Server Installation

ZENworks® Mobile Management 3.2.x

October 2015

Novell®

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/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

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).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (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

ZENworks Mobile Management Overview

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

The *ZENworks Mobile Management* solution includes an application downloaded to devices, a server application, and an Update Manager application for applying server software updates.

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 ZENworks Mobile Management Server

The *ZENworks Mobile Management* server is capable of managing devices in two capacities.

- **ActiveSync Present** - When an ActiveSync server is part of the environment, the *ZENworks Mobile Management System* serves as a gateway that proxies ActiveSync traffic*. Settings for the policies that govern devices in your environment are configured from *ZENworks Mobile Management*. For ActiveSync policies, the *ZENworks Mobile Management* policy setting takes precedence over the settings configured on the ActiveSync server. In addition, the *ZENworks Mobile Management* 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 ZENworks Mobile Management system serves as a stand-in ActiveSync server* that synchronizes policies and issues security command messages. In this scenario, email and PIM are not proxied through the *ZENworks Mobile Management* server.

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

> * The *Add Organization Wizard* provides an option to disable the *ZENworks Mobile Management* server's function as a proxy for ActiveSync traffic. See Organization Management Guide: MDM Proxy

ZENworks Mobile Management as a Gateway Server

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

In addition, the *ZENworks Mobile Management* server can be configured to allow only devices that meet security and usage standards to access the corporate ActiveSync server. The server allows ActiveSync traffic through if a device is currently using the policies defined for it. When policies are updated in the *ZENworks Mobile Management* Web, devices are required to synchronize the updated security policies in order to continue accessing the corporate server.

Security. The *ZENworks Mobile Management* server intercepts security policy updates sent from the ActiveSync server to prevent them from being sent to the device. Instead, the policies defined in the *ZENworks Mobile Management* server are enforced on the device.

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

Authentication. For devices that have an ActiveSync server defined, the *ZENworks Mobile Management* server uses the ActiveSync server to authenticate the user's credentials.

Email and PIM. For devices that have an ActiveSync server defined, the *ZENworks Mobile Management* Server relays ActiveSync Email and PIM traffic to and from the ActiveSync server.

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

ZENworks Mobile Management as a Stand-in ActiveSync Server

Security. *ZENworks Mobile Management* can provide ActiveSync security enforcement even when ActiveSync is not used for Email or PIM synchronization. When functioning in this role, *ZENworks Mobile Management* provides 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 *ZENworks Mobile Management* 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 *ZENworks Mobile Management* server by using the password associated with the user account set up on the *ZENworks Mobile Management* server.

