Pre-Installation Guide and Post-Installation Configuration Checklist

This guide provides information on . . .

. . . Preparing for the NotifyMDM installation

. . . NotifyMDM software installation: an overview

. . . ActiveSync Server Best Practices

. . . Configuring the newly installed NotifyMDM server: a post-installation checklist

. . . Provisioning user devices: a post-installation checklist

Table of Contents

Pre-Installation Tasks

Use the pre-installation checklist in Appendix A.

Server Preparation

1. Review the *NotifyMDM Installation Guide*.
2. Successful installation of the *NotifyMDM* system requires an **SMTP server**.
3. You must use **SSL** with the servers where the *NotifyMDM Web/HTTP* component is installed to meet best practices for security.

   The following secure certificates have been tested and confirmed to work with all supported *NotifyMDM* devices.

   - DigiCert Secure Server CA: "Secure Site" or "Secure Site Pro"
   - Thawte Server CA: "SSL Web Server Certificate"
4. **Software Prerequisites** for the *NotifyMDM* Installation are listed below. *NotifyMDM* consists of an SQL Database component and a Web/HTTP component. Install English versions **only**.

   - **On any server where a *NotifyMDM* component will be installed:**

     Install Windows Server 2019, Windows Server 2016, 2012 R2, or Windows Server 2012. Apply all *Windows Server* updates.

     The *NotifyMDM Server* is also supported on any of the above operating systems running as a virtual machine.

     Note: *NotifyMDM* must be installed on a system with a freshly installed operating system. If the system was previously used with *NotifyLink Enterprise Server*, for example, it is required that you reinstall the OS before you install *NotifyMDM*.

   - **Do not install the Web/Http Component on a server with existing PHP websites.**

     PHP is distributed with the *NotifyMDM* Web/Http Component and can cause issues with any existing installation of PHP.
   - **On the server(s) where the *NotifyMDM* Web/HTTP component will be installed:**

     Install Microsoft IIS versions 10, 8.5,or 8.0.
   - **On the server where *NotifyMDM* SQL Database will be installed:**

     Install Microsoft SQL Server 2019, Microsoft SQL Server 2017, Microsoft SQL Server 2016, Microsoft SQL Server 2014, or Microsoft SQL Server.

     Note: Microsoft SQL Express is supported for product evaluations but is not recommended for production.

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.

Port Requirements and Port Connection tests

Port requirements for *NotifyMDM* integration into your environment are listed in the chart below. It is good practice to perform connection tests before you begin the installation.

Port Requirements for NotifyMDM Installation

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
Devices	Web/HTTP	443	HTTPS
Web/HTTP	Licensing server (www.notify.net)	443	HTTPS
Web/HTTP	SQL DB	1433	ODBC-SQL
Web/HTTP	LDAP	389/636*	LDAP/LDAPS
	SMTP server	25/465	SMTP/SMTPS
Web/HTTP	ActiveSync server	443	HTTPS
Web/HTTP	Apple Data Center server	2195 and 2196	HTTPS
Web/HTTP	FCM Connection server	5235	HTTPS
** Not required unless you are using this feature*			

Telnet to Test the Port Connections

If you DO NOT get a 'Connect Failed' message for each test, the port is open. **Test an external connection to:**

- ***NotifyMDM* Web Server (port 443)** telnet <Web Server DNS> 443 **Test the connection from *NotifyMDM* Web Server to:**
- **Licensing Server (port 443)**

  From a Web browser, enter http://www.notify.net/test.htm. The page displays a "Test Complete" message.
- **LDAP Server (port 636)** telnet <LDAP Server IP> 636
- **SQL Server (port 1433)** telnet <Database Server IP> 1433
- **SMTP Server (port 465)** telnet <SMTP Server IP> 465
- **Apple Data Center (2195/2196)** telnet gateway.push.apple.com 2195

  telnet feedback.push.apple.com 2196
- **GCM Connection Server (port 5235)** telnet gcm.googleapis.com 5235

NotifyMDM Software Installation

Before the installation:

Gather the Internal and External IP addresses of your web server.
Create an external DNS entry for the *NotifyMDM* web server.

