Dell Wyse Device Manager
Version 5.0 — Installation Guide
Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.
## Contents

1 Introduction
   - What's New in the Installer ................................................................. 5
   - Installer Matrix .................................................................................. 6
   - Support Information ........................................................................... 7
   - Dell Wyse Technical Support ............................................................... 9
     - Related Documentation and Services .................................................. 9
     - Dell Wyse Online Community .............................................................. 9

2 Prerequisites ...................................................................................... 11
   - Pre-installation Checklist .................................................................... 11
   - Hardware Requirements ........................................................................ 12
     - Server Hardware Requirements for 32–bit OS .................................... 12
     - Server Hardware Requirements for 64–bit OS .................................. 12
   - Software Requirements ......................................................................... 12
     - Server Software Requirements ............................................................ 12
   - Communication Port Requirements ...................................................... 13
     - Communication Ports ......................................................................... 14
   - Requirements for Managing PCoIP Devices .......................................... 15
   - Checklist to Install WDM Enterprise Edition Only .................................. 16

3 Installing Dell Wyse Device Manager (WDM) ........................................ 17
   - Installing the WDM Workgroup Edition ................................................. 17
   - Installing the WDM Enterprise Edition .................................................. 19
   - Installing WDM in a Distributed Setup .................................................. 20
     - Installing the WDM Database .............................................................. 21
     - Installing Management Server/Other Services/Management Console .. 22
     - Installing the Software Repository ....................................................... 23
   - Upgrading WDM .................................................................................... 24
     - Configuring Secure Communications .................................................. 24

4 Uninstalling a Standalone Installation of WDM .................................... 29
   - Uninstalling WDM in a Distributed Setup ............................................. 29

5 Configuring High Availability Database Clustering for WDM .............. 31
   - Components Required for Database Clustering ..................................... 32
   - Pre-requisites for Database Clustering .................................................. 32
   - Configuring the Primary and Secondary VMs ....................................... 32
     - Validating a Configuration ................................................................ 33
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a Cluster on the Primary Node</td>
<td>33</td>
</tr>
<tr>
<td>Implementing a Node and File Share Majority Quorum</td>
<td>34</td>
</tr>
<tr>
<td>Installing .NET Framework on Primary and Secondary Nodes</td>
<td>35</td>
</tr>
<tr>
<td>Installing SQL Server on Primary and Secondary Nodes</td>
<td>35</td>
</tr>
<tr>
<td>Installing SQL Server Failover Cluster on Primary Node</td>
<td>36</td>
</tr>
<tr>
<td>Post Clustering Procedure</td>
<td>37</td>
</tr>
<tr>
<td>Running the HA Configuration Utility</td>
<td>38</td>
</tr>
<tr>
<td>Adding a License on WDM</td>
<td>39</td>
</tr>
<tr>
<td>Creating Load Balancing</td>
<td>41</td>
</tr>
<tr>
<td>Setting up the ARR Proxy Server</td>
<td>41</td>
</tr>
<tr>
<td>Installing Internet Information Services (IIS)</td>
<td>42</td>
</tr>
<tr>
<td>Installing the ARR Module</td>
<td>44</td>
</tr>
<tr>
<td>Configuring the Application Pool Process for ARR</td>
<td>44</td>
</tr>
<tr>
<td>Creating a Server Farm of WDM Management Servers</td>
<td>45</td>
</tr>
<tr>
<td>Configuring SSL</td>
<td>47</td>
</tr>
<tr>
<td>Configuring Server Farm Properties for ARR</td>
<td>48</td>
</tr>
<tr>
<td>Configuring Request Filtering</td>
<td>49</td>
</tr>
<tr>
<td>Setting up Proxy FQDN in WDM Preferences</td>
<td>50</td>
</tr>
<tr>
<td>Installing WDM Components</td>
<td>50</td>
</tr>
<tr>
<td>Configuring Load Balancing for ThreadX Devices</td>
<td>51</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>53</td>
</tr>
<tr>
<td>.NET Framework Installation Error in Windows 2012</td>
<td>53</td>
</tr>
<tr>
<td>Failure While Attaching the Database</td>
<td>53</td>
</tr>
<tr>
<td>Database Installation Failure After Manual Uninstallation of SQL Server Express 2008</td>
<td>54</td>
</tr>
<tr>
<td>Troubleshooting Load Balancing Issues</td>
<td>54</td>
</tr>
<tr>
<td>Health Test Feature in ARR Proxy (with SSL) Fails with Error Code 80072F8F</td>
<td>54</td>
</tr>
<tr>
<td>ARR Proxy Returns HTTP Error Code 502.3</td>
<td>55</td>
</tr>
<tr>
<td>ARR Proxy Returns HTTP Error Code 502.4</td>
<td>55</td>
</tr>
<tr>
<td>Enabling SSL Offloading on Proxy</td>
<td>55</td>
</tr>
</tbody>
</table>
Introduction

Dell Wyse Device Manager (WDM) is a software that manages all Dell Wyse thin and zero clients. WDM enables IT administrators to perform the following functions with ease:

- Software Imaging, updating, and configuring thin and zero client devices
- Asset tracking of devices
- Monitoring the health of devices
- Managing the policies and network settings on devices
- Remotely administering and shadowing the devices

WDM uses industry standard communication protocols and a component-based architecture to efficiently manage the devices on your network. This guide provides information on the prerequisites to install WDM, and the steps to install and configure WDM in your environment.

