

Pre-Installation

ZENworks® Mobile Management 2.8.x

September 2013

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2012-13 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Table of Contents

Pre-Installation Tasks	4
Server Preparation	4
Requirements for GroupWise DataSync and Other ActiveSync 2.5 Mail Servers.....	5
Port Requirements and Port Connection Tests.....	6
ZENworks Mobile Management Software Installation	7
Post-Installation Tasks	8
Configuring NotifyMDM	8
ActiveSync Server Best Practices.....	10
Exchange ActiveSync Servers	10
Novell GroupWise DataSync Servers	11
FirstClass Servers	11
Provisioning Smart Devices and Users.....	12

Pre-Installation Tasks

Server Preparation

1. Review the *ZENworks Mobile Management Installation Guide*
2. Successful installation of the *ZENworks Mobile Management* system requires an SMTP server.
3. You must use SSL with the servers where the *ZENworks Mobile Management 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 *ZENworks Mobile Management* devices.

- [VeriSign/RSA Secure Server CA](#): “Secure Site” or “Secure Site Pro”
 - [Thawte Server CA](#): “SSL Web Server Certificate”
4. Software Prerequisites for *ZENworks Mobile Management* Installation. Install English versions only.
 - **On any server where a *ZENworks Mobile Management* component will be installed:**

Install Windows Server 2012, Windows Server 2008 R2 SP1, Windows Server 2008 with SP2, Windows Server 2003 R2 x64, or Windows Server 2003.
Apply all *Windows Server* updates.
The *ZENworks Mobile Management* server is also supported on any of the above operating systems running as a virtual machine.
[Setup on Windows 2008 x64 or 2012](#)
[Setup instructions for Windows 2003 R2 x64](#)

Note: *ZENworks Mobile Management* must be installed on a system with a freshly installed operating system.
 - **On the server where *ZENworks Mobile Management SQL Database* will be installed:**

Install Microsoft SQL Server 2012, Microsoft SQL Server 2008 R2, Microsoft SQL Server 2008 R2 SP1, or Microsoft SQL Server 2008 SP1, Microsoft SQL Server 2008 SP3.

Note: Microsoft SQL Express 2008 is supported for product evaluations, but is not recommended for production.
 - PHP, Version 5.3.26, which is distributed with the *ZENworks Mobile Management Web/Http* Component, can cause issues with any existing installation of PHP. Therefore, you should not install the Web/Http Component on a server with other PHP websites.
 - **On the servers where *ZENworks Mobile Management Web/HTTP* Component will be installed:**

Install Microsoft IIS versions 7.5, 7.0, or 6.0.

Requirements for GroupWise DataSync and Other ActiveSync 2.5 Mail Servers

Configuring the Data Synchronizer with ZENworks Mobile Management Information

GroupWise Data Synchronizer users must configure the system with information about ZENworks Mobile Management.

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 ZENworks Mobile Management server where you provided information about your Synchronizer server.
4. (Conditional) If you configured multiple ZENworks Mobile Management 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.

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 *ZENworks Mobile Management* 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 ZENworks Mobile Management Installation

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 ZENworks Mobile Management Components

Source	Destination	Port	Service
Devices	Web/HTTP	443	HTTPS
Web/HTTP	www.zmmupdate.novell.com	443	HTTPS
Web/HTTP	SQL DB	1433	ODBC-SQL
Web/HTTP	LDAP	636*	LDAPS
	SMTP server	465	SMTPS
Web/HTTP	ActiveSync server	443	HTTPS
Web/HTTP	Apple Data Center server	2195 and 2196	HTTPS

* Not required unless you are using this feature

Telnet to Test the Port Connections

Note: If you DO NOT get a 'Connect Failed' message for each test, the port is open.

Test an external connection to ZENworks Mobile Management Web Server (port 443) :

telnet <Web Server DNS> 443.

Test the connection from ZENworks Mobile Management Web Server to:

- **Internet (port 443):**
From a Web browser, enter <http://zmmupdate.novell.com>
The test has succeeded if you are prompted for login credentials.
- **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

ZENworks Mobile Management Software Installation

Before the installation:

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

1. Review the [Installation Guide](#).
2. Install the SQL Database Component and Web/Http Component:
 - Open a web browser and enter <http://download.novell.com/>
 - In the **Product** or **Technology** list, select *ZENworks Mobile Management*, then click **Search**.
 - Click **ZENworks Mobile Management** and download the ZMM .zip file.
 - Extract the files and run **Launch.exe**.
 - Begin the installation by selecting the SQL Database button. Reference the *Installation Guide*.
 - When the installation is completed, use the *ZENworks Mobile Management Update Manager* to check for and apply server software updates. Reference the *Update Management Guide*.

3. Establish quick access to the ZENworks Mobile Management Dashboard.

Add the address to your browser's favorites or create a shortcut on your desktop.

The address for the ZENworks Mobile Management 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.

Post-Installation Tasks

Configuring NotifyMDM

When the *ZENworks Mobile Management* components have been installed on your servers, you can access the administrative dashboard and begin configuring the *ZENworks Mobile Management* environment.