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

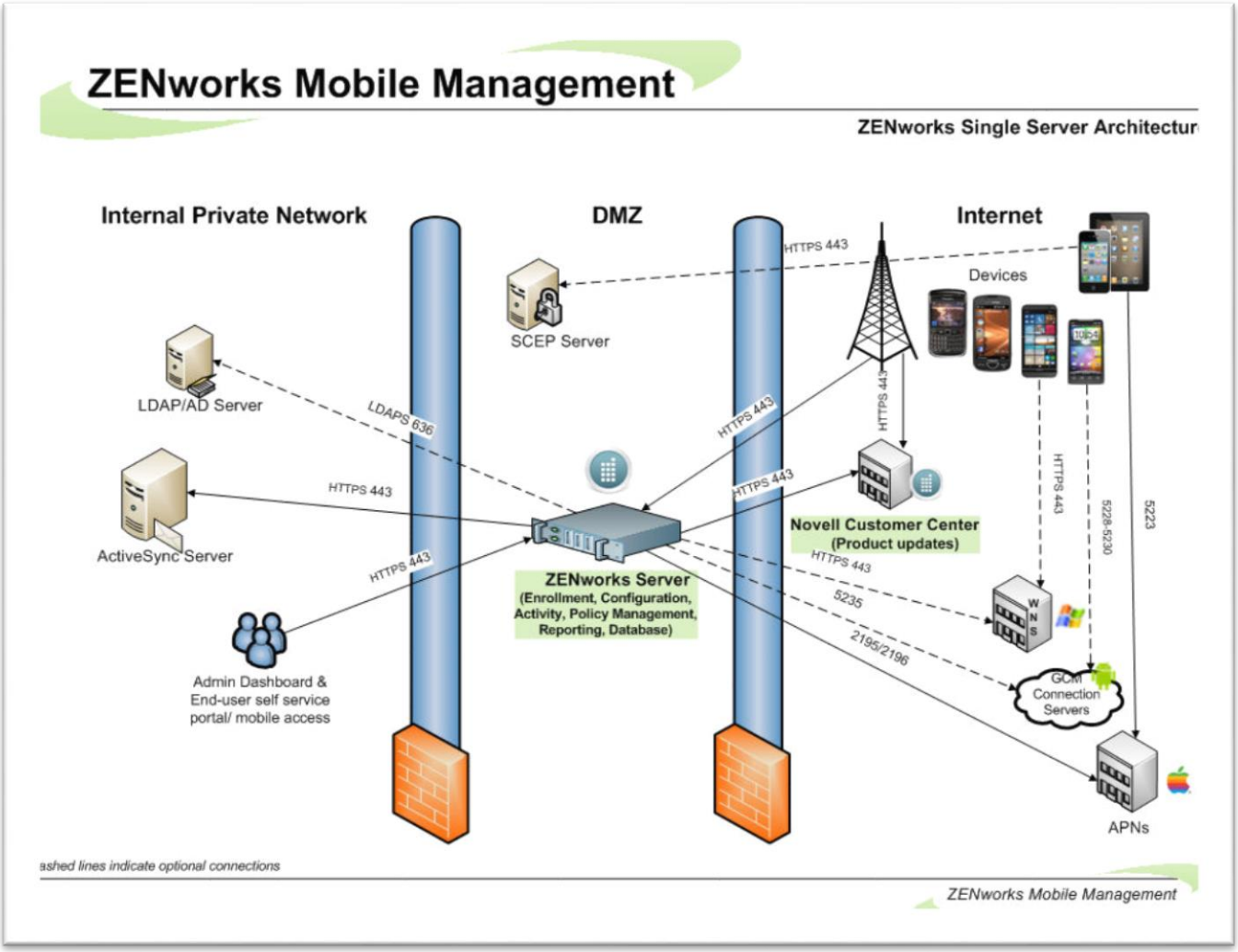
System Architecture

The *ZENworks Mobile Management System* consists of two components that can be installed on a single or multiple servers.

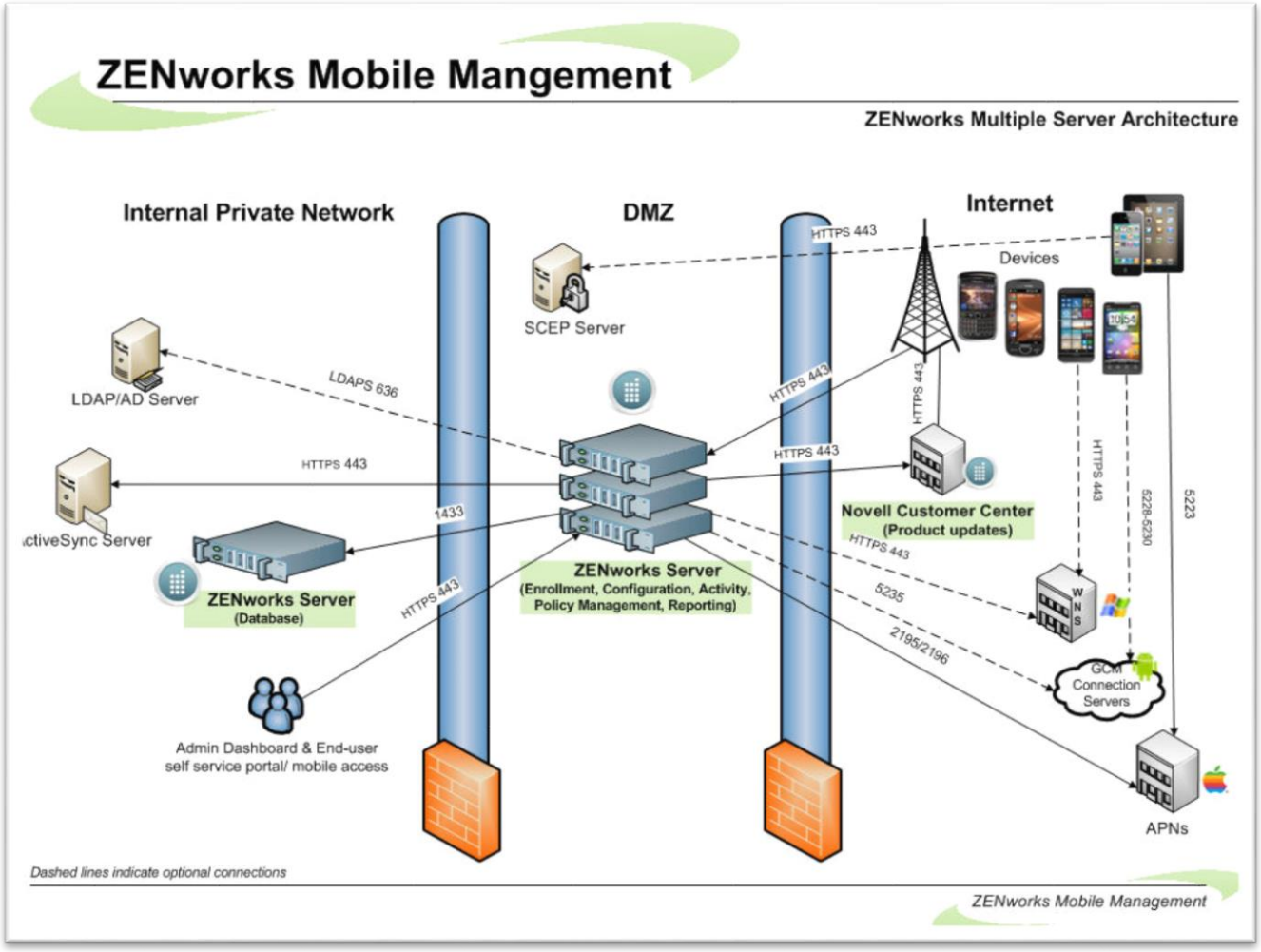
- SQL Database Component
- Web/Http Server Component

