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

. . . ActiveSync server best practices

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

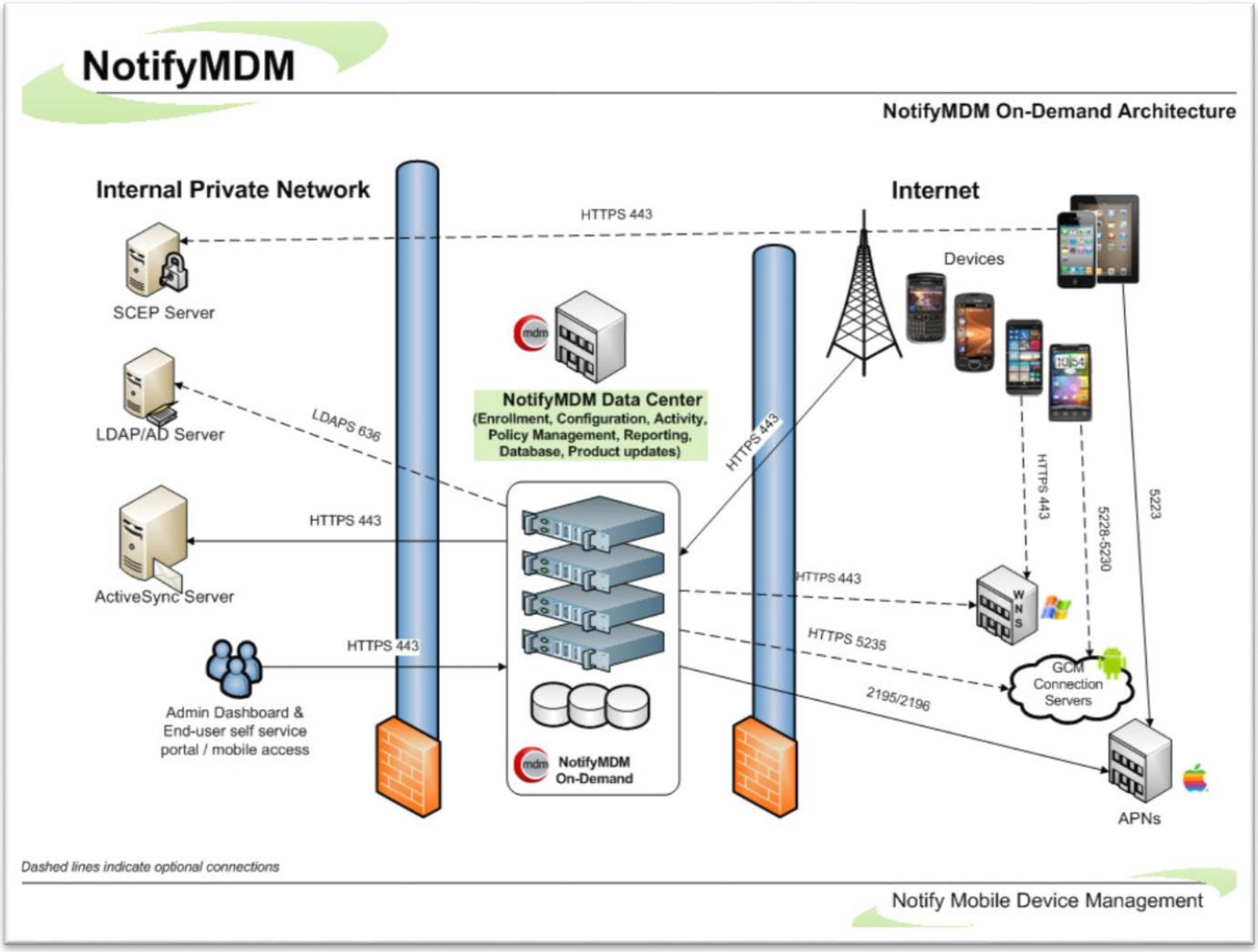
Security. *NotifyMDM* can provide ActiveSync security enforcement even when ActiveSync is not used for Email or PIM synchronization. When functioning in this role *NotifyMDM* will provide a minimum implementation of ActiveSync to send security policies and remote wipe messages, and to record device statistics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

Requirements for GroupWise DataSync and Other ActiveSync 2.5 Mail Servers

Configuring the Data Synchronizer with NotifyMDM Information

GroupWise Data Synchronizer users must configure the system with information about NotifyMDM.

