NotifyMDM
Mobile Device Management

NotifyMDM System Security Guide

This guide provides information on . . .

. . . An overview of NotifyMDM System Security

Table of Contents

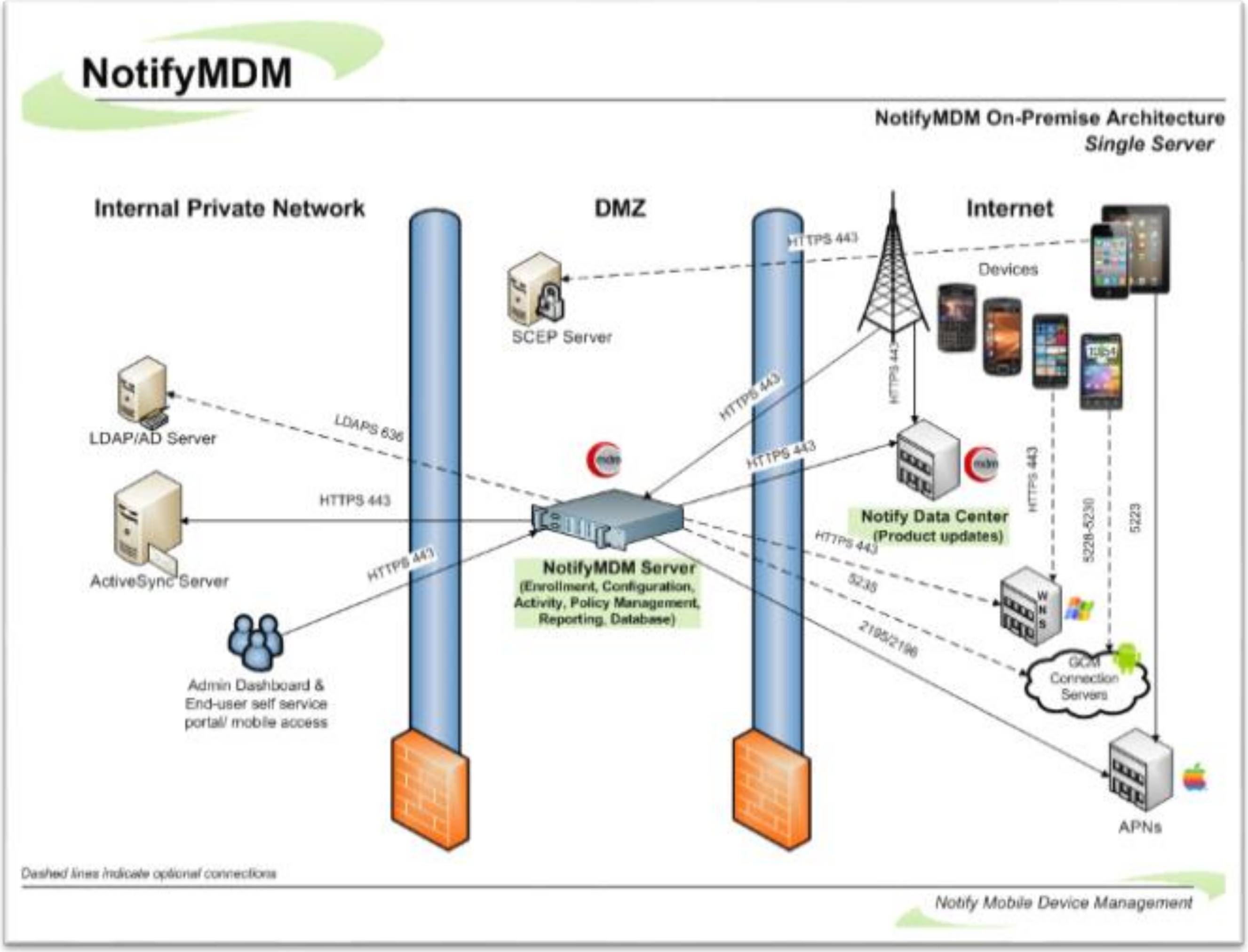
Architecture

NotifyMDM consists of an ***SQL Database Component*** and a ***Web/HTTP Server Component***. The components may be installed on a single server or multiple servers. The architecture you choose will depend on system size and complexity.

In addition to the setups illustrated below, a reverse proxy setup is also supported as long as the proxy is sufficiently scalable. For the long term, redundant proxies may be advisable to help ensure high availability. Achieving redundancy through SQL and web clusters is a good way to ensure high availability.