1. Review the Installation Guide. This guide details system architecture and the installation process.
2. **Install the NotifyMDM software components:** SQL Database Component and Web/Http Component
    - Open a web browser and enter http://notifymdm.notify.net/
    - Select *NotifyMDM* Server Installation.
    - Extract the contents of the zip file and run Launch.exe.
    - Begin the installation by selecting the SQL Database button. Reference the *Installation Guide*.
    - When the installation is completed, use the *NotifyMDM* Update Manager to check for and apply server software updates. Reference the *Update Management Guide***.**
3. **Establish quick access to the NotifyMDM Dashboard.**

    Add the address to your browser's favorites or create a shortcut on your desktop. **The address for the NotifyMDM Dashboard is:** *https://<your web server or domain name>/dashboard*

    Log in with the administrative username and password you defined during the Web/Http component installation.
4. Begin the process of configuring the server for your organization.
    - Configure the Organization: Use the post-installation checklist in Appendix B
    - Provision Users/Devices: Use the post-installation checklist in Appendix C

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, however, also blocks users from web access. Implement this configuration after you install the *NotifyMDM* system and 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. If you choose not to block access, you should closely monitor the traffic coming through the ActiveSync server.

Exchange ActiveSync Servers

1. Launch the IIS Manager on your Microsoft Exchange Server.
    - **Windows Server 2012 (IIS 8.0)**: Navigate to Administrative Tools and select Internet Information Services (IIS) Manager.
2. Expand your website.
    - **Windows Server 2012 (IIS 8.0)**: Click the + symbol next to ***Default Website****.*
3. Select the IIS Application for Microsoft Exchange ActiveSync.
    - **Windows Server 2012 (IIS 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 2012 (IIS 8.0)**: With the Microsoft-Server-ActiveSync application selected, double-click on ***IP Address and Domain Restrictions.***
    - Set a default rule to deny all traffic over the ActiveSync Protocol. Then add the exceptions or computers that you will allow (*NotifyMDM* server) to communicate with the *Microsoft-ServerActiveSync* application.
        - **Windows Server 2012 (IIS 8.0):**
            - Click ***Edit Feature Settings*** and configure the access for unspecified clients. Configure this setting to ***Deny*** the traffic and click ***OK***.
            - Then, click ***Add Allow Entry***. At the prompt, enter the IP address for the *NotifyMDM* Server. (*NotifyMDM On-Demand* users should contact Notify Technology Corporation Technical Support for the range of IP addresses that should be entered here.)

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 of the *NotifyMDM* Server. (*NotifyMDM On-Demand* users should contact Notify Technology Corporation Technical Support for the range of IP addresses that should be entered for the exception.)

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 of the *NotifyMDM* Server. (*NotifyMDM On-Demand* users should contact Notify Technology Corporation Technical Support for the range of IP addresses that should be entered for the exception.)

FirstClass Servers

Systems Using SSL

ActiveSync devices communicate with the server using port 443 for HTTPS Web Services. 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 such as 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 of the *NotifyMDM* Server. (*NotifyMDM On-Demand* users should contact Notify Technology Corporation Technical Support for the range of IP addresses that should be entered for the exception.)

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. When PC Webmail users use a different port number than devices, creating a firewall policy to block non-*NotifyMDM* devices does 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 of the *NotifyMDM* Server. (*NotifyMDM On-Demand* users should contact Notify Technology Corporation Technical Support for the range of IP addresses that should be entered for the exception.)

Appendix A: Pre-Installation Checklist

This checklist outlines the tasks, actions, and requirements to be completed before NotifyMDM On-Premise Server solution is installed locally. Each item should be verified, and the document completed and returned to Notify Technology Corporation at least 48 hours before the scheduled installation date. Please reschedule your installation if you have not completed the tasks prior to any scheduled call. For questions, contact your Notify Technology Corporation representative.