1. Log into Synchronizer Web Admin.
2. Click the Mobility Connector, then scroll down to the *MDM Server* field.
3. Specify the IP address of the NotifyMDM server where you provided information about your Synchronizer server.
4. (Conditional) If you configured multiple NotifyMDM servers with information about your Synchronizer server, specify the IP addresses in a comma-delimited list.
5. Click *Save Custom Settings*.
6. Click *Home* on the menu bar to return to the main Synchronizer Web Admin page.
7. In the Actions column for Mobility Connector, click the stop icon to stop the Mobility Connector, then click the start icon to start the Mobility Connector.

The Mobility Connector now allows communication from the specified servers.

Accommodating iOS Device Users

Systems where iOS users are interfacing with a Novell GroupWise DataSync server must use DataSync Update 4 (Mobility 1.2.4) to fully utilize the hands-off enrollment functionality. Users need to enroll using their entire email address in lieu of their username if they are enrolling by the hands-off method. Similar processes must be followed to use hands-off enrollment when users interface with Exchange 2003 or any other mail server running ActiveSync 2.5 protocol. A user’s username and the string of characters to the left of the @ sign in their email address must be the same.

This is not a requirement for Mail/PIM servers running ActiveSync protocol 12.0, 12.1, 14.0, or 14.1.

If the ActiveSync server is linked to a fully configured LDAP server, however, users who exist on the LDAP server need not enroll using the full email address, as the LDAP server is queried for this information.

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. Customize the default Policy Suite and/or create additional Policy Suites.
    - From the *NotifyMDM* dashboard choose **Organization Management** > **Policy Suites**
5. Customize the default Device Connection Schedule and/or create additional Connection Schedules.
    - From the *NotifyMDM* dashboard choose **Organization Management** > **Device Connection Schedules**
6. Configure the Compliance Manager.
    - Reference the guide, Configuration Guide: Compliance Manager
    - From the *NotifyMDM* dashboard choose **Organization Management** > **Compliance Manager**
7. Define additional administrative logins (optional).
    - Reference the System Administration Guide: Organization Administrator Logins.
    - From the *NotifyMDM* dashboard choose **System Management** > **Organization Administrators** > **Add Administrator**
8. Deploy Smart Devices and Users
    - Reference the Configuration Guide: Adding Users, Enrolling Devices and the **Device App User Guides**.

ActiveSync Server Best Practices

Best practices regarding the ActiveSync server in the *NotifyMDM* environment include configuring ActiveSync so that users who are not enrolled through *NotifyMDM* are blocked from accessing the ActiveSync server. This forces even users with devices not running a *NotifyMDM* device application to enroll against the *NotifyMDM* server, thereby effectively allowing you to manage all devices through *NotifyMDM*.

Procedures for implementing best practices are outlined below for Exchange, GroupWise and FirstClass servers.

For those servers not listed below, administrators can create a firewall policy that blocks users from the ActiveSync server. This will also block users from web access. If you choose not to block access, you should closely monitor the traffic coming through the ActiveSync server.

You should implement this configuration after you have given users ample time to enroll through the *NotifyMDM* server. Users who have not enrolled through *NotifyMDM* by the set deadline will then be blocked from the ActiveSync server.

