policy Suite Rules: iOS Specific	**Description**	iOS 4	iOS 4 w/o NMDM	iOS4 w/MDM API
Ratings				
Rating Region	Determines the media content rating scale used by a particular region.	•		•
Application Ratings	Determines the maximum allowed ratings for apps.	•		•
Movie Ratings	Determines the maximum allowed ratings for movies.	•		•
TV Show Ratings	Determines the maximum allowed ratings for TV shows.	•		•
Security				
Allow Profile Removal	Determines whether or not an iOS user may delete the NotifyMDM configuration profile from the device. Includes an option to allow deletion with the use of a password.	•		•
Profile Removal Password	Defines the password with which a user may remove the profile.	•		•
iOS MDM				
Record Installed Applications	Access and record applications installed on devices.			•
Record Installed Configuration Profiles	Access and record configuration profiles installed on devices.			•

Policy Rules: TouchDown Specific

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

Policy Suite Rules: TouchDown Specific	**Description**	TD/A	Anrd	Anrd w/o NMDM
	option is not visible and the function is disabled. At least one of two suppression rules must be enabled in order for this to function: *Allow appointment alert configuration* or *Allow email alert configuration*.			
Show TouchDown PIN	This setting is dependent upon the ActiveSync policy, *Require Password*. When *Require Password* is disabled, this setting has no effect and neither the device or the TouchDown app will lock or require a password. When *Require Password* is enabled, behavior varies by Android OS version. *For Android OS 2.2 or greater* – The device will lock and require a password. The *Show TouchDown PIN* setting determines whether the TouchDown (TD) app locks/requires a password as well. When enabled, TD locks. When disabled, TD does not lock. *For Android OS 2.1 or less* – When the *Show TouchDown PIN* setting is enabled, the device does not lock, but TouchDown (TD) does. When it is disabled, neither the device or TD app locks, however, user is still prompted to create a PIN/password.	•		
Show calendar info on notification bar	Determines whether appointment subjects are displayed in the device notification bar when reminders are shown. To successfully display notifications, the following TouchDown settings must also be configured on the device: In the Advanced TouchDown Settings, enable the *Appointment reminders at non-peak times* options and configure *Appointment Alerts* to "*Use system settings."*	•		

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

Policy Suite Rules: TouchDown Specific	**Description**	TD/A	Anrd	Anrd w/o NMDM
Allow TouchDown task widget	Determines whether or not TouchDown task widget shows data.	•		
Allow TouchDown universal widget	Determines whether or not TouchDown universal widget shows email, calendar and task data.	•		
Show widget data when TouchDown is locked	Determines whether widget data will be 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 will synchronize when users copy contacts to the device phone book. Choosing all or some of the fields is a prerequisite for the suppression rules: *Allow copy phone format options* and *Allow update contact changes to phone options*	•		
Suppressions				
Suppression configuration	Choose which options to hide or expose to TouchDown users. Disabling an option will suppress or hide it on the device and locks how it was previously set on the device. Enabling an option will allow the user to access and change it on the device.	•		
Suppressions: Calendar, Contacts, Tasks				
Allow appointment alert configuration	Enables users to customize the alerts displayed for appointment reminders.	•		
Allow appointment reminders at non-peak times option	Enables users to allow appointment reminders during periods when the device is not synchronizing.	•		
Allow appointment synchronization option	Enables users to set how many days worth of appointments to keep on the device.	•		
Allow category configuration	Enables users to select colors for contact, event, and task categories.	•		

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

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

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

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

Policy Suite Rules: TouchDown Specific	**Description**	**TD/A**	**Anrd**	**Anrd w/o NMDM**
Suppressions: Synchronization				
Allow defer server updates option	When enabled, TouchDown updates will not sync to the server until: the next scheduled sync occurs, an item arrives via direct push, or 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 device is roaming, but users may initiate a manual sync.	•		
Allow notify on password failure option	When enabled, user is notified if synchronization fails due to a user password issue.	•		
Allow notify on polling failure option	When enabled, user is notified if synchronization fails.	•		
Allow notify on successful polling option	When enabled, user is notified when synchronization is successful.	•		
Allow peak time configuration	Enables users to set the hours during which TouchDown synchronizes with the server.	•		
Allow poll during off-peak times option	When enabled, during off peak times (times outside the peak schedule), TouchDown will pull down updates from the server when user sends an email, reply, or forward from the device.	•		