NotifyMDM
Mobile Device Management

Preparing for NotifyMDM On-Demand Service

This guide provides information on . . .

. . . An overview of NotifyMDM

. . . Preparing your environment for NotifyMDM On-Demand

. . . Firewall rules and port requirements

. . . NotifyMDM Server Configuration

Table of Contents

NotifyMDM Overview

NotifyMDM is a mobile device management solution that provides organizations with centralized management and control of the wireless device platforms in their enterprise network.

The *NotifyMDM* solution includes a small application downloaded to devices and a server application running as either a hosted on-demand service or as an on-premise enterprise.

A single instance of the server application supports a multi-tenant architecture allowing an enterprise to manage one or multiple organizations.

The Role of the NotifyMDM Server

The *NotifyMDM* server is capable of managing devices in two capacities.

- **ActiveSync present** - When an ActiveSync server is part of the environment, the *NotifyMDM System serves as a gateway that proxies ActiveSync traffic*. Settings for the policies that govern devices in your environment are configured from *NotifyMDM*. For ActiveSync policies, the *NotifyMDM* policy setting will take precedence over those configured on the ActiveSync server. In addition, the *NotifyMDM* server relays all email and PIM data to and from the ActiveSync server. ActiveSync servers using protocol version 12.0 or greater should be configured to enable *Autodiscover* so that actual server address information can be discovered as users enroll.
- **ActiveSync not present** - For systems that do not use the ActiveSync protocol, *the NotifyMDM system serves as a stand-in ActiveSync server* in that it synchronizes ActiveSync policies and issues security command messages. In this scenario, email and PIM are not proxied through the *NotifyMDM* server.

The purpose of taking either of these roles is to control security policies available through ActiveSync and to allow the *NotifyMDM* server to issue remote security command messages.

NotifyMDM as a gateway server

Access. ActiveSync servers can be configured so that users are blocked from accessing the server without going through *NotifyMDM*. This forces even users with devices not running a *NotifyMDM* device application to enroll against the *NotifyMDM* server. This effectively allows you to manage all devices through *NotifyMDM*.

In addition, the *NotifyMDM* server can be configured to allow only devices that meet security and usage standards to access the corporate ActiveSync server. Server will allow ActiveSync traffic through as long as a device is currently using the policies defined for it. When policies are updated in the NotifyMDM web, devices are required to synchronize the updated security policies in order to continue accessing the corporate server.

Security. The *NotifyMDM* server intercepts security policy updates sent from the ActiveSync server to prevent them from being sent to the device. The policies defined in the *NotifyMDM* server are instead enforced on the device.

Remote wipe commands can be issued from either the *NotifyMDM* server or the ActiveSync server. Remote wipes are a crucial security feature, so if intent to wipe is expressed on the ActiveSync server, the *NotifyMDM* server will relay the wipe message to the device.

Authentication. For devices that have an ActiveSync server defined, the *NotifyMDM* server will use the ActiveSync server to authenticate the user's credentials.

Email and PIM. For devices that have an ActiveSync server defined, the *NotifyMDM* Server will relay ActiveSync Email and PIM traffic to and from the ActiveSync server.

NotifyMDM Device App Enrollment. Users associated with a defined ActiveSync server will install the *NotifyMDM* device app and enroll their devices with the *NotifyMDM* server using their ActiveSync account user credentials.