Exchange ActiveSync Servers

1. Launch the IIS Manager on your Microsoft Exchange Server.
    - **Windows Server 2003 (IIS 6.0)**: Click on START and navigate to Settings → Control Panel → Administrative Tools → Internet Information Services (IIS) Manager.
    - **Windows Server 2008 or 2012 (IIS 7.0/8.0)**: Navigate to Administrative Tools and select Internet Information Services (IIS) Manager.
2. Expand your website.
    - **Windows Server 2003 (IIS 6.0)**: Click the “+” symbol next to ***Default Website****.*
    - **Windows Server 2008 or 2102 (IIS 7.0/8.0)**: Click the “+” symbol next to ***Default Website****.*
3. Select the IIS Application for Microsoft Exchange ActiveSync.
    - **Windows Server 2003 (IIS 6.0)**: While navigating through the Default Website, select ***Microsoft-Server-ActiveSync*****.**
    - **Windows Server 2008 or 2012 (IIS 7.0/8.0)**: While navigating through the Default Website, select ***Microsoft-Server-ActiveSync*****.**
4. Open up the Security Properties for the IIS Application and navigate to the *IP Address and Domain Restrictions*.
    - **Windows Server 2003 (IIS 6.0)**: Right click on the application and select **Properties.** Select the ***Directory Security*** tab and click on the ***Edit*** button under ***IP Address and Domain Restrictions.***
    - **Windows Server 2008 or 2012 (IIS 7.0/8.0)**: With the Microsoft-Server-ActiveSync application selected, double click on ***IP Address and Domain Restrictions.***
5. Set a default rule to deny all traffic over the ActiveSync Protocol. Then add the exceptions or computer(s) that you will allow (*NotifyMDM* server) to communication with the *Microsoft-Server-ActiveSync* application.
    - **Windows Server 2003 (IIS 6.0)**:
        - Select the dot next to ***Denied Access*** to configure the application so that ***By Default, all computers will be denied access. Except the following…”***
        - Then, click on the ***Add*** button and enter the IP address range of the On-Demand *NotifyMDM* Servers. (Contact Notify Technical Support for this range of addresses.)
    - **Windows Server 2008 or 2012 (IIS 7.0/8.0)**:
        - Click on ***Edit Feature Settings*** and you will be prompted to configure the access for unspecified clients. Configure this setting to ***Deny*** the traffic and click ***OK***.

- Then, click on ***Add Allow Entry…*** At the prompt, enter the IP address range of the On-Demand *NotifyMDM* Servers. (Contact Notify Technical Support for this range of addresses.)

Novell GroupWise DataSync Servers

Systems Using SSL – Create a firewall policy that blocks incoming traffic to your Novell GroupWise DataSync Server over TCP Port 443. Include an exception to allow traffic from the *NotifyMDM* Server by entering the IP address range of the On-Demand *NotifyMDM* servers. (Contact Notify Technical Support for this range of addresses.)

Systems Not Using SSL – Create a firewall policy that blocks incoming traffic to your Novell GroupWise DataSync Server over TCP Port 80. Include an exception to allow traffic from the *NotifyMDM* Server by entering the IP address range of the On-Demand *NotifyMDM* servers. (Contact Notify Technical Support for this range of addresses.)

FirstClass Servers

Systems Using SSL

ActiveSync devices communicate with the server using port 443 for HTTPS Web Services. You will create a firewall policy to block all devices except those enrolled through *NotifyMDM*. However, so that you do not block PC Webmail users, you must first change the number of the TCP port that FirstClass uses for Webmail access over SSL. Assign it a unique, non-standard number so that PC Webmail users are not blocked when you create the firewall policy that blocks port 443.

1. Log into the FirstClass Administration Panel.
2. Double click the ***Internet Services*** icon to enter the Web Services configuration for this server.
3. Double click the ***Advanced Web & File*** icon to modify the port configuration for the FirstClass Web Services.
4. By default, FirstClass uses TCP port 443 for Webmail access over SSL. Change this port to a unique, non-standard number, for example, 8443.

Now, create a firewall policy that blocks incoming traffic to your FirstClass Server over TCP Port 443. Include an exception to allow traffic from the *NotifyMDM* Server by entering the IP address range of the On-Demand *NotifyMDM* servers. (Contact Notify Technical Support for this range of addresses.)

Systems Not Using SSL

ActiveSync devices communicate with the server using port 80 for HTTP Web Services. By default, FirstClass uses TCP port 8080 for Webmail access over HTTP. Since PC Webmail users use a different port number than devices, creating a firewall policy to block non-*NotifyMDM* devices will not affect PC Webmail users.
For systems not using SSL, the only step is to create a firewall policy that selectively blocks the port through which devices connect (80).

Create a firewall policy that blocks incoming traffic to your FirstClass Server over TCP port 80. Include an exception to allow traffic from the *NotifyMDM* Server by entering the IP address range of the On-Demand *NotifyMDM* servers. (Contact Notify Technical Support for this range of addresses.)