In addition to the setups illustrated, a reverse proxy setup is also supported as long as the proxy is sufficiently scalable. For the long term, redundant proxies might 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



Multiple Server Configuration Diagram



System Requirements

The *ZENworks Mobile Management System* consists of an *SQL Database Component* and a *Web/Http Server Component*.

General Requirements

- Successful installation of the *ZENworks Mobile Management* system requires an SMTP Server.
- The *ZENworks Mobile Management* server requires Secure Sockets Layer (SSL) encryption to meet best practices for security.

  Note: The *ZENworks Mobile Management* server must have a CA signed certificate. Self-signed certificates are not supported.

  Note: During a product evaluation period, it is acceptable to use internal CA issued certificates for user authentication. Send the trusted root certificate (in .cer format) to users in an email along with installation instructions.
- Install *ZENworks Mobile Management* on a system with a freshly installed operating system.
- If your organization will be supporting iOS devices, obtain an Apple Push Notification Service (APNs) Certificate. The certificate must be ready to upload to the server once *ZENworks Mobile Management* is installed and the organization is configured. See the document on obtaining a certificate.
- ZENworks Mobile Management currently supports Mail/PIM servers operating with ActiveSync protocol version 2.5, 12.0, 12.1, 14.0, or 14.1.

SQL Database Component Requirements

These are minimum system requirements. Actual requirements might vary depending on the nature of your environment.

Windows Server 2012 R2
Windows Server 2012
Windows Server 2008 R2 SP1
Windows Server 2008 with SP2
Windows Server 2003 R2 x64 or Windows Server 2003

See also:

Setup on Windows 2008 x64 or 2012

Setup instructions for Windows 2003 R2 x64

Use English versions. 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.

32-bit Intel Xeon processor or better

2 GB RAM (minimum)

3 GB free hard drive space

Microsoft SQL Server, 2014 (*Standard Edition*)
Microsoft SQL Server, 2012 (*Standard Edition*)
Microsoft SQL Server, 2008 R2 SP1 (*Standard Edition*)
Microsoft SQL Server, 2008 R2 (*Standard Edition*)
Microsoft SQL Server, 2008 SP3 (*Standard Edition*)
Microsoft SQL Server, 2008 SP1 (*Standard Edition*)
Microsoft SQL 2008 Web Edition or

Microsoft SQL Express, 2008 *(Supported for product evaluations; not recommended for production)*

Use English versions.