What’s New in the Installer

WDM now comes packaged in a new installer with enhanced features that include:

- New look and feel that is simple and user-friendly.
- Simplified installation flows for both the Workgroup and Enterprise versions of WDM.
- The License key is pre-populated for the 30 days Enterprise Evaluation and the Workgroup versions.
- Support for installing services such as DHCP Proxy, TFTP, and ThreadX.
- Windows authentication support for the WDM Database (RapportDB).
- Default installation of secure communication mode (HTTPS) for WDM.
- Support for CIFS and HTTPS protocols for the software repository during installation.
- Customized user option for Software Repository and WDM Database (RapportDB).
- Provision of detailed installation logs under the folder you have specified for WDM Installation. For example, C:\ProgramFiles\Wyse\WDM. The files are Detail_WDMInstall and Summary_WDMInstall.
- The Administrator installing WDM must provide passwords for the WDM database and software repositories. There are no default passwords. The WDM database password is also set for the SQL administrator ‘sa’, which must be used for uninstallation.
# Installer Matrix

The following matrix describes the various combinations of Microsoft SQL Server, and Microsoft Windows Server that the installer supports.

<table>
<thead>
<tr>
<th>RapportDB Authentication</th>
<th>SQL</th>
<th>Windows Server 2008 R2 SP1</th>
<th>Windows Server 2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Workgroup</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Distributed</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Windows 2008 R2 SP1 + SQL 2008 R2 Express</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Windows 2008 R2 SP1 + SQL Server 2008</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Windows 2008 R2 SP1 + SQL Server 2012</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Windows 2012 + SQL 2008 R2 Express</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Windows 2012 + SQL Server 2008 R2</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Windows 2012 + SQL Server 2008</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
</table>

| Windows 2012 + SQL Server 2012 | Yes | Yes | Yes | Yes | Yes | Yes |
## Support Information

This section lists out the supported operating systems, the supported databases, and the supported thin client devices for WDM version 5.0.

| Supported Operating Systems for WDM Server | • Windows 2008 R2 SP1 Enterprise Edition  
• Winodws 2008 SP2 32–bit  
• Windows 2012 Standard  
• Windows 2012 Standard R2  
• Windows 7 (32–bit)  
• Windows 7 (64–bit) |
|---|---|
| Supported Operating Systems for to Upgrade all WDM Components | • Windows 2003 R2 SP2 (only for upgrades from WDM 4.9.1)  
• Windows 2008 SP2 32–bit (only for upgrades from WDM 4.9.1)  
• Windows 2008 R2 SP1 Enterprise |
| Supported Operating Systems for WDM GUI | • Windows 2008 R2 SP1 Enterprise  
• Windows 2012 Standard  
• Windows 2012 Standard R2  
• Windows 7 32–bit SP1 Enterprise  
• Windows 7 64–bit SP1 Enterprise |
| Supported Databases | • Microsoft SQL Server 2005  
• Microsoft SQL Server 2008 R2 Express - English  
• Microsoft SQL Server 2008 R2 – English  
• Microsoft SQL Server 2008 Enterprise (32 bit)  
• Microsoft SQL Server 2012 |
| Supported Thin Client Devices | Wyse Enhanced Microsoft Windows XP Embedded build 587 or later:  
• C90LE  
• R90L  
• R90LE  
• V90LE  
Wyse Enhanced Microsoft Windows Embedded Standard 2009 (WES2009) build 641 or later:  
• C90LEW  
• D90DW  
• R90LW  
• R90LEW  
• V90LEW  
• X90CW |
- X90MW
- Z90DW
- Z90SW

**Wyse Enhanced Microsoft Windows Embedded Standard 7 (WES7) build 818 or later:**
- C90LE7
- D90D7
- D90Q7
- R90L7
- R90LE7
- X90C7
- X90M7
- Z90D7
- Z90DE7
- Z90S7
- Z90Q7

**Wyse Enhanced Microsoft Windows Embedded Standard 7p (WES7p) build 850 or later:**
- X90M7p
- Z90D7p
- Z90DE7p
- Z90S7p

**Wyse Enhanced Microsoft Windows Embedded 8 Standard (32-bit)(WE8S):**
- D90D8
- Z90D8
- Z90D8E
- D90D8X
- Z90D8X
- Z90D8EX

**Wyse Enhanced Microsoft Windows Embedded 8 Standard (64-bit) (WE8S):**
- D90D8
- D90Q8
- Z90D8
- Z90Q8

**Wyse Enhanced SUSE Linux Enterprise:**
- C50LE
- D50D
- R50L
Dell Wyse Technical Support

To access Dell Wyse technical resources, visit [http://www.wyse.com/support](http://www.wyse.com/support). If you still have questions, you can submit your questions using the Dell Wyse Self-Service Center at [http://support.wyse.com/selfservice.html](http://support.wyse.com/selfservice.html) or call Customer Support at 1-800-800-WYSE (toll free in U.S. and Canada). Hours of operation are from 6:00 A.M. to 5:00 P.M. Pacific Time, Monday through Friday.

To access international support, visit [http://www.wyse.com/global](http://www.wyse.com/global).

Related Documentation and Services

Fact Sheets containing features of hardware products are available on the Dell Wyse Web site. Go to [http://www.dell.com/wyse](http://www.dell.com/wyse) and select your hardware product to locate and download the Fact Sheet.