1. Review the [Configuration Guide: Organization, Policy Suites, Connection Schedules](#).
2. **Create an organization** by using the *Organization Setup Wizard*.
 - This wizard steps you through defining default servers, the default policy suite, and the default device connection schedule.
 - From the *ZENworks Mobile Management* dashboard choose **System > System Administration > Organizations > Add Organization**.
3. **Obtain an Apple Push Notification Service (APNs) Certificate** if the organization supports iOS devices. The certificate is required in order to support iOS devices.
 - For instructions, refer to [Obtaining an Apple Push Notification Service Certificate](#).
 - Upload the certificate to the server from the *ZENworks Mobile Management* dashboard **System > Organization** > click the **Upload** button next to the **APNs Certificate** field.
4. **Customize the default Policy Suite and/or create additional Policy Suites**.
 - From the *ZENworks Mobile Management* dashboard choose **Organization > Policy Suites**.
5. **Customize the default Device Connection Schedule and/or create additional Connection Schedules**.
 - From the *ZENworks Mobile Management* dashboard choose **Organization > Device Connection Schedules**.
6. **Configure the Compliance Manager**.
 - For instructions, refer to the [Configuration Guide: Compliance Manager](#)
 - From the *ZENworks* dashboard choose **Organization > Compliance Manager**.
7. **Define additional administrative logins** (optional).
 - For instructions, refer to the [System Administration Guide: System Administrator Logins or Organization Administrator Logins](#).

8. Database Maintenance

- **Database Cleanup.** Verify that the database cleanup tasks have been enabled. When the *ZENworks Mobile Management* 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. See the [System Administration Guide](#): Server Logging.

- **Backup.** 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 *ZENworks* directory. Default directory: C:\Program Files\Novell\ZENworks\mobile.

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.

ActiveSync Server Best Practices

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

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 also blocks 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 installed the *ZENworks Mobile Management* system and given users ample time to enroll through the *ZENworks Mobile Management* server. Users who have not enrolled through *ZENworks Mobile Management* by the set deadline, will 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 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 2012 (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 the application and select **Properties**. Select the **Directory Security** tab and click 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 **IP Address and Domain Restrictions**.
5. Set a default rule to deny all traffic over the ActiveSync Protocol. Then add the exceptions or computers that you will allow (*ZENworks Mobile Management* server) to communicate 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 the **Add** button and enter the IP address of the *ZENworks Mobile Management Server*. (*ZENworks Mobile Management* users should contact Novell Technical Support for the range of IP addresses that should be entered here.)
- **Windows Server 2008 or 2012 (IIS 7.0/8.0):**
 - Click **Edit Feature Settings** to be prompted to configure the access for unspecified clients. Configure this setting to **Deny** the traffic and click **OK**.
 - Click **Add Allow Entry**. At the prompt, enter the IP address for the *ZENworks Mobile Management Server*. (*ZENworks Mobile Management* users should contact Novell 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 *ZENworks Mobile Management Server* by entering the IP address of the *ZENworks Mobile Management Server*. (*ZENworks Mobile Management* users should contact Novell 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 *ZENworks Mobile Management Server* by entering the IP address of the *ZENworks Mobile Management Server*. (*ZENworks Mobile Management* users should contact Novell 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. You need to create a firewall policy to block all devices except those enrolled through *ZENworks Mobile Management*. 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 *ZENworks Mobile Management Server* by entering the IP address of the *ZENworks Mobile Management Server*. (*ZENworks Mobile Management* users should contact Novell 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. Because PC Webmail users use a different port number than devices, creating a firewall policy to block non-*ZENworks Mobile Management* 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 *ZENworks Mobile Management* Server by entering the IP address of the *ZENworks Mobile Management* Server. (*ZENworks Mobile Management* users should contact Novell Technical Support for the range of IP addresses that should be entered for the exception.)

Provisioning Smart Devices and Users

Provisioning users for *ZENworks Mobile Management* can be accomplished in several ways. You can add users individually, deploy a fleet of devices using batch import methods, or you can configure the ActiveSync server for Hands-Off Enrollment.

1. Review the [Configuration Guide: Adding Users, Enrolling Devices](#) and the Device App User Guides.
2. **Enable Hands-Off Enrollment** (optional).

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 *ZENworks Mobile Management* 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 *ZENworks Mobile Management* 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 auto-provisioned 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.
 - See the [Organization Configuration Guide](#) for details.
3. **Create a Welcome Letter** to email to users when they enroll (optional).
 - From the *ZENworks Mobile Management* dashboard, select **Organization > Policy Suites**. Select a policy suite and create a letter.
 - Select **System > Organization** and check the *Send Welcome Letter to Users* option.
 4. **Define Corporate Resources** (server and network resources) with which to associate iOS device users.
 - From the *ZENworks Mobile Management* dashboard, choose **Organization**
 5. **Add device users to the *ZENworks Mobile Management* server.**

- Use a .CSV file or LDAP server for batch loading user or add each user manually.
- From the *ZENworks Mobile Management* dashboard, choose **Users > Add User**.

6. **Install device application software and enroll devices.**

Procedures vary slightly for each device type. Follow instructions in the corresponding device User Guides.