- Make sure that you select SQL server authentication when installing SQL.
- If you will be installing the Web/Http Component on the same server as the SQL Database Component, we recommend that you restrict the amount of system resources that Microsoft SQL Server uses. You can accomplish this by adjusting the *min server memory* and *max server memory* options in SQL Server 2008.
- If SQL Express 2008 is used, enter /SQLEXPRESS after the server address.

Web/Http Component Requirements

These are minimum system requirements. Actual requirements might vary depending on the nature of your environment.

Windows Server 2012 R2
Windows Server 2012
Windows Server 2008 R2 SP1
Windows Server 2008 with SP2
Windows Server 2003 R2 x64 or Windows Server 2003

See also: Setup on Windows 2008 x64 or 2012C:\Sourcesafe Notifycorp\HELP (help.notify.net)\TechDocs\ZENworks\Server\Install\zen_mobile_install_kb1.pdf
Setup instructions for Windows 2003 R2 x64zen_mobile_install_kb2.pdf

Use English versions. 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.
Recommended: **VMWare 3.0**, **VMWare vSphere 4.0/4.1**, or **Hyper-V** on Windows 2008/2012 servers

32-bit Intel Xeon processor or better

Microsoft SQL Server Native Client 10.0

Microsoft .NET Framework 3.5 SP1

- Automatically installed with Windows Server 2008
- Manual installation required for Windows Server 2003

2 GB RAM (minimum)

256 MB free hard drive space Additional space may be required for log files.

Microsoft IIS Supported Microsoft IIS versions: English versions 7.5, 7.0, or 6.0

PHP, Version 5.6.12 is distributed with the *ZENworks Mobile Management* Web/Http Component.

Note: This can cause issues with any existing installation of PHP. Therefore, it is recommended that you do NOT install the Web/Http Component on a server with other PHP Websites.

Port 80/443 (http/https) inbound and outbound must be open for device ← → server communications.
Port 1433 for communication with SQL Server.
itunes.apple.com outbound must be open to enable iOS managed app store search functionality

***ZENworks Mobile Management* dashboard requirements:**

- Internet Explorer or Firefox
- Adobe Flash Player 10.1.0
- Minimum screen resolution: 1024 x 768

An **SSL certificate** is required for the Web component
The following certificates have been tested and confirmed to work with all supported *ZENworks Mobile Management* devices:

- **Verisign/RSA Secure Server CA: "Secure Site" certificate**: http://www.verisign.com/ssl/
- **Thawte Server CA: "SSL Web Server Certificate"**: https://www.thawte.com/products/index.html

ZENworks Mobile Management Installation

The *ZENworks Mobile Management* server software is made up of the SQL Database Component and the Web/Http Server Component.

If you are planning on configuring a highly available *ZENworks Mobile Management* setup with Network Load Balancing or SQL Failover Clusters, please read the *ZENworks Mobile Management* High Availability Guide before you proceed with installation.

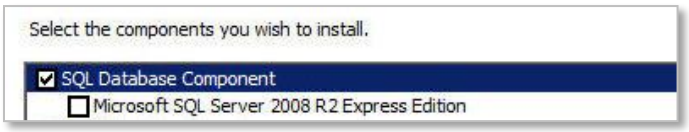
Upgrades: All software updates should be applied using the *ZENworks Mobile Management Update Manager*. The Update Manager applies all software patches and may even call up the installer when it is required for an upgrade. See the ZENworks Mobile Management Update Management Guide for details.

Download the ZENworks Mobile Management Server Software

1. Open a Web browser and enter http://download.novell.com
2. In the **Product** or **Technology** list, select *ZENworks Mobile Management*, then click **Search**.
3. Click **ZENworks Mobile Management**.
4. Download the **ZMM Server and Admin Software.zip** file.
5. Extract the files and run **Install.exe**.
6. Click **Next** at the welcome screen.