If you need to upgrade your Windows Embedded Standard operating system, contact Dell Wyse Customer Support at: [http://www.dell.com/wyse](http://www.dell.com/wyse).

Dell Wyse Online Community

Dell Wyse maintains an online community where users of our products can seek and exchange information on user forums. Visit the Dell Wyse Online Community forums at: [http://community.wyse.com/forum](http://community.wyse.com/forum).
Prerequisites

This section lists the prerequisites, the hardware, and software requirements that you must complete to prepare your environment to install and configure WDM. This section consists of:

- Pre-installation checklist
- Hardware requirements
- Software requirements
- Communication port requirements
- Upgrade requirements
- Requirements for managing PCoIP devices

Pre-installation Checklist

Before you begin installing WDM, ensure that you meet the following requirements:

- The server on which you install WDM should be dedicated to WDM services and should not be performing additional functions. For example, the server should not be functioning as a Domain Controller, Backup Controller, Mail Server, Production Web Server, DHCP Server, MSMQ Server, or Application Server.
- Install a supported operating system on the server on which you install WDM. For more information, see Software Requirements.
- Install Microsoft Internet Explorer version 6.0 or higher on all systems.
- Install the latest Java/JRE version for your operating system on the system on which you install the WDM Administrators Console.
- If you are running IIS 7.0 on Windows Server 2008 SP1, or IIS 7.5 on Windows Server 2008 R2 or Windows 7, update the HAgent on your devices to the latest WDM agents.
- Ensure that no other applications that require IIS are running on the system on which you are installing WDM.
- Ensure that all required communication ports are available and open for communication between servers, routers, and switches. For more information, see Communication Port Requirements.
- Ensure that you have access to your operating system CD-ROM and your Microsoft Windows system files during your installation. The WDM installer checks the system for all the software requirements. If any software is not installed, the installer prompts you to install the required software. Therefore, you must have access to your operating system CD-ROM or the network location to access the Microsoft Windows system files.
- Install Adobe Acrobat reader to read the End User License Agreement (EULA) and the Installation Guide.
Hardware Requirements

The system on which you install WDM should meet or exceed the minimum system requirements and depends on the operating system you install. The actual free space required depends on the number and size of the packages you register, and also on the number of devices you will be managing.

Server Hardware Requirements for 32–bit OS

<table>
<thead>
<tr>
<th>Category</th>
<th>Minimum Requirements</th>
<th>Recommended Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2.5 GHz Dual core Intel or AMD</td>
<td>Quad Core Intel or AMD</td>
</tr>
<tr>
<td>RAM</td>
<td>4 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td></td>
<td>In case of a Virtual Machine, it should be 2 GB initially allocated</td>
<td></td>
</tr>
<tr>
<td>Minimum Free Space</td>
<td>40 GB</td>
<td>40 GB</td>
</tr>
</tbody>
</table>

Server Hardware Requirements for 64–bit OS

<table>
<thead>
<tr>
<th>Category</th>
<th>Minimum Requirements</th>
<th>Recommended Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2.5 GHz Dual core Intel or AMD</td>
<td>Quad Core Intel or AMD</td>
</tr>
<tr>
<td>RAM</td>
<td>6 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>Minimum Free Space</td>
<td>40 GB</td>
<td>40 GB</td>
</tr>
</tbody>
</table>

Software Requirements

WDM 5.0 supports English versions of software. It is highly recommended that you install the latest version of each software package.

Server Software Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Software Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>WDM</td>
<td>You can choose any of the following operating systems:</td>
</tr>
<tr>
<td></td>
<td>• Windows 2003 R2 SP2 (only for upgrades from WDM 4.9.1)</td>
</tr>
<tr>
<td></td>
<td>• Windows 2008 SP2 32-bit (only for upgrades from WDM 4.9.1)</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 (64–bit)</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 SP1 (64–bit)</td>
</tr>
<tr>
<td></td>
<td>• Windows 2012 Enterprise</td>
</tr>
<tr>
<td></td>
<td>• Windows 2012 Enterprise R2</td>
</tr>
<tr>
<td>Component</td>
<td>Software Requirements</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WDM 5.0</td>
<td>Available in English version and supports installation on OS running English, French,</td>
</tr>
<tr>
<td></td>
<td>German, and Japanese language versions.</td>
</tr>
<tr>
<td>WDM GUI</td>
<td>• Windows 7 (32-bit)</td>
</tr>
<tr>
<td></td>
<td>• Windows 7 (64-bit)</td>
</tr>
<tr>
<td>Database Server</td>
<td>You can choose any of the following packages for the database server:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2005</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2005 Express</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2008</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2008 Express</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2008 R2 Express (32-bit)</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2012</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: SQL Server Express is recommended only when you are managing less than 2000</td>
</tr>
<tr>
<td></td>
<td>devices. When you are managing more than 2000 devices, you need to install SQL Server.</td>
</tr>
<tr>
<td>Online Help File</td>
<td>If you are unable to view the online help file on your browser correctly, then you need</td>
</tr>
<tr>
<td></td>
<td>to install the Active X Components and Java/JRE components.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: This issue may come up in browsers older than IE 9.0</td>
</tr>
</tbody>
</table>

**Communication Port Requirements**

WDM software components require certain communication ports to remain open on your servers, routers, and switches. For example, WDM relies on the HTTP/HTTPS communications ports for operations initiated by WDM and pushed to devices.