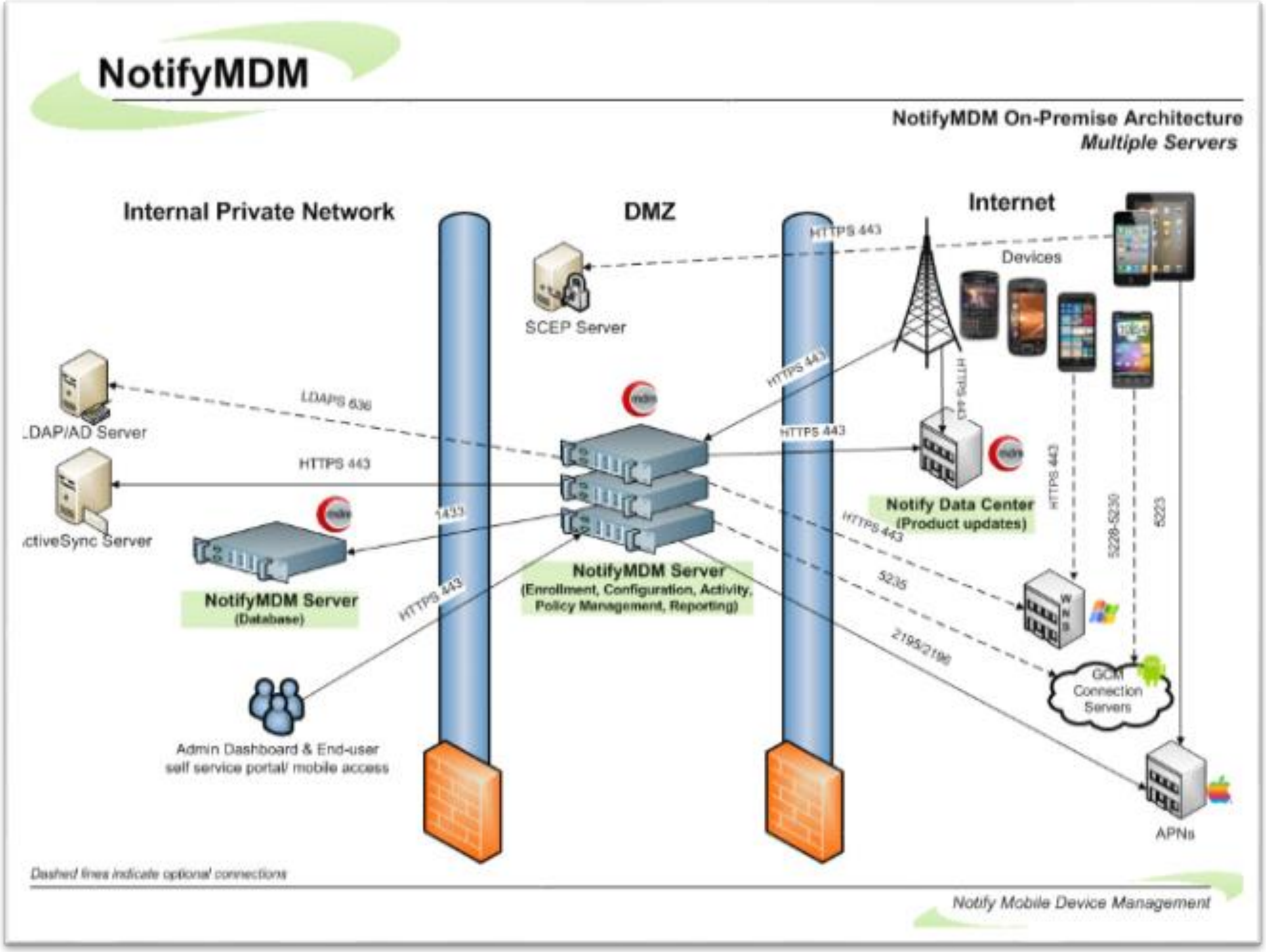
Single Server Configuration Diagram

Typical configuration suitable for general-purpose deployment where a single server meets all the requirements needed for installation.



Multiple Server Configuration Diagram

Deployment options for larger, more complex deployments where a single server does not meet all the requirements needed for installation.



See related topics:

System Performance: Sizing/Tuning (found on the NotifyMDM portal under Server Documentation).

High Availability Configuration (found on the NotifyMDM portal under Server Documentation).

To simplify a description of the *NotifyMDM* security system, we have grouped the security features into several categories, which we refer to as the “layers” of security.

- Server to Server Data Transmission Security
- Database Security: Data-at-Rest Encryption
- Server Log File Security
- Device to Server Data Transmission Security
- Device Security

NotifyMDM System Security

Terms:

***FIPS140-2 Encryption**: Federal Information Processing Standard. A government computer security standard used to accredit cryptographic modules.*

***SSL Encryption**: Secure Socket Layer Security. Using SSL to secure data exchanges provides an encrypted tunnel between the NotifyMDM servers and other servers or devices.*

***TLS Encryption**: Transport Layer Security Encryption. TLS is a FIPS 140-2 compliant encryption protocol that provides an encrypted tunnel through which sensitive data can travel. You can enable TLS through IIS. However, this may limit the types of devices that can connect to the NotifyMDM server since not all devices support TLS.*

FIPS 140-2 Encryption

FIPS 140-2 is an information security standard developed by governments in both the United States and Canada for the protection of sensitive information in IT and telecommunications systems within non-military federal government agencies. It mandates that agencies use strong validated encryption algorithms to implement a DLP strategy that protects sensitive information both at-rest and in-motion.

Products described as FIPS 'compliant' or 'enabled' or 'conforming' or 'equivalent' do not meet this requirement. There is a difference between these terms and the term 'validated' when describing claims to support FIPS 140-2 certified encryption. In order to achieve certification, vendors' cryptographic modules are validated by an independent 3rd party lab using CMVP (Validation Program), a rigorous four step certification process that verifies correct implementation of the modules. Any vendor that has achieved certification has a FIPS 140-2 certificate issued in their name. Notify Technology Corporation is one such vendor.

Notify Technology Corporation has incorporated FIPS 140-2 certified libraries into the *NotifyMDM* mobile management console and mobile app solutions to provide end-to-end security for data-at-rest and data-in-transit.

What follows are lists of the encrypted fields in each of the *NotifyMDM* components.