NotifyMDM as a stand-in ActiveSync server

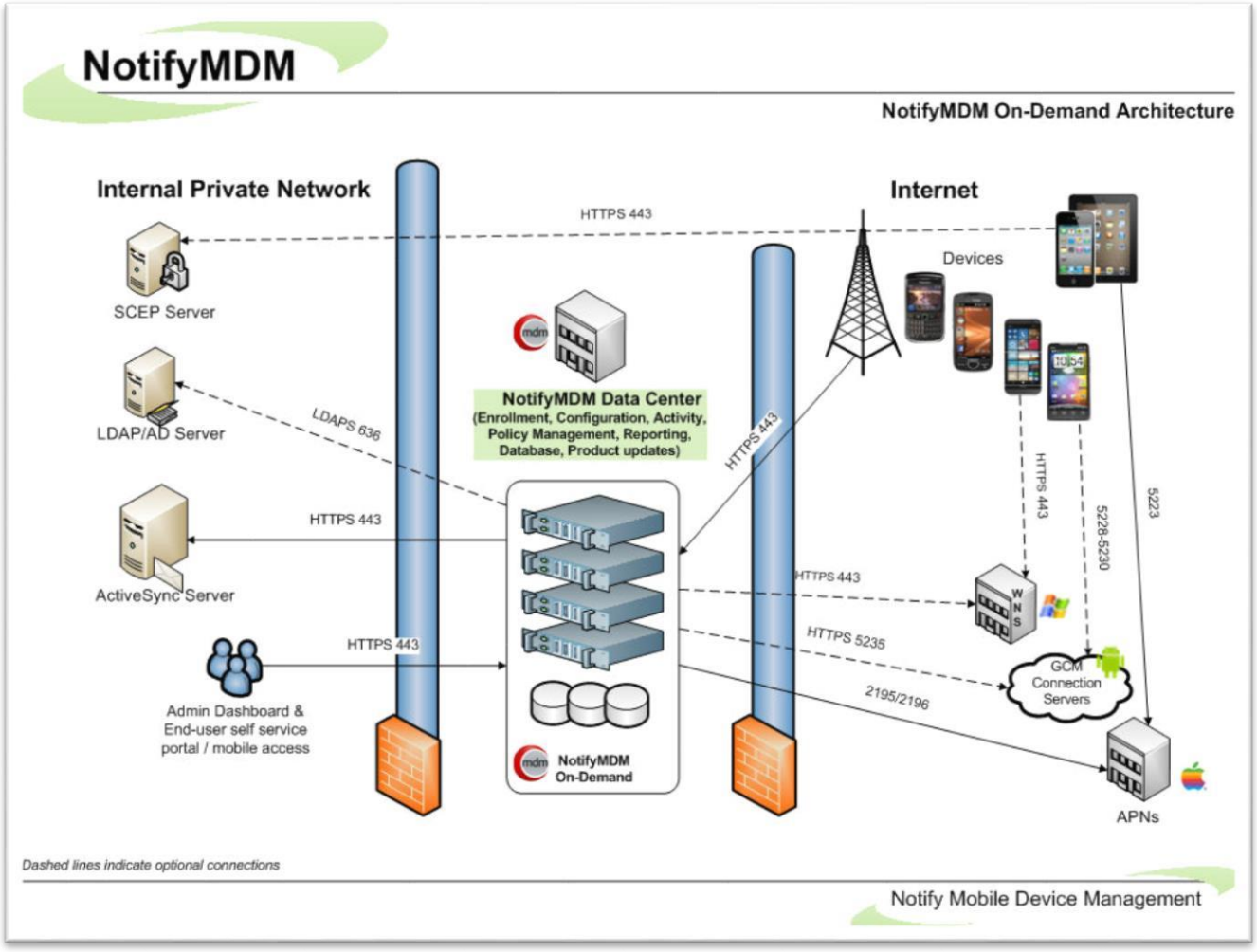
Security. *NotifyMDM* can provide ActiveSync security enforcement even when ActiveSync is not used for Email or PIM synchronization. When functioning in this role *NotifyMDM* will provide a minimum implementation of ActiveSync to send security policies and remote wipe messages, and to record device statistics when they are sent to the server.

The *NotifyMDM* server serves as a stand-in ActiveSync server only when a user is not associated with a defined ActiveSync server.

Authentication. Devices are authenticated directly against the *NotifyMDM* server using the password associated with the user account set up on the *NotifyMDM* server.

NotifyMDM Device App Enrollment. Users not interfacing with an ActiveSync server will install the *NotifyMDM* device app and enroll their devices with the *NotifyMDM* server using the credentials associated with the user account set up on the *NotifyMDM* server.

System Architecture



Preparing Your Environment

Integrating NotifyMDM: Firewall Rules, Port Requirements, SSL Encryption

During the initial setup of your *NotifyMDM* system, you will need to obtain the range of IP addresses utilized by the *NotifyMDM On-Demand* servers from Notify Technical Support. A Virtual Private Network (VPN) is available if *NotifyMDM On-Demand Premier* service is required. See your Notify Technology Enterprise Sales Manager for details. **Firewall Rules**

Create firewall rules that block incoming traffic to your system over the TCP ports listed in the chart 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

Source	Destination	Port	Service
NotifyMDM On-Demand Server	ActiveSync server	443	HTTPS
NotifyMDM On-Demand Server	LDAP server*	636	LDAPS
NotifyMDM On-Demand Server	SMTP server**	465	SMTPS

* Not required unless using this feature
** If you opt to use the SMTP server in your own environment

NotifyMDM Server Configuration

Once your *NotifyMDM* organization has been added to the on-demand server you will want to access the administrative dashboard and begin configuring the *NotifyMDM* environment.

1. Review the Configuration Guide: Organization, Policy Suites, Connection Schedules.
2. Verify the settings entered for your organization.
    - From the *NotifyMDM* dashboard choose: **System Management** > **Organization**
3. Obtain an Apple Push Notification Service (APNs) Certificate if the organization supports iOS devices. This certificate is required in order to support iOS devices.
    - Reference the guide, Obtaining an Apple Push Notification Service Certificate.
    - Upload the certificate to the server. From the *NotifyMDM* dashboard choose **System Management** > **Organization** > click the **Upload** button beside the **APNs Certificate** field
4. Configure Google EMM Administrator account. The integration provides a highly secure and efficient service for onboarding Android devices and managing existing Android user devices and apps via either a Work Profile or a Fully Managed Device.
    - From the NotifyMDM dashboard, select ***System Management*** > ***Organization*** to access the Google EMM settings
5. Customize the default Policy Suite and/or create additional Policy Suites.
    - From the *NotifyMDM* dashboard choose **Organization Management** > **Policy Suites**
6. Customize the default Device Connection Schedule and/or create additional Connection Schedules.
    - From the *NotifyMDM* dashboard choose **Organization Management** > **Device Connection Schedules**
7. Configure the Compliance Manager.
    - Reference the guide, Configuration Guide: Compliance Manager
    - From the *NotifyMDM* dashboard choose **Organization Management** > **Compliance Manager**
8. Define additional administrative logins (optional).
    - Reference the System Administration Guide: Organization Administrator Logins.
    - From the *NotifyMDM* dashboard choose **System Management** > **Organization Administrators** > **Add Administrator**
9. Deploy Smart Devices and Users
    - Reference the Configuration Guide: Adding Users, Enrolling Devices and the **Device App User Guides**.