Push operations include:

- Issuing quick device commands such as Refresh Device Information, Reboot, Change Device or Network Information, Get Device Configuration, and so on.
- Distributing packages at a specific time.

Typically, port 80 is the default HTTP port and port 443 is the default HTTPS port. If either of these ports are closed, WDM cannot push updates or quick commands to devices.
### Communication Ports

<table>
<thead>
<tr>
<th>WDM Component</th>
<th>Protocol and Corresponding Ports</th>
<th>Port</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GUI</strong></td>
<td>HTTP</td>
<td>80</td>
<td>Communicate with the Web Service and Standard Service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>280</td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td></td>
<td>21</td>
<td>Register new packages into the Master Software Repository.</td>
</tr>
<tr>
<td>OLE DB</td>
<td>1433 (default)</td>
<td></td>
<td>Can be configured during installation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Communicate with the WDM database.</td>
</tr>
<tr>
<td>VNC</td>
<td></td>
<td>5800</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5900</td>
<td>Remote shadows devices.</td>
</tr>
<tr>
<td>Web Service</td>
<td>HTTP</td>
<td>80</td>
<td>Communicates with the Web Agent, GUI, and Standard Service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>280</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td></td>
<td>443</td>
<td>Secure Communication with the Web Agent, GUI, and Standard Service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8443</td>
<td></td>
</tr>
<tr>
<td>OLE DB</td>
<td>1433 (default) Can be configured during installation</td>
<td></td>
<td>Communicate with the WDM Database.</td>
</tr>
<tr>
<td>Web Agent</td>
<td>HTTP</td>
<td>80</td>
<td>Communication with the Web Service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>280</td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td></td>
<td>21</td>
<td>Read and write files to the master and remote software repositories.</td>
</tr>
<tr>
<td>DHCP Proxy and TFTP Services</td>
<td>OLE DB</td>
<td>1433 (default) Can be configured during installation</td>
<td>Communicate with the WDM database.</td>
</tr>
<tr>
<td></td>
<td>HTTP</td>
<td>8008</td>
<td>Communicate with the GUI and Web Service.</td>
</tr>
<tr>
<td>DHCP Proxy and TFTP Services and PXE</td>
<td>DHCP</td>
<td>67</td>
<td>Process UDP requests from PXE-enabled devices to the Standard Service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>68</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4011</td>
<td></td>
</tr>
<tr>
<td>WDM Component</td>
<td>Protocol and Corresponding Ports</td>
<td>Port</td>
<td>Function</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------</td>
<td>------</td>
<td>----------</td>
</tr>
<tr>
<td>TFTP</td>
<td>69</td>
<td></td>
<td>Download bootable image to enable management processing.</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td></td>
<td>Communicate with the Web Service regarding actions and status of current task.</td>
</tr>
<tr>
<td>FTP</td>
<td>21</td>
<td></td>
<td>Download and upload files to the master and remote software repositories.</td>
</tr>
<tr>
<td>DHCP Proxy and TFTP Services and legacy support for older WDM agents</td>
<td>UDP</td>
<td>44956</td>
<td>Discover devices using subnet directed broadcasts that have older WDM Agents (5.0.0.x and earlier) installed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>44957</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>44955</td>
<td></td>
<td>Discover devices using IP Range Walking. Upgrade devices that have an older WDM Agent (5.0.0.x and earlier) installed.</td>
</tr>
<tr>
<td>ThreadX Manager Service</td>
<td>TCP</td>
<td>9880</td>
<td>Communicate with ThreadX devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>50000</td>
<td></td>
</tr>
</tbody>
</table>

**Requirements for Managing PCoIP Devices**

PCoIP devices that run the ThreadX firmware require a DNS Service Location (SRV) resource record to perform the following actions:

- **Partial Check-In (heartbeat)** — The device performs a heartbeat check-in ever hour.
- **Firmware Download Completion Status** —

  The firmware upload is initiated by the server and the download completion is initiated by the device using the DNS SRV record.

- Configure FTP if you intend to use the firmware upgrade feature for PCoIP (ThreadX) devices. You must enable this in the Software Repository. For more information on enabling FTP in the Software Repository, see the *Dell Wyse Device Manager Administrator’s Guide*.
Checklist to Install WDM Enterprise Edition Only

If you are installing WDM Enterprise Edition only, then ensure the following:

- Obtain and have access to your WDM Enterprise Sales Key or Enterprise Evaluation Key that you use during installation.
- Install the supported version of SQL Server. The WDM installer provides Microsoft SQL Server 2008 R2 Express as the default option, but you can choose another supported version of SQL Server.
- Your FTP service should be running if you plan to use FTP. Configure FTP if you intend to use the firmware upgrade feature for Dell Wyse PCoIP (ThreadX) devices.

![NOTE:
If you plan to use PCoIP (Thread X), create and configure a DNS Service Location (SRV) resource record. For more information, see Configuring Load Balancer for ThreadX Devices.](image-url)
Installing Dell Wyse Device Manager (WDM)

This section guides you through the complete WDM installation procedures. WDM consists of the following components:

- Database
- Management Server
- Software Repository
- Other Services
- Management Console

You can install all the components on the same system or you can have a distributed setup where each component is installed on different systems.

You can install WDM in two flavours:

- **Enterprise Edition** —
  This edition needs a specific license key and comes packaged with all the features of WDM. You can manage a very large number of thin client devices using this edition. You can install this edition in a distributed environment and can install every component on different systems.