***NotifyMDM for Android* app**	
Table	**Column**
AccountsTable	Password

***NotifyMDM for iOS* app**
Shared user password User password Managed apps URL Profile download URL

NotifyMDM Server

Table Name	**Encrypted Column Name**
Administrators	Password
Administrators	PinCode
Apps	ManifestFile
CertificateAuthorities	Password
Certificates	CertificatePassword
Devices	RoverPinReset
Files	Data
GCMServerInfo	APIKey
iOSAPNUsers	Password
iOSDEPServerTokenInfo	ServerTokenData
iOSDEPServerTokenInfo	ConsumerKey
iOSDEPServerTokenInfo	ConsumerSecret
iOSDEPServerTokenInfo	AccessToken
iOSDEPServerTokenInfo	AccesSecret
iOSGlobalHTTPProxy	Password
iOSMDM	PrivateKey
iOSMDM	EnterpriseAPNMessagingCertificatePassword
iOSSubscribedCalendarUsers	Password
LDAPServers	Password
LinkedServers	SOAPPassword
MailMessageLog	Message
MailMessageLog	HtmlMessage
MDMUsers	ConfiguratorIdentifier
MDMUsers	Password
Organizations	KNOXPremiumLicenseKey
Organizations	LicenseAttributes
Organizations	NPNSPrivateKeyPassword
SAMLIdentityProviders	Metadata
ServerInformation	LicensingPassword
ServerRSAKeyPair	PrivateKey
ServerRSAKeyPair	Publickey
SigningCertificates	PrivateKey
SMTPServers	Password
UserCertificates	CertificatePassword
User_CalDAV	Password
User_CardDAV	Password
Users_Email	IncomingMailPwd
Users_Email	OutgoingMailPwd
Users_Exchange	Password

Users_LDAP	Password
Users_SCEP	Challenge
Users_Vpn	Password
Users_WIFI	Password
UserSCEPSettings	Fingerprint
UserVpnSettings	SharedSecret
UserVpnSettings	ProxyAddress
UserVpnSettings	ProxyPassword
UserWIFISettings	Password
UserWIFISettings	ProxyPassword
VPPConfigurations	SToken
VPPConfigurations	Token
WEPKeys	WEPKey
CertificateAuthorities	SigningCertificate
DeviceLocations	Latitude
DeviceLocations	Longitude
DeviceLogs	LogData
AuditedFiles	FileData
TextMessageLog	BodyOfText
TextMessageAttachments	FileData
Devices	RecoveryPassword
iOSMDM	APNPrivateKey
Licenses	LicenseData
ServerUpdates	Archive

Server to Server Data Transmission Security

NotifyMDM requires the use of SSL or TLS with the server(s) where the *NotifyMDM Web/HTTP* component is installed, to meet best practices for security. NotifyMDM supports the use of SSL or TLS certificates from trusted Certification Authorities to ensure secure server to server data transmission.

- Server to server connections within the Internal Private Network may include connections between:
  - ActiveSync server and an On Premise NotifyMDM server
  - LDAP/AD server and an On Premise NotifyMDM server
  - SCEP server and an On Premise NotifyMDM server
- Connections from an On Premise NotifyMDM server to servers outside the Internal Private Network may include:
  - On Premise NotifyMDM server to Notify Data Center (product updates, etc.)
  - On Premise NotifyMDM server to Apple Data Center (when Apple Advanced MDM API is implemented through the application of an APNs certificate)

Database Security: Data-at-Rest Encryption

Sensitive data-at-rest is secured in the *NotifyMDM* database using AES encryption algorithm. *NotifyMDM* servers use a 256 bit encryption key size to encrypt user information in the database. *NotifyMDM*'s procedures for key storage and key derivation are FIPS compliant.

Encrypted database information includes:

- Passwords
- User Encryption Key
- Authentication Password (stored only if authenticating via *NotifyMDM*, not ActiveSync)
- Text Message Log (can be disabled so it will not be sent to the server)
- Location Data (can be disabled so it will not be sent to the server)
- Phone Log (can be disabled so it will not be sent to the server)
- Device Logging (can be disabled so it will not be sent to the server)
- File Archive (can be disabled so it will not be sent to the server)

The *NotifyMDM* database component itself is secured using built-in SQL Server security features. By default, *NotifyMDM* creates a single SQL Server login with access to the *NotifyMDM* database. Permissions can be set within SQL Server, as desired, to access the database by other SQL Server logins or by using Windows Authentication.

Server Log Security

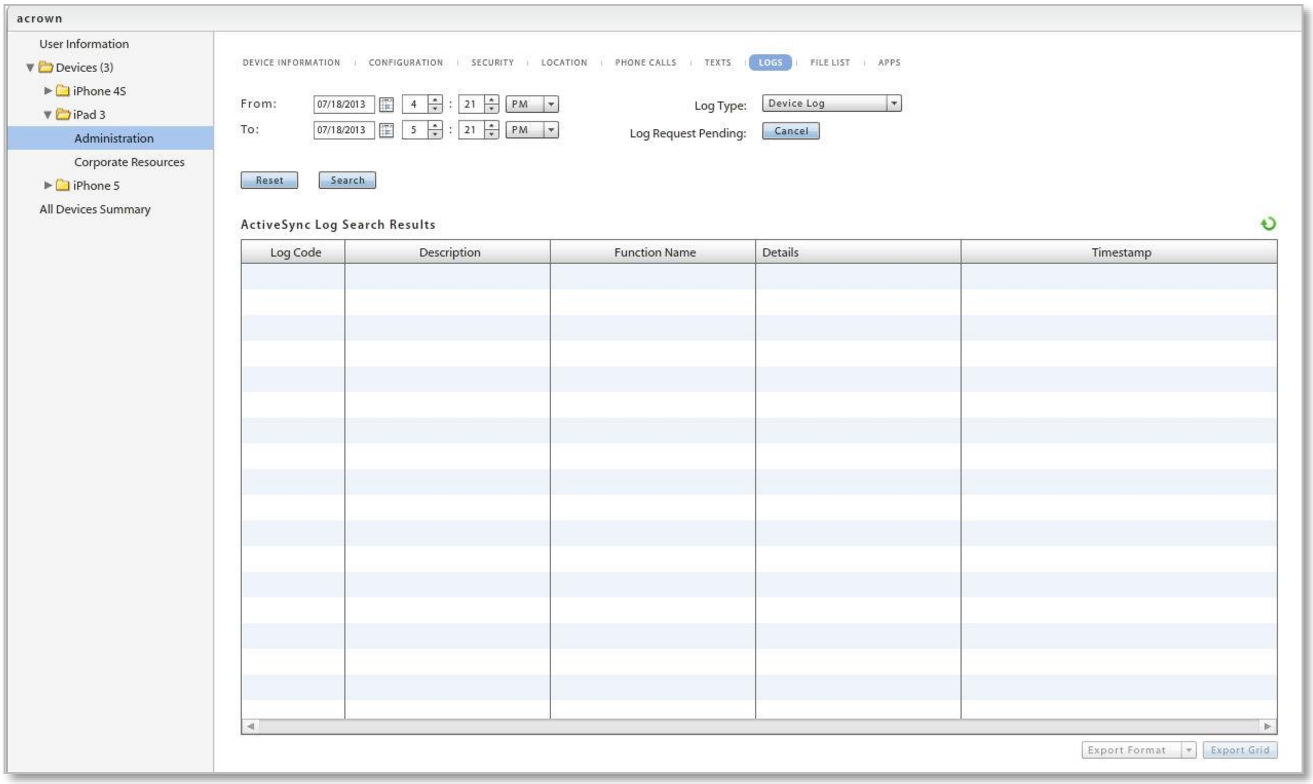
NotifyMDM Server error logging is intended to be used as a diagnostic tool by Technical Support staff.