Step 1: Run the Installer

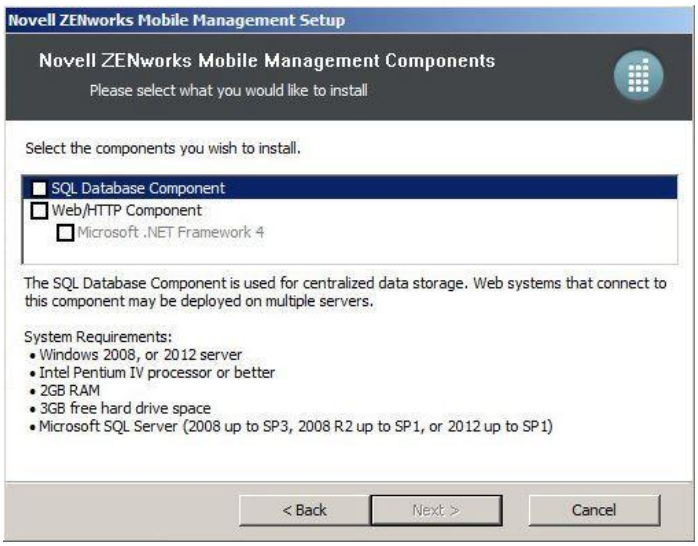
1. Select the components you wish to install at this time. Both the *SQL Database* and *Web/HTTP Component* are required for an initial installation.
    - Check the box beside **SQL Database Component** to install the *ZENworks Mobile Management* database component on an existing Microsoft SQL server
    - *(Conditional)* If you choose to use SQL Express Edition, you can check the box beside *Microsoft SQL Server 2008 R2 Express Edition*. This option will install the Express Edition and use it in place of the SQL Standard Edition. This is only recommended for product evaluations.

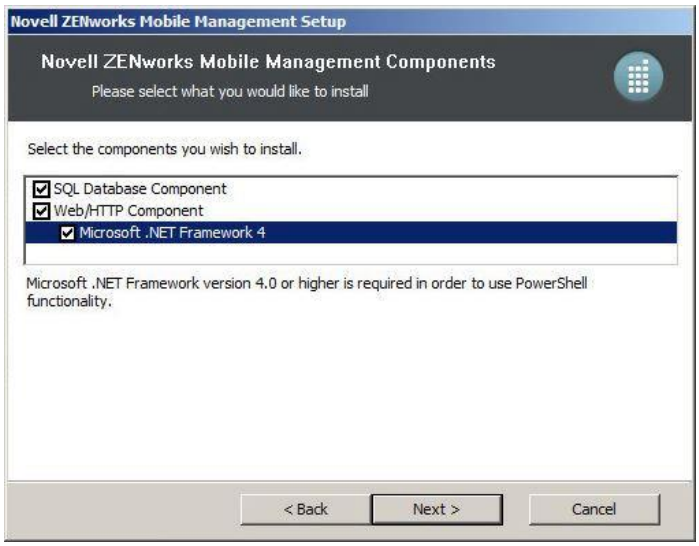


Installer with the SQL Express option

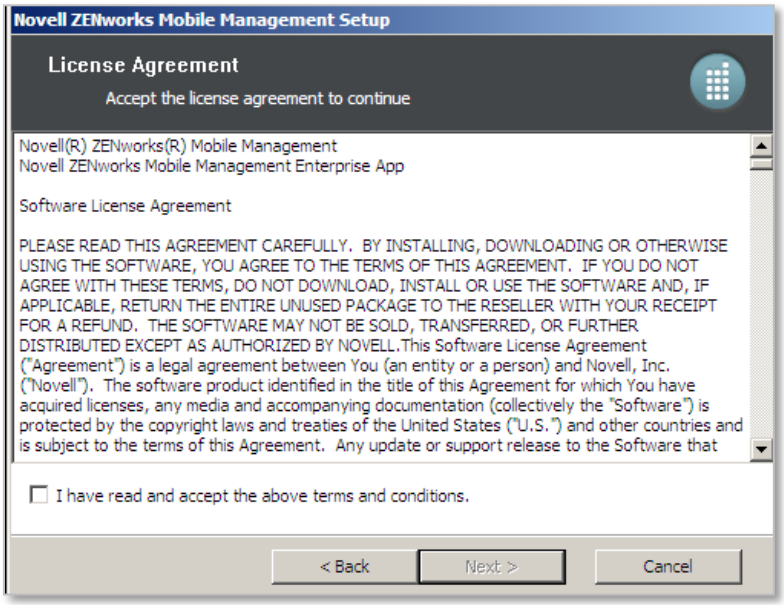
    - Check the box beside **Web/HTTP Component**.
    - *(Conditional)* If **Microsoft .NET Framework 4** is not already installed on the server, an option to install it will be included in the list of components. Check the box to install this software which is required for PowerShell functionality. When integrated ZENworks Mobile Management, PowerShell will give you the ability to auto-discover device and user information on an ActiveSync server and import it into the MDM server. See Organization Configuration and Management: *ActiveSync Server PowerShell Connection Settings*.