- **Workgroup Edition** —
  This edition consists of a free license key and certain features of WDM are disabled. You can manage up to 10,000 thin client devices using this edition. You must install all the components in the same system and you cannot have a distributed setup with this edition.

**NOTE:** You cannot install WDM on servers running other services such as the DNS, or DHCP, AD Domain Services or other services that conflict with the WDM functionality and resources.

**NOTE:** To run the WDM Installer (Setup.exe), you must log in to the system as an Administrator.

**NOTE:** When you are installing the WDM database in a standalone or a distributed setup, and want to use an existing SQL database, make sure that it is a full version of SQL Server and not SQL Server Express.

Installing the WDM Workgroup Edition

Before you begin the Installer make sure that you have met all the prerequisites. For more information, see Prerequisites.
To install the Workgroup edition:

1. Extract the contents of the WDM installer on the system where you want to install WDM.
2. Navigate to the folder where you have extracted the installer and run Setup.exe.
   The Welcome screen is displayed.
3. Click Next.
4. Select Workgroup as the License Type and click Next.
   For Workgroup edition, the license key is provided within the Installer and you do not need to enter any details.
5. The components are all selected by default and you cannot de-select any component. Click Next.
6. In the Configure Database screen, you can choose one of the following options:
   - **Install New Database Server (Microsoft SQL Express 2008 R2)** — Select this option if you do not have any supported version of Microsoft SQL Server installed on the system. Proceed to step 7.
   - **Use Existing Database Server (SQL Server Express or full)** — Select this option if you have already installed a supported version of Microsoft SQL Server on the system. Proceed to step 8. If you select this option, make sure that the existing database server is on the same system where you are installing WDM Workgroup edition.

   For more information on supported SQL Server versions, see [Software Requirements](#).
7. Provide the RapportDB database credentials. RapportDB is the WDM database instance that is created on SQL Server.
   a. SQL Server Authentication is selected by default. Select Windows Authentication if you want to connect to the Rapport Database using your Windows login credentials.
   b. **Username** — The default username is rapport. You can retain the default or change the username.
   c. **Password** — Enter the password to connect to the database.
   d. **Confirm Password** — If you are creating a new user, enter the password again.
8. If you have selected the second option in step 6, then provide the following details:
   a. **Server** — Provide the IP address of the server.
   b. **Port** — This is entered by default and the port number is 1433
   c. **Username** — Enter the user name to connect to the existing database.
   d. **Password** — Enter the password to access the database.
9. Click Next. The Configure Software Repository Server screen is displayed.
10. Enter the authentication details for the Software Repository:
    a. **Configure New Repository Server** — select this option if you want the installer to configure the repository server. You can create a new user or use an existing user.
    b. **Use Existing Repository Server** — select this option if you have already configured the Repository Server.
    c. **Enter Protocols** — Select the protocol and settings to distribute software to the managed devices. HTTPS is selected by default. You can also select FTP and CIFS.
    d. **Authentication Type** — Windows is selected by default. You can also select Basic.
    e. **Username** — Rapport is displayed by default. You can change this. If you select the Use existing Repository user option, enter the user name of the existing user.
    f. **Password** — Enter the password to access the repository.
    g. **Confirm Password** — If you are creating a new user, enter the password again.
11. Click Next to install the other services.
12. **DHCP Proxy** is selected by default. Select the other services if required. Click Next.
13. Provide the installation path and click Next. The summary screen is displayed.
14. Click Next to begin the installation.
The installation progress is displayed on the screen and after installation is complete, you are prompted to restart your system.
Restart the system for the system changes to take effect.

Installing the WDM Enterprise Edition

The WDM Enterprise Edition has all the features of WDM and you can install all the components on a single system or on different systems.
Make sure you have met all the pre-requisites. For more information, see Prerequisites.
To install the Enterprise Edition:

1. Extract the contents of the WDM installer on the system where you want to install WDM.
2. Navigate to the folder where you have extracted the installer and run Setup.exe.
The Welcome screen is displayed.
3. Click Next.
4. Select Enterprise as the License Type.
   a. If you have the WDM License key, select the I have WDM Enterprise License Key option and enter the license key in the space provided.
   b. If you do not have the License key, select the 30–days Enterprise Evaluation option.
      The license key is entered by default. However, after the 30 days evaluation period, you need to obtain the license key and add it to WDM. For more information on adding the license key, see the Dell Wyse Device Manager Administrator’s Guide.
5. Click Next.
6. Select the components you want to install and click Next.
   You can install all the components on the same system or each component on a different system.
   
   NOTE: If you are installing the components separately on different systems, make sure you install the Database first. If you do not install the database, you cannot install the remaining components.
7. In the Configure Database screen, you can choose one of the following options:
   - Install New Database Server (Microsoft SQL Express 2008 R2) — Select this option if you do not have any supported version of Microsoft SQL Server installed on the system. Proceed to step 8.
   - Use Existing Database Server (SQL Server Express or full) — Select this option if you have already installed a supported version of Microsoft SQL Server on the system. Proceed to step 9.
     For more information on supported SQL version, see Software Requirements.
8. Provide the RapportDB database credentials. RapportDB is the WDM database instance that is created on SQL Server.
   a. SQL Server Authentication is selected by default. Select Windows Authentication if you want to connect to the WDM database (RapportDB) using your Windows login credentials.
      