Servers where the log files reside should, of course, be secured. In addition, administrators should limit access to the directory where the logs are contained.

Server logs are displayed in NotifyMDM dashboard and access to these views can be restricted via administrative login credentials. The data displayed in the Server Logging page of the dashboard is system level data and has no user associations. Displayed logging information that is associated with users is limited to *NotifyMDM* and ActiveSync synchronization data.

There is also a log file stored on the server that is not dependent on access to the database tables. This is secured by standard Windows authentication and file system security configurations.

In the Device Profile, there is also a way to request user level logs from the device. These logs assist administrators with diagnosing problems and in understanding the communications between devices and the server.



From: 07/18/2013 4 : 21 PM

To: 07/18/2013 5 : 21 PM

Log Type: Device Log

Log Request Pending: Cancel

ActiveSync Log Search Results

Log Code	Description	Function Name	Details	Timestamp

- For **BlackBerry and iOS platforms**, a log file will only have NotifyMDM-specific log entries.

  Examples of log entries for BlackBerry and iOS:

  - Beginning Sync
  - Ending Location Sync
  - Beginning Device Log Sync
  - Ending Device Log Sync
  - Registration status code: 200

    - Reg - Account Removed
    - DeviceStats returned: 200
    - GetAppListConnection returned: 200
    - Account loading

- For **Android**, a log file will have log entries encompassing NotifyMDM-specific logs, device logs, and the log entries from Touchdown (if installed and registered).

  Examples of log-entries for Android:

    - ConnectivityChange for mobile: CONNECTING/CONNECTING
    - ConnectivityChange for mobile: CONNECTED/CONNECTED
    - DISABLE_CLOCK: yes
    - DISABLE_NAVIGATION: yes
    - Attempting to switch to WIFI
    - Attempting to switch to BLUETOOTH_TETHER
    - Scheduling restart of crashed service
    - SyncHandler: Attempting to send device location command

Device to Web/HTTP Server Data Transmission Security

Device to Web/HTTP server data transmission must be secured by employing SSL or TLS. With SSL or TLS enabled, *NotifyMDM* transmits “data-in-motion” (information originating on a device or server) in an encrypted tunnel so it is secure in transit.

Data-in-motion includes both *NotifyMDM* traffic and ActiveSync server traffic that is proxied by the *NotifyMDM* server.

In extreme cases or where certain security standards are imposed, you might want or need to further secure the Web/HTTP server by locking down the virtual directories. Access to the *NotifyMDM* dashboard and the User Self-Administration Portal from external sources can be blocked. Pages accessed by mobile devices for synchronization, however, must be kept open. See instructions for locking down the virtual directories below.

Connections to the *NotifyMDM* server made by users may also include:

- Administrative access from sources either inside or outside the Internal Private Network via the web based NotifyMDM dashboard to an On Premise NotifyMDM server.
- Desktop or mobile access from sources either inside or outside the Internal Private Network via the web based NotifyMDM User Self Administration Portal to an On Premise NotifyMDM server.

These connections can also be secured using SSL or TLS.

All ‘Data-in-motion’ can be secured using the SSL or TLS protocols. The device-side has SSL; while the server-side has the options of SSL or TLS (the server automatically negotiates the best option, and hence uses TLS most of the time).

Implementation Guidelines: Device to Server Data Transmission Security

Enable SSL for device to Web/Http server communication.

- Install an SSL certificate on the server where the *NotifyMDM* Web/HTTP component resides and enable SSL (or TLS) in IIS.
- Use the ‘Require SSL’ option through IIS and instruct users to enroll with SSL enabled or enable it in the device settings.

Secure the Web/HTTP server by locking down virtual directories.
In extreme cases or where certain security standards are imposed, you might want or need to further secure the Web/HTTP server by locking down the virtual directories.

1. Open Windows Server Internet Information Services (IIS) Manager
2. Expand the directory and select **Sites** > **Default Web Site**.
3. At the root level, double-click **IP Address & Domain Restrictions**. (If *IP Address & Domain Restrictions* is not present, you must install the *IP and Domain Restrictions Role*. Right-click *Computer* and select *Roles*. Under the *Web Server (IIS)* section, click *Add Role Service*. Install the *IP and Domain Restrictions* role under *Security* in the popup window.)
4. From the *Actions* panel on the right, click **Edit Feature Settings** and set the value to **Deny**.
5. From the *Actions* panel, click **Add Allow Entry** and add the following rules to allow only *local* access to the dashboard and User Self-Administration Portal:
    a. IP: (the internal IP address of the *NotifyMDM* Server)
    b. IP: 127.0.0.1

   Add any other IP address, from which you will allow access, in the same manner.