#	Complete	Pre-Installation Tasks	Reference
1	☐	SSL certificate acquired	Server Preparation
2	☐	Microsoft Windows Server software installed on any server where a *NotifyMDM* component will reside	Server Preparation
3	☐	Server where NotifyMDM Web/HTTP component will be installed has no existing PHP websites (PHP is distributed with NotifyMDM)	Server Preparation
4	☐	Microsoft IIS installed on server where NotifyMDM Web/HTTP component will reside	Server Preparation
5	☐	Microsoft SQL Server installed on server where NotifyMDM SQL Database will reside	Server Preparation
7	☐	Web Service URL is reachable	Port Requirements
8	☐	Web Service URL is reachable from Console Server	Port Requirements
9	☐	Licensing Server is reachable from NotifyMDM Web Server	Port Requirements
10	☐	SQL Server is reachable from NotifyMDM Web Server	Port Requirements
11	☐	SMTP Server is reachable from NotifyMDM Web Server	Port Requirements
12	☐	Apple APNs Server is reachable from NotifyMDM Web Server	Port Requirements
13	☐	FCM Connection Server is reachable from NotifyMDM Web Server	Port Requirements
14	☐	LDAP Server is reachable from NotifyMDM Web Server (optional)	Port Requirements

Appendix B: Configure NotifyMDM

When the *NotifyMDM* components have been installed on your server(s), access the administrative dashboard and begin configuring the *NotifyMDM* environment. Use the checklist on the next page. Use the checklist in Appendix C for tasks related to provisioning users and deploying devices.

Before you begin:

Have the *NotifyMDM* license provided by your Notify Technology Corporation Sales Representative ready. You will need when you use the Organization Setup Wizard.

A Note about Database Maintenance:

- **Database Cleanup.** Once you have installed NotifyMDM, verify that the database cleanup tasks have been enabled. When the *NotifyMDM* server software is installed, tasks are enabled, by default, with parameters for a system accommodating 1000 devices.

  Administrators of larger systems should adjust the task parameters according to the recommendations in the Database Maintenance Guide. To verify that the jobs are running, access the *Database Task Scheduler* from the dashboard and view the task grid. The grid displays which cleanup jobs are enabled, the last time each job was executed, and when each job will run again.

  If a database task has failed to run, you can check the *DatabaseTaskSchedulerLogs* database table for errors. Reference: System Administration Guide: Server Logging.

- **Back up.** Periodically backing up the database is an essential practice for system maintenance. A daily back up of the database, preferably streamed off site, is recommended at minimum.

  In addition, back up the MDM.ini file on the Web/Http server. This file is found under the *NotifyMDM* directory. Default directory: C:\Program Files\NotifyMDM Server.

  Regular back ups insure that data can be recovered if the database becomes compromised. With both a database back up and a back up of the MDM.ini file, a system can be fully restored if necessary.

#	Optional	Post Installation: Server Configuration Tasks	From the Dashboard	Reference
1	NO	Create an organization using the Organization Setup Wizard – defines default servers, a default device connection schedule, and a default policy suite.	**System Management** > **System Administration** > **Organizations** > **Add Organization**	Organization Configuration Guide
2	NO	Obtain an Apple Push Notification Service (APNs) Certificate for iOS devices.	----	Obtaining an APNs Certificate
3	NO	Upload the APNs certificate to the NotifyMDM server	**System Management** > **Organization** > click the **Upload** button next to the *APNs Certificate* field	Obtaining an APNs Certificate
4	NO	Enable FCM Toggle for Google Cloud Messaging	**System Management > Organization**	System Administration Guide
5	YES	Customize the default device connection schedule and/or create additional connection schedules.	**Organization Management** > **Policy Management** > **Device Connection Schedules**	Organization Configuration Guide
6	YES	Customize the default policy suite and/or create additional policy suites and policy schedules.	**Organization Management** > **Policy Management** > **Policy Suites**	Organization Configuration Guide
7	YES	Set up corporate resources for Android and iOS devices.	**Organization Management** > **iOS Corporate Resources** or **Android Corporate Resources**	User Management Guide
8	YES	Set up Managed App lists and categories	**Organization Management** > **Application Management** > **Managed Apps**	User Management Guide
9	YES	Designate blacklist or whitelist apps.	**Organization Management** > **Application Management** > **Whitelist/Blacklists**	User Management Guide
10	YES	Create a File Share list.	**Organization Management** > **Organization Control** > **File Share**	User Management Guide
11	YES	Configure the Compliance Manager.	**Organization Management** > **Compliance Manager**	Compliance Manager Guide
12	YES	Configure NotifyMDM for OpenID secure administrator sign-on.	**Organization Management** > **Administrative Servers** > **OpenID Provider**	System Administration Guide
13	YES	Configure NotifyMDM for SAML secure end-user sign-on.	**Organization Management** > **Administrative Servers** > **SAML Identity Provider**	Organization Configuration Guide
14	YES	Define administrative role permissions.	**System Management** > **Organization Administrative Roles** > **Role Permissions** OR **System Management** > **System Administrative Roles** > **Role Permissions**	System Administration Guide