      NOTE: Even if you choose Windows Authentication, the WDM installation always requires the SQL Authentication to access the SQL database. In a standalone installation, after you complete the WDM database installation, the WDM Installer takes care of assigning the Active Directory user to the database and the same user is used for installing the WDM services.
   b. Username — The default username is rapport. You can retain the default or change the user name.
   c. Password — Enter the password to connect to the database.
   d. Confirm Password — If you are creating a new user, enter the password again.
9. If you have selected the second option in step 7, then provide the following details:
   a. **Server** — Provide the IP address of the system on which you have installed Microsoft SQL Server.
   b. **Port** — This is entered by default and the port number is 1433
   c. **Username** — Enter the user name to connect to the existing database.
   d. **Password** — Enter the password to access the database.

10. Click Next. The **Configure Software Repository Server** screen is displayed.

11. Enter the authentication details for the Software Repository:
   a. **Configure New Repository Server** — select this option if you want the installer to configure the repository server. You can create a new user or use an existing user.
   b. **Use Existing Repository Server** — select this option if you have already configured the Repository Server.
   c. **Enter Protocols** — Select the protocol and settings to distribute software to the managed devices. HTTPS is selected by default. You can also select FTP and CIFS.
   d. **Authentication Type** — Windows is selected by default. You can also select Basic.
   e. **Username** — Rapport is displayed by default. You can change this. If you select the Use Existing Repository User option, enter the user name of the existing user.
   f. **Password** — Enter the password to access the repository.
   g. **Confirm Password** — If you are creating a new user, enter the password again.

12. Click Next to install the other services.

13. **DHCP Proxy** is selected by default. Select the other services if required. Click Next.

14. Provide the installation path and click Next. The summary screen is displayed.

15. Click Next to begin the installation.

The installation progress is displayed on the screen and after installation is complete, you are prompted to restart your system.

Restart the system to take effect.

### Installing WDM in a Distributed Setup

You can split the WDM components and install them on different systems. This setup is called a distributed setup of WDM. Ideally you can split the components as follows:

- **WDM Database**
- **WDM Management Server, WDM Management Console, and Other Services**
- **WDM Software Repository**

You can also have multiple instances of WDM Management Server and Other Services installed on different systems to enable load balancing. For more information, see [Configuring the Load Balancing Feature](#).

Installing WDM in a distributed setup is most suitable in a large enterprise where you are managing a large number of devices. This section describes in detail the following:

- **Installing the WDM Database**
- **Installing Management Server**
Installing the Software Repository

Installing the WDM Database

Before you install the WDM database on a system or virtual machine (VM), make sure you have the supported version of Microsoft SQL Server installed on the system. If you do not have SQL Server on the system, you can choose to install Microsoft SQL Express 2008 R2 that comes packaged with the WDM installer.

For more information on supported SQL versions, see Software Requirements.

To install the WDM database:

1. Extract the contents of the WDM installer on the system where you want to install WDM.
2. Navigate to the folder where you have extracted the installer and run Setup.exe.
   The Welcome screen is displayed.
3. Click Next.
4. Select Enterprise as the License Type.
   a. If you have the WDM License key, select the I have WDM Enterprise License Key option and enter the license key in the space provided.
   b. If you do not have the License key, select the 30–days Enterprise Evaluation option.
      The license key is entered by default. However, after the 30 days evaluation period, you need to obtain the license key and add it to WDM. For more information on adding the license key, see the Dell Wyse Device Manager Administrator’s Guide.
5. Click Next.
   The Components screen is displayed.
6. Select only the Database component.
7. In the Configure Database screen, you can choose one of the following options:
   • Install New Database Server (Microsoft SQL Express 2008 R2) — Select this option if you do not have any supported version of Microsoft SQL Server installed on the system. Proceed to step 8.
   • Use Existing Database Server (SQL Server Express or full ) — Select this option if you have already installed a supported version of Microsoft SQL Server on the system. Proceed to step 9.
8. Provide the RapportDB database credentials. RapportDB is the WDM database instance that is created on SQL Server.
   a. SQL Server Authentication is selected by default. Select Windows Authentication if you want to connect to the WDM Database (RapportDB) using your Windows login credentials.
      NOTE: Even if you choose Windows Authentication, the WDM installation always requires the SQL Authentication to access the SQL database. After you complete the WDM database installation, you must manually add the Active Directory user to the SQL database with the required security rights. You can install the remaining components only after you have completed this step.
   b. Username — The default username is rapport. You can retain the default or change the user name.
   c. Password — Enter the password to connect to the database.
   d. Confirm Password — If you are creating a new user, enter the password again.
9. If you have selected the second option in step 7, then provide the following details:
   a. **Server** — Provide the IP address of the system on which you have installed Microsoft SQL Server.
   b. **Port** — This is entered by default and the port number is 1433
   c. **Username** — Enter the user name to connect to the existing database.
   d. **Password** — Enter the password to access the database.
   e. Click Next.

10. Provide the installation path and click Next. The summary screen is displayed.

11. Click Next to begin the installation.

The installation progress is displayed on the screen and after installation is complete, you are prompted to restart your system.

Restart the system for the system changes to take effect.

### Installing Management Server/Other Services/Management Console

You can install the Management Server, Other Services, and Management Console on the same system or on different systems.