The IP addresses that you added to the root level automatically populate for all the subdirectories, however, the *Feature Settings* value must be manually set to *Deny* for all but the *Sync* subdirectory. Select each *Default Web Site* subdirectory, **except *Sync***, and double-click *IP Address & Domain Restrictions*. Set the *Edit Feature Settings* to **Deny**.

Device Security

NotifyMDM device security implements proactive features that can help deter security breaches. It also includes reactive security options that can be implemented when a device is lost or stolen and therefore more vulnerable to a breach.

This section highlights *NotifyMDM's* core device security features.

Proactive Device Security Options

Device Data-at-Rest Encryption

Data-at-rest encryption on the device storage disk is supported by several device types and can be enforced through the *NotifyMDM* Policy Suite.

- Android with TouchDown – encrypts TouchDown data (email, calendar, contacts, tasks) only
    - Versions 7.x and higher – AES 256-bit
- Android (Native) devices - OS version 3.0; manufacturer/model dependent for OS versions less than 3.0
    - AES 128-bit
- BlackBerry – With *NotifySync for BlackBerry,* encrypts the *NotifySync* email
    - Secure (AES 128-bit)
    - More Secure (AES 192-bit)
    - Most Secure (AES 256-bit)
- iOS Devices – AES 256 bit
    - Note that iOS4 (3GS and 4) and iOS5 devices have hardware encryption that is always enabled. The ActiveSync policy is not used to enable/disable.
- Windows Phone – *This device does not currently support Data-at-Rest encryption.*

Device Rules: Lock Rules

<u>Inactivity Timeout</u>

- *BlackBerry, iPhone/ iPod touch/ iPad, Android Native, Android with TouchDown™, and Windows Phone platforms*
  The maximum inactivity timeout can be enforced by the server and an interval that does not exceed this maximum can be set on the device.

<u>Challenge Timeout</u>

- *BlackBerry*

  The *NotifyMDM* Challenge Timeout lock is initiated regardless of inactivity and is intended to challenge the use of the device if it is lost or stolen. It must be greater than the *Inactivity Timeout*.
- *iPhone/ iPod touch/ iPad, Android Native Android with TouchDown™, and Windows Phone platforms* – Not supported

Device Rules: Password Rules

<u>Device Password Expiration</u>

- *BlackBerry, iOS Device, Android Native (some models), Android with TouchDown^{TM}, and Windows Phone Platforms*
  If enabled, user is prompted to create a new password after a specified number of days. When the password expires, the device locks. The user must unlock it with the current password and then create a new password at the prompt.

Device Password History

- *BlackBerry, iOS Device, Android Native (some models), Android with TouchDown^{TM}, and Windows Phone Platforms*
  If enabled, this feature prevents users from reusing passwords too soon. On BlackBerry, iOS, and Windows Phone devices, the server can enforce the number of passwords a device should store (1 to 50) EX: If the number of stored passwords is 10, you will not be able to use the past ten passwords. When you create the 11th password, the oldest stored password becomes available for use again.

Reactive Device Security Options

NotifyMDM supports remote WIPE and LOCK executions and local (device) WIPE executions (where applicable). Remote WIPE and LOCK are controlled via the *NotifyMDM* dashboard and work when wireless is on.

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. SD card is not erased.
- 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. This 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.
- BlackBerry - This removes the *NotifyMDM* account and locks the device if Require Password is enabled. It also erases the entire SD card, including saved attachments.
- iOS - This deletes all data and applications from the device. The device returns to the state it was in when purchased (factory settings).
- iOS with APNs Certificate - iOS MDM API functionality allows for Full Wipe to be applied immediately to iOS devices.
- WebOS and WP7 - This deletes all data and applications from the device. The device returns to the state it was in when purchased (factory settings).

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) - This removes the *NotifyMDM* account information.
- Android w/ TouchDown (using any supported OS) - This removes all mail and PIM (calendar, contact, tasks) data associated with the TouchDown application and returns TouchDown to a pre-registration state. It erases TouchDown data from the SD Card and 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 - This removes all mail and PIM data associated with *NotifyMDM* and locks the device if Require Password is enabled.

- iOS with APNs Certificate - This 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 devices. * Command is applied immediately; however, device is capable of postponing the action.

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 and Android with TouchDown (OS 2.2 or greater), and BlackBerry support this policy.
- iOS devices interfacing with servers employing Apple's advanced MDM functionality support this policy.
- Windows Phone devices – Not supported.