    Click **Next**.

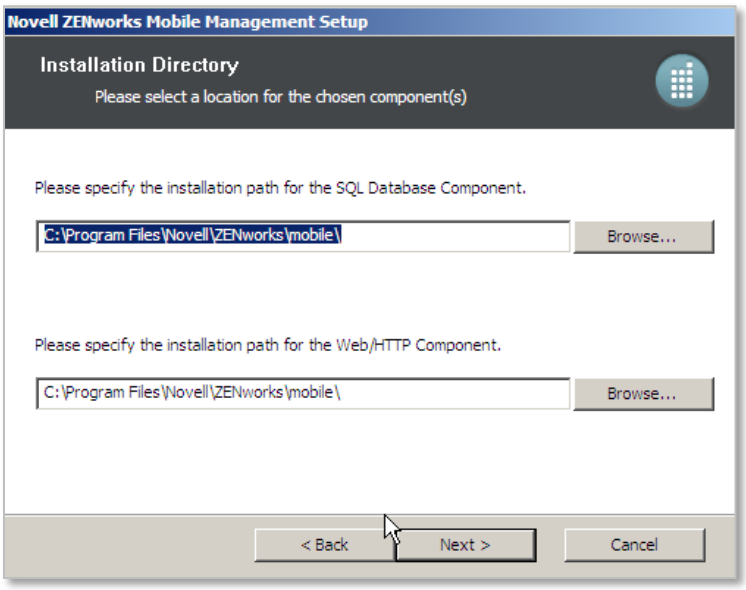




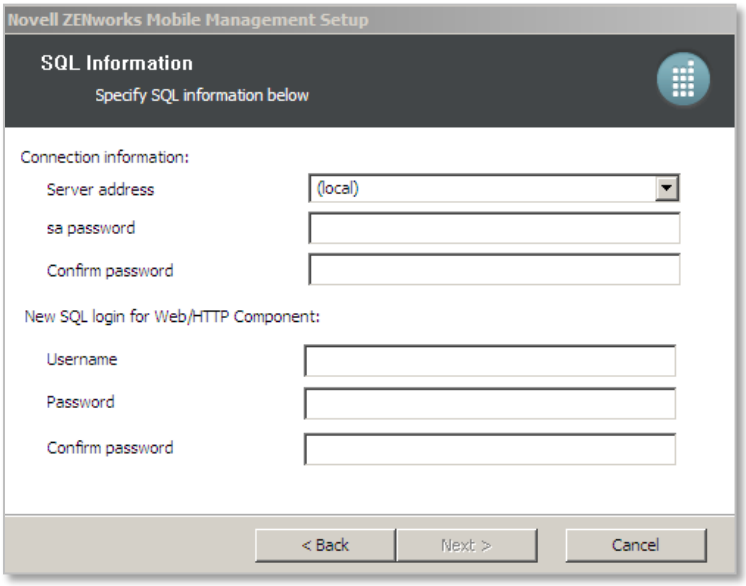
2. Read the **License Agreement** carefully and mark the acceptance checkbox. Click **Next.**



3. At the *Installation Directory* screen, browse to select the installation path for the SQL Database and Web/HTTP components. Click **Next**.