To install these components:

1. Extract the contents of the WDM installer on the system where you want to install the WDM components.
2. Navigate to the folder where you have extracted the installer and run `Setup.exe`.
   The Welcome screen is displayed.
3. Click Next.
4. Select **Enterprise** as the **License Type**.
   a. If you have the WDM License key, select the **I have WDM Enterprise License Key** option and enter the license key in the space provided.
   b. If you do not have the License key, select the **30–days Enterprise Evaluation** option.
      The license key is entered by default. However, after the 30 days evaluation period, you need to obtain the license key and re-install WDM.

5. Click Next.
   The Components screen is displayed.

6. Select **Management Server**, **Other Services**, and **Management Console**. If you are installing each of these components on separate system, you can select them one by one after following steps 1 to 5 given above.

7. Click Next to specify the WDM Database details.

8. In the **Configure Database** screen specify the following details:
   a. Select the Authentication Method. **SQL Server Authentication** is selected by default. Select **Windows Authentication** if you want to connect to the **WDM Database (RapportDB)** using your Windows login credentials.
   b. If the WDM database is created on SQL Server, then provide only the server name. If the WDM database is created on SQL Server Express, then provide the server name and the database instance name. For example, TESTVM1\RapportDB.
   c. Enter the user name and the password to access the WDM Database.
   d. Click Next.

9. In the **Services** screen, only the **ThreadX Service** is enabled and selected by default. You can select the other options and click Next.

10. Provide the installation path and click Next. The summary screen is displayed with the components you have selected.
11. Click Next to begin the installation.

The installation progress is displayed on the screen and after installation is complete, you are prompted to restart your system.
Restart the system for the system changes to take effect.

Installing the Software Repository

The Software Repository is another important component of WDM. The packages to be deployed on the client systems are saved and stored in the software repository. Before you install the Software Repository, make sure you have installed and configured the WDM database.

To install the software repository:

1. Extract the contents of the WDM installer on the system where you want to install WDM.
2. Navigate to the folder where you have extracted the installer and run Setup.exe.
The Welcome screen is displayed.
3. Click Next.
4. Select Enterprise as the License Type.
   a. If you have the WDM License key, select the I have WDM Enterprise License Key option and enter the license key in the space provided.
   b. If you do not have the License key, select the 30–days Enterprise Evaluation option.
The license key is entered by default. However, after the 30 days evaluation period, you need to obtain the license key and re-install WDM.
5. Click Next.
The Components screen is displayed.
6. Select only the Software Repository component and click Next to specify the WDM Database details.
7. In the Configure Database screen specify the following details:
   a. Select the Authentication Method. SQL Server Authentication is selected by default. Select Windows Authentication if you want to connect to the WDM Database (RapportDB) using your Windows login credentials.
   b. If the WDM database is created on SQL Server, then provide only the server name. If the WDM database is created on SQL Server Express, then provide the server name and the database instance name. For example, TESTVM1\RapportDB.
   c. Enter the user name and the password to access the WDM Database.
   d. Click Next.
   The Configure Software Repository Server screen is displayed.
8. Enter the authentication details for the Software Repository:
   a. Configure New Repository Server — select this option if you want the installer to configure the repository server. You can create a new user or use an existing user.
   b. Use Existing Repository Server — select this option if you have already configured the repository server.
   c. Select Protocols — Select the protocol and settings to distribute software to the managed devices. HTTPS is selected by default. You can also select FTP and CIFS.
   d. Authentication Type — Windows is selected by default. You can also select Basic.
   e. Username — Rapport is displayed by default. You can change this. If you select the Use existing user option, enter the user name of the existing WDM database user.
   f. Password — Enter the password to connect to the database.
   g. Confirm Password — If you are creating a new user, enter the password again.
   h. Click Next.
9. Provide the installation path and click Next. The summary screen is displayed.
10. Click **Next** to begin the installation.

The installation progress is displayed on the screen and after installation is complete, you are prompted to restart your system. Restart the system for the system changes to take effect.

**Upgrading WDM**

The current version of WDM supports an upgrade from WDM version 4.9.1 only. You cannot upgrade from any other version. If you are running an older version of WDM, you must first upgrade to version 4.9.1 and then upgrade to the latest version.

**NOTE:** After you upgrade to WDM version 5.0, you must upgrade all devices with the latest HAgent packages available to make sure your devices can be managed using WDM. For more information, see the *WDM 5.0 Release Notes*.

Before you upgrade, make sure you apply the following patches on the WDM 4.9.1 installation:

- WDM_4.9.1_HF04091034412_1
- WDM_4.9.1_HF04091013717_2
- WDM_4.9.1_HF04091025213_3
- WDM_4.9.1_HF04091031613_4

To upgrade to WDM version 5.0:

1. Extract the contents of the WDM installer on the system where you have installed WDM version 4.9.1.
2. Navigate to the folder where you have extracted the installer and run *Setup.exe*.
3. Click **Next**.
   
   The **Component Information** screen is displayed with the list of components that need to be upgraded.
4. Click **Next**.
   
   The Security Information screen is displayed.
5. Read the **Security Information** carefully and click **Next**.
   
   The upgrade process begins.

**NOTE:** The Security Information prompts you to configure the Secure Communications on your system. For more information, see *Configuring Secure Communications*.

6. After the upgrade process is complete, click **Restart Now** for the system changes to take effect before you start using WDM.

**Configuring Secure Communications**

Configuring Secure Communication using SSL:
There are different ways to install SSL in IIS 6.0 and IIS 7.0. The procedures to configure SSL in IIS 6.0 and IIS 7.0 are given below.