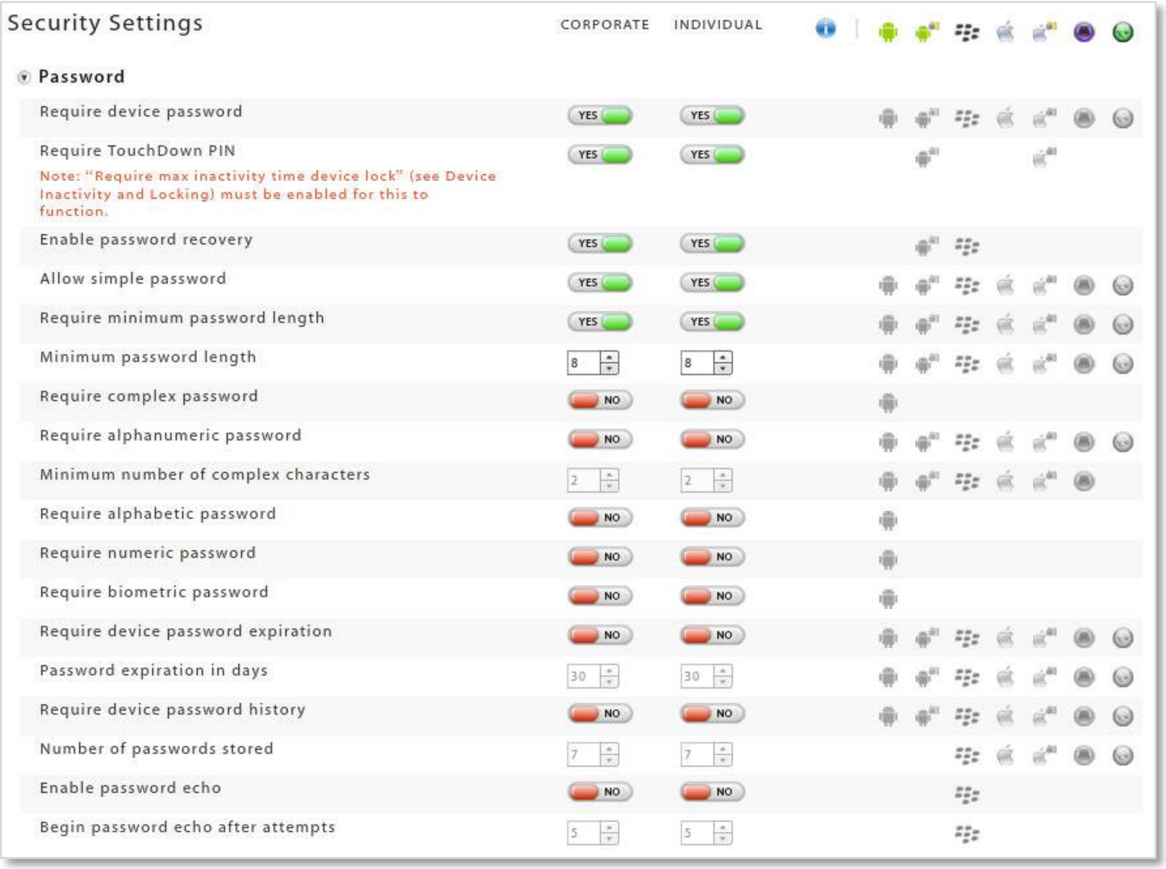
Wipe Storage Card

Administrators or end users can remotely wipe all data from the device's storage card. This is supported for Android and BlackBerry platforms.

Implementation Guidelines: Preventing Device Breaches

The *NotifyMDM* dashboard is considered the main point of control and security enforcement. From here, administrators can ensure that security is being optimally maintained through continuous monitoring of the connected user devices. All administrative actions indicated in the Device Security section of this document can be executed through this dashboard.

NotifyMDM provides a number of preventative policy settings designed to avert security breaches with regard to mobile devices. Lock, password, and encryption rules are enforced from the **Organization Management: Policy Suites** view of the *NotifyMDM* dashboard.