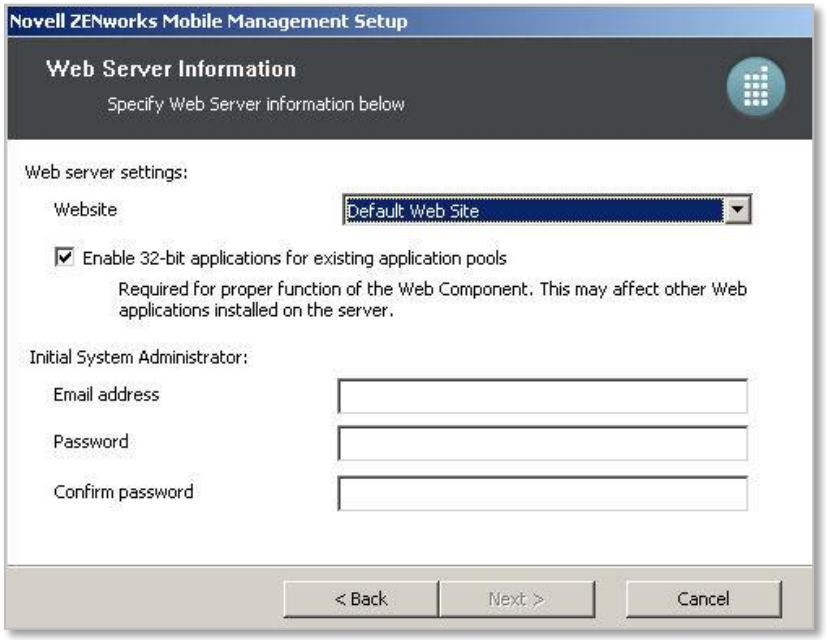


4. At the *SQL Information* screen, enter the following information for the SQL server.
   - **Server address** – Accept (local) or enter the address of a remote server where SQL resides.
   - **sa password** – Enter the password for an existing SQL server or create an sa password for the SQL Express installation. If creating one, a strong password is required. It must be at least six characters and contain three of these four criteria: uppercase letters, lowercase letters, numbers, and non-alphanumeric characters. An error displays if the password does not meet the criteria.
     (SQL Express is only appropriate for systems accommodating 1000 devices or less.)
   - **New SQL Login for Web/HTTP Component** – Create a **username** and **password** for SQL Server login. Confirm the password. This will be used by the *ZENworks Mobile Management* components to access the database. Click **Next** to continue.

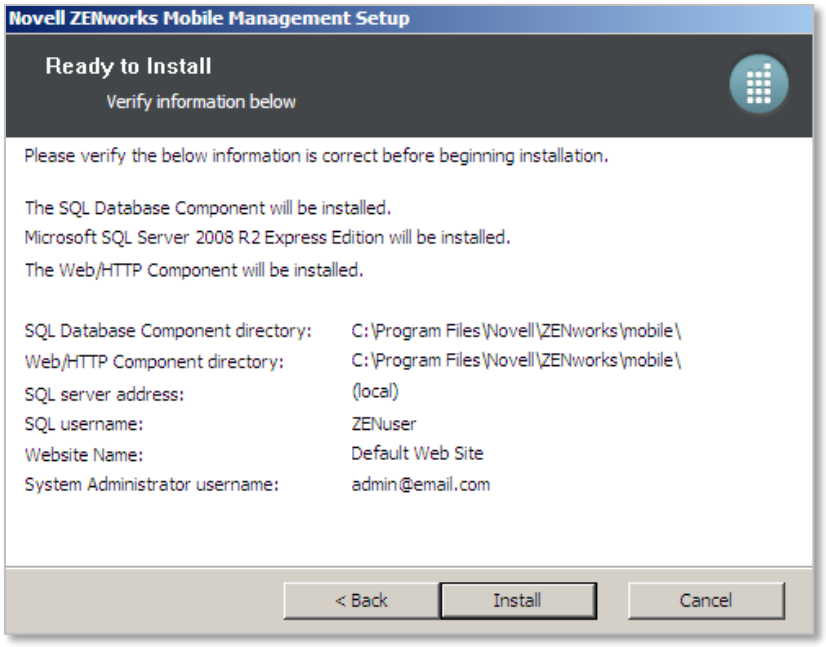


5. At the *Web Server Information* screen, enter the following:
   - Select the **Website** to which you are installing. By default, the Enterprise Server Web/Http Component will be installed to the *Default Web Site*. Install to a Web site that is not currently in use or create a new Web site with Microsoft IIS before installation (so that it appears in the drop-down list).
   - If you are installing on a 64-bit machine, mark the checkbox to **Enable 32-bit applications**. Verify that this will not affect other Web applications installed on the server. This option does not appear on 32-bit machines.
   - Enter the email address of the administrator designated as the **Initial System Administrator**. Create a password for the administrator and confirm it. A *ZENworks Mobile Management* administrator login with full admin privileges is created using this information. Use it for your initial *ZENworks Mobile Management* dashboard login.