15	YES	Create additional administrative logins.	**System Management** > **Organization Administrators** OR **System Management** > **System Administration** > **System Administrators**	System Administration Guide
16	YES	Adjust database cleanup job parameters for system accommodating more than 1000 devices.	**System Management** > **System Administration** > **Database Task Scheduler**	Database Maintenance Guide

Appendix C: Provision Smart Devices/Users

#	Optional	Post-Installation: User/Device Provisioning Tasks	From the Dashboard	Reference
1	YES	Enable Hands-off enrollment* to allow users to enroll without administrator involvement.	**Organization Management** > **Organization Control** > **ActiveSync Servers** or **Organization Management** > **Organization Control** > **LDAP Servers**	Organization Configuration Guide
2	YES	Create a user welcome letter and configure the system to send it automatically when each user enrolls.	**Organization Management** > **Policy Suites** > (select a policy suite) > **Welcome Letter** . . .then. . . **System Management** > **Organization,** check the *Send Welcome Letter* option	Configuration Guide: Adding Users
3	YES	Create Custom Columns to store additional user information.	**Organization Management** > **Organization Control** > **Custom Columns**	Configuration Guide: Adding Users
4	YES	Create local groups to categorize users (if not using LDAP to do so).	**Organization Management** > **Organization Control** > **Local Groups**	User Management Guide
5	YES	Assign Corporate Resources to LDAP groups/folders, or individual users.	**Organization Management.** From *Corporate Resources* click the **Assign to LDAP Groups/Folders** option	User Management Guide
6	YES	Assign Managed Apps to LDAP groups/folders, local groups, or individual users.	**Organization Management.** From *Corporate Resources* or *Managed Apps* click the **Assign to Groups/Folders** option	User Management Guide
7	YES	Categorize Managed Apps and assign to LDAP groups/folders, local groups, or users in bundles.	**Organization Management** > **Application Management** > **Manage Categories**	User Management Guide
8	YES	Add users to the server in batches (using .CSV file or LDAP server) or individually.	**Smart Devices and Users** > **Add User**	Configuration Guide: Adding Users
9	YES	Install Device App and enroll devices.	----	Device App User Guides
10	YES	Provision and distribute Apple DEP devices.	**Smart Devices and Users**, click the Apple DEP Devices button. Click **Manage Profile**.	User Management Guide
11	YES	Enable app-less enrollment for iOS devices. NotifyMDM app subsequently pushes to devices.	**System Management > Organization,** enable *Push NotifyMDM to iOS devices*	System Administration Guide

*Hands-Off enrollment can be configured two ways:

- Enable the *Hands-Off Enrollment* option when defining an ActiveSync server so that users with credentials on the ActiveSync server can self-enroll against the *NotifyMDM* server. When the user enrolls a device, an account is created and auto-provisioned using the organization default settings.
- Enable the *Hands-Off Enrollment* option when defining an LDAP server so that users with credentials on the LDAP server can self-enroll against the *NotifyMDM* server. You can allow hands-off enrollment for all users associated with the LDAP server or you can allow it only for selected LDAP folder/group members. When the user enrolls a device, an account is created and autoprovisioned using assignments associated with LDAP groups/folders to which users belong.

When an ActiveSync server and LDAP server are linked, configuring one server for hands-off enrollment will automatically configure the other server for hands-off enrollment.