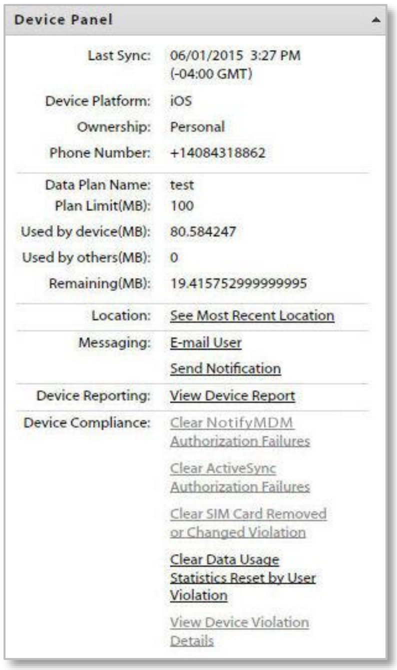


Security Settings

Password

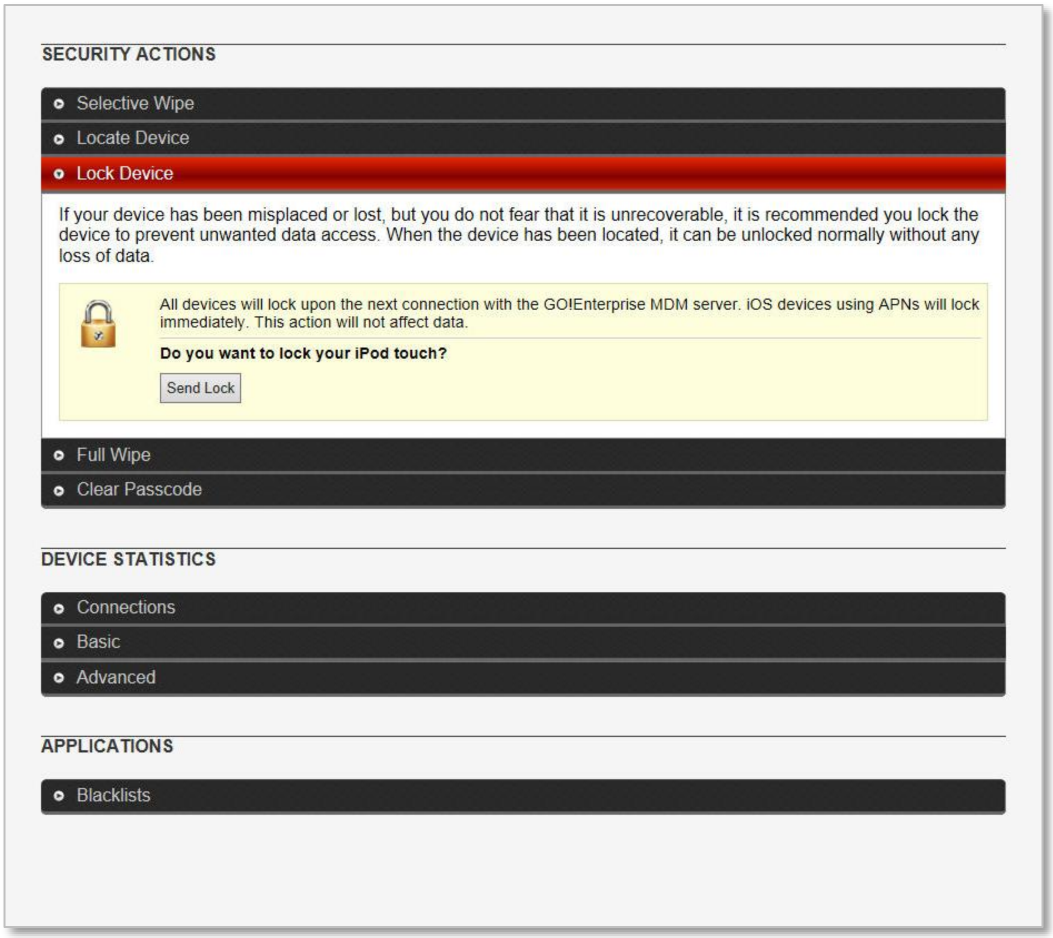
	CORPORATE	INDIVIDUAL
Require device password	YES	YES
Require TouchDown PIN Note: "Require max inactivity time device lock" (see Device Inactivity and Locking) must be enabled for this to function.	YES	YES
Enable password recovery	YES	YES
Allow simple password	YES	YES
Require minimum password length	YES	YES
Minimum password length	8	8
Require complex password	NO	NO
Require alphanumeric password	NO	NO
Minimum number of complex characters	2	2
Require alphabetic password	NO	NO
Require numeric password	NO	NO
Require biometric password	NO	NO
Require device password expiration	NO	NO
Password expiration in days	30	30
Require device password history	NO	NO
Number of passwords stored	7	7
Enable password echo	NO	NO
Begin password echo after attempts	5	5

Wipe and Lock commands are issued from the **Smart Devices and Users** page (Device Panel) on the *NotifyMDM* dashboard. Users may also issue the commands via the User Self Administration Portal.



Device Panel

Last Sync:	06/01/2015 3:27 PM (-04:00 GMT)
Device Platform:	iOS
Ownership:	Personal
Phone Number:	+14084318862
Data Plan Name:	test
Plan Limit(MB):	100
Used by device(MB):	80.584247
Used by others(MB):	0
Remaining(MB):	19.415752999999995
Location:	See Most Recent Location
Messaging:	E-mail User Send Notification
Device Reporting:	View Device Report
Device Compliance:	Clear NotifyMDM Authorization Failures Clear ActiveSync Authorization Failures Clear SIM Card Removed or Changed Violation Clear Data Usage Statistics Reset by User Violation View Device Violation Details



If your device has been misplaced or lost, but you do not fear that it is unrecoverable, it is recommended you lock the device to prevent unwanted data access. When the device has been located, it can be unlocked normally without any loss of data.

All devices will lock upon the next connection with the GO!Enterprise MDM server. iOS devices using APNs will lock immediately. This action will not affect data.

Do you want to lock your iPod touch?

User Self Administration Portal

NotifyMDM On-Demand Security

NotifyMDM On-Demand is the outsourced solution chosen by many organizations not wanting to manage a *NotifyMDM* server on premise. It is a simple solution to immediate mobility needs, and offers the flexibility of migration to an On Premise solution should growth require it.

This section of the document describes the standards in place for securing the On-Demand service.

Data Center Architecture

NotifyMDM On-Demand is hosted in a state-of-the-art, hardened data facility located in Youngstown, Ohio. The data center is ***SSAE16* certified**. The data center undergoes regular audits of control objectives and control activities, which include controls over information technology and related processes.

Data center physical features include:

- Multi-layered security control procedures: non-descript building with no public access, 24/7 closed-circuit video and alarm monitoring, biometric entry system, locked server cage area
- Uninterruptible redundant AC and DC power, onsite backup power generators
- HVAC redundant design for maximum temperature and humidity control
- Smoke detection and dry-pipe fire suppression systems

Physical and logical security of *NotifyMDM On Demand* servers:

- Dual redundant firewalls
- Load balanced and redundant gateway server clusters
- Servers fed by dual power sources
- Virus protection, antivirus signatures updated daily