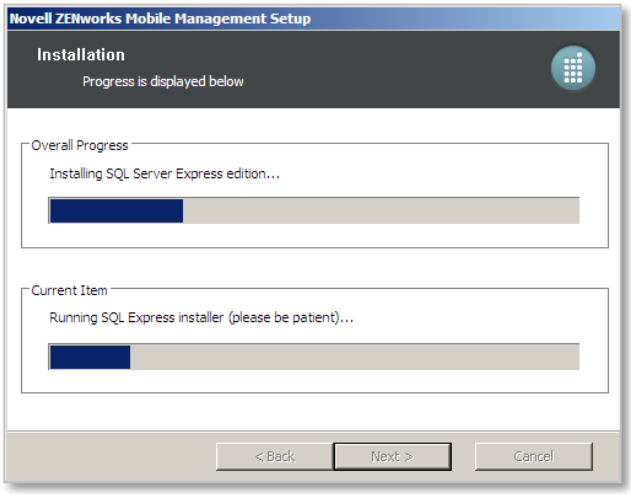
   Click **Next** to continue.

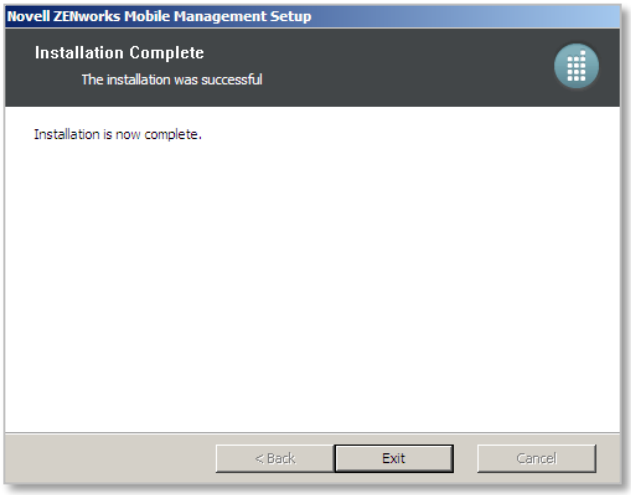


6. At the summary screen, verify that the information you have provided is accurate. Click **Back** to make corrections if necessary. Click **Install** to initiate the installation.



A progress bar and completion notification display as the installation continues and finishes.





The *ZENworks Mobile Management* installation is now complete.

Note: If you have installed on a machine using Microsoft Windows Server 2003, you must restart your system before proceeding.

Step 2: Apply Software Updates

Use the *ZENworks Mobile Management Update Manager* application to check for and apply available software updates.

The *Update Manager* is a Windows application that allows the administrator to apply *ZENworks Mobile Management* server software updates. You can also use the application to check for new updates and read change logs.

> **Note:** If you have configured your system with multiple Web servers for a Network Load Balanced setup, apply updates to all servers where the *ZENworks Mobile Management* Web/HTTP component resides.

For complete instructions on using the Update Manager, see the *ZENworks Mobile Management* Update Management Guide.

To check for available updates

1. Access the *ZENworks Mobile Management Update Manager* via the desktop shortcut on the *ZENworks Mobile Management* server.
2. Click **Check for Updates** to determine whether updates are available. Your initial use of the *Update Manager* requires that you enter the Customer Center login credentials provided by your Novell Sales Representative.
3. Click the **Download Available Updates** button to check the server for and download available updates. A progress meter displays as the updates download.
4. If you want to view descriptions of the updates, click the **View Change Log** button.
5. Select the latest update available (the default) to install.

See the Upgrade Recommendations Guide for version specific upgrade notes.

Post-Installation Tasks

When the *ZENworks Mobile Management* components have been installed on your server(s), 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 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.
    - For instructions, refer to Obtaining an Apple Push Notification Service Certificate.
    - Upload the certificate to the server from the *ZENworks Mobile Management* dashboard. Select **System** > **Organization** > click the **Upload** button beside the **APNs Certificate** field.
4. Customize the default Policy Suite 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 Configuration Guide: Compliance Manager
    - From the *ZENworks Mobile Management* dashboard, choose

      Organization > **Compliance Manager**
7. Define additional administrative logins (optional).
    - For instructions, refer to the System Administration Guide.
    - From the *ZENworks Mobile Management* dashboard, choose

      System > **Organization Administrators** > **Add Administrator**
8. Configure ActiveSync so that users who are not enrolled through *ZENworks Mobile Management* are blocked from accessing the ActiveSync server.
    - For instructions, refer to the Pre-Installation Guide.
9. Deploy Smart Devices and Users
    - For instructions, refer to Configuration Guide: Adding Users, Enrolling Devices and the device app user guides.

10. 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.

- **Back up.** Periodically backing up the database is an essential practice for system maintenance. A daily backup 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 backups 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.