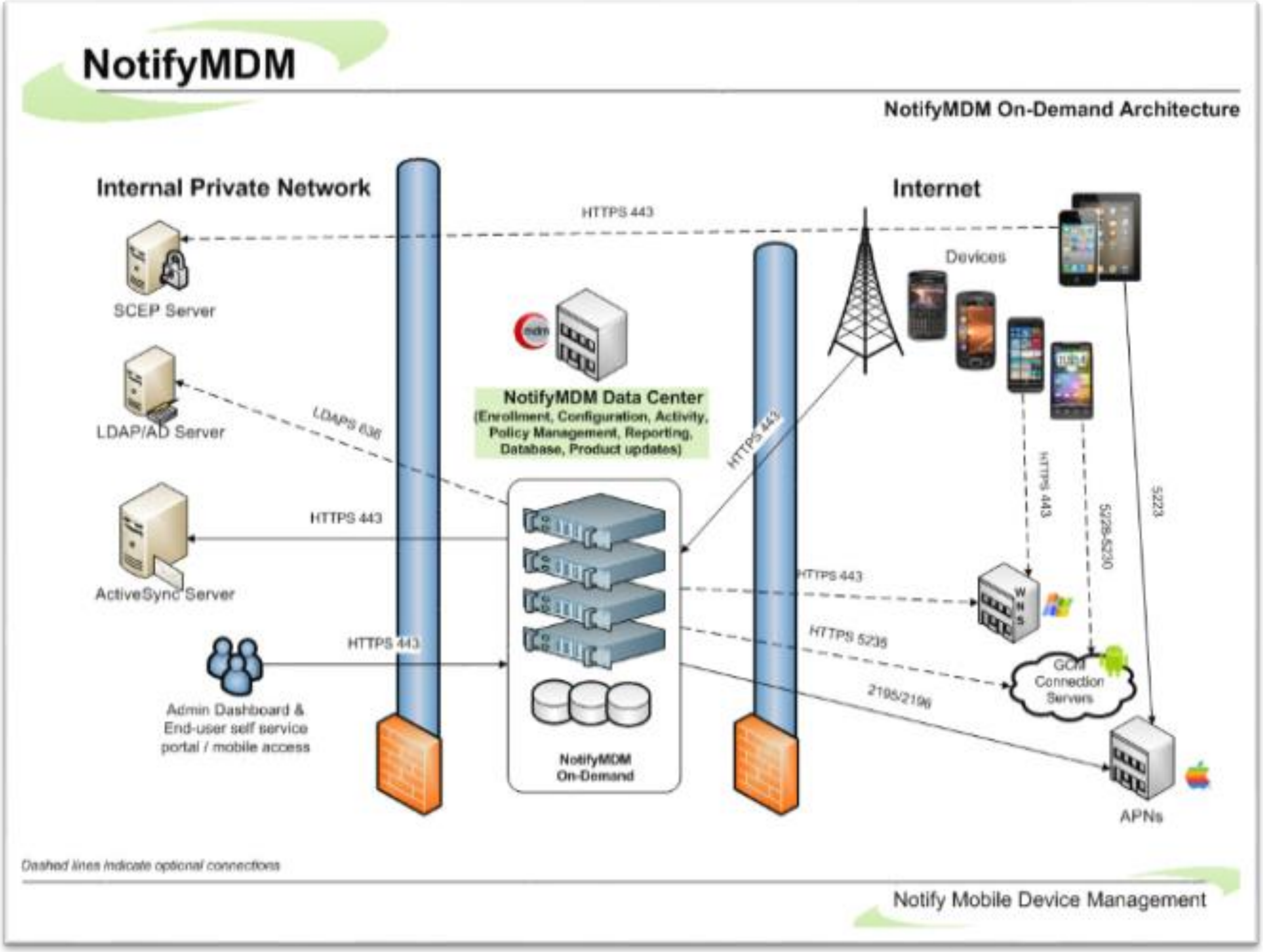
Data Center Access and System Maintenance Policies:

- Access restricted to key personnel, role based access control is used, root access is given and other privileges are only assigned on an as needed basis
- Login IDs are not shared; remote access is only conducted by key personnel and over a virtual private network
- Passwords are made up of complex patterns and are changed on a regular basis
- Automatic backups are performed several times a day and are not done by a third party
- Timely upgrades are performed to secure and provide optimum operations. Patches and updates are applied regularly to conform to current patch and release levels described by Notify Technology Corporation and by manufacturers of third party software used by Notify Technology Corporation. This generally occurs within two weeks from the time the patch is available.

Network Security

The network topology is illustrated in the following diagram. More complete information on system architecture is included in the beginning of this document under Architecture.

Data Center Architecture


NotifyMDM
NotifyMDM On-Demand Architecture
Internal Private Network
Internet
HTTPS 443
SCEP Server
Devices
NotifyMDM Data Center
(Enrollment, Configuration, Activity, Policy Management, Reporting, Database, Product updates)
LDAP/AD Server
LDAPS 636
HTTPS 443
HTTPS 443
ActiveSync Server
HTTPS 443
HTTPS 443
5228-5230
5223
HTTPS 443
W N S
HTTPS 5236
GCM Connection Servers
2195/2196
Admin Dashboard & End-user self service portal / mobile access
NotifyMDM On-Demand
APNs
Dashed lines indicate optional connections
Notify Mobile Device Management

The *NotifyMDM* system is protected by a firewall. The only port/protocol allowed incoming is 443 (HTTPS).Outgoing ports are specific to each groupware server type and are listed in the charts below. The *NotifyMDM* system uses TLS (where applicable) or SSL public key of 128 bytes.

Firewall Rules

Create firewall rules that block incoming traffic to your system over the TCP ports listed in the chart under the **Port Requirements for NotifyMDM Communication** section below. Include exceptions using the range of *NotifyMDM* IP addresses to allow traffic from the *NotifyMDM* Server.

Mobile devices must enroll against, and thus access your network through, the *NotifyMDM* On-Demand server.

Secure Encrypted Systems

Default TCP port numbers used for secure environments are listed in the chart below, as it is highly recommended that SSL certificates be installed on your server.

SSL certificates are used on all *NotifyMDM On-Demand* servers to facilitate secure data-in-motion between server and devices. Therefore, when users enroll devices they must always enable the SSL option.

Port Requirements for NotifyMDM Communication

Note: *Port numbers listed below are well-known default TCP port numbers, but are subject to change within your network.*

Firewall Rules/Policies Needed for NotifyMDM Components

Source	Destination	Port	Service
Web/HTTP	LDAP	636*	LDAPS
Web/HTTP	ActiveSync server	443**	HTTPS
	SMTP server	465***	SMTPS

* *Only required if using LDAP*

** *Only required if using corporate AS server*

*** *Only required if you choose to use your own SMTP server and not the SMTP server on NotifyMDM's hosted server*