**Configuring SSL in IIS 6.0 on Windows Server 2003**

To configure SSL in IIS 6.0:

1. Download **IIS 6.0 Resource Kit Tools** from the link [IIS 6.0 Resource Kit Tools](#).
2. Install **IIS 6.0 Resource Kit Tools**.
3. Go to and change the directory to the location of binary `selfssl.exe` (e.g. `c:\Program Files\IIS Resources\SelfSSL`).
4. Execute the utility `selfssl` with the following parameters:
   - `selfssl /N:cn=certificate_name /S:site_id` (e.g. `selfssl /N:cn=MyComputer.Sample.com /S:1`, if site id is 1, `cn` should be a combination of computer's FQDN name and IP address)
5. Next configure the SSL Settings.
   - Go to **command prompt** and change the directory to the location of file `adsutil.vbs` (e.g. `c:\Inetpub\AdminScripts`).
   - Run the `adsutil.vbs` from the command prompt as mentioned below:
     ```
     cscript.exe adsutil.vbs set /w3svc/site_id/SecureBindings ":443
     ```

**Configuring SSL in IIS 7.0 on Windows Server 2008 R2**

To configure SSL in IIS 7.0:

1. Download **SelfSSL7** utility from the link [SelfSSL.exe](#).
2. Call the utility `SelfSSL7.exe` with the below mentioned parameters:
   ```
   SelfSSL7.exe /Q /N cn=Certificate_Name /I /S Web_Site_Name.
   ```

**Configuring Secure Communication Using Root Certificate Authority**

**Installing Root Certificate Authority in IIS 7 on Windows Server 2008 R2**

Use the following guidelines:

In order to install the certificate, two steps need to be followed:

- Install the certificate on **Domain Controller** server.
- Install the certificate on **WDM** server.

**Installing the Certificate on the Domain Controller Server**

Use the following guidelines:

1. Go to the **Server Manager**.
2. In the tree pane select **Roles** -> **Add Roles**.
3. In **Add Roles** wizard, select **Server Roles** from the tree pane.
4. In select **Server Role** window, check **Active Directory Certificate Service** from **Roles**.
5. Click **Next** -> **Next**. Then in **Role Services**, check the options **Certification Authority** and **Certificate Authority Web Enrolment**.
6. After checking the option Certificate Authority Web Enrolment, if IIS is not installed in the server, another window Add Required Role Services window will appear.

7. On the above window, click on Add Required Role Services button and click Next to invoke Specify Setup Type window.

8. In the above window depending on the requirement select either Enterprise or Standalone radio button and click Next to open Specify CA Type window.

9. In Specify CA Type window, depending on the requirement select either Root CA or Subordinate CA radio button and click Next to open Setup Private Key window.

10. In Setup Private Key window, depending on the requirement select either Create a new private key or Use existing private key radio button and click Next to open Configure Cryptography for CA window.

11. In Configure Cryptography for CA window, depending on the requirement select the value for field Select a cryptography service provider (CSP) from the combo box, provide the Key character length from the combo box, select the value for field Select the Hash algorithm for signing certificate issued by this CA and either check or uncheck Allow administrator interaction when the private key is accessed by the CA check box and click Next button to open Configure CA Name window.

   NOTE: Common name of the certificate should match with WDM server’s computer name.

12. In Configure CA Name window, provide the values for Common name for this CA and Distinguished name suffix fields and click Next to open Set Validity Period window.

13. In the Set Validity Period window, select the validity period for the certificate generated for this CA and click Next to open Configure Certificate Database window.


15. Select the default values and click Next-> Install.

16. It will install the Active Directory Certificate Services, Web Server (IIS) and Remote Server Administration Tools.

17. Once the installation of certificate is over, go to the Internet Information Services Manager of the domain controller.

18. In the Server Manager tree pane, expand Roles, and then click on Web Server (IIS)-> Internet Information Services (IIS) Manager to open IIS Manager window.

19. In the tree pane select the Server and on the right pane double click on Server Certificates.

20. In the right pane of Server Certificates, double click on Create Domain Certificate... to begin creating a certificate.

21. Fill in the information requested in the Create Certificate window and click Next to open Online Certification Authority.

22. In Online Certification Authority, click select to Specify Online Certification Authority and provide a Friendly Name for the same and click Finish.

23. Now the installation of certificate in domain controller server is done, go to the installation of certificate on WDM server.

Installing the Certificate on the WDM Server

Use the following guidelines:

1. On the taskbar, click Start-> Administrative Tools -> Internet Information Services (IIS) Manager to open the IIS Manager window.

2. In the tree pane, click on the Server and on the right pane double click on Server Certificates to open Server Certificates Window.

3. Fill in the information requested in the Create Certificate window and click Next to open Online Certification Authority.
4. In **Online Certification Authority**, click **select** to **Specify Online Certification Authority** and provide a **Friendly Name** for the same and click **Finish**.

5. Now the installation of certificate in WDM server is done.

6. After the installation of certificate, browse through **Server ->Web Sites->Rapport HTTP Server** and click on **Bindings...** on right most pane to open **Site Bindings** window.

7. In **Site Bindings** window, click **Add** to **Add Site Binding**

8. In **Add Site Binding**, select the **recently created certificate** from **SSL Certificate** combo box and click **OK** button.

9. In order to start only HTTPS communication, select **SSL Settings** under **Server->Web Sites->Rapport HTTP Server**.

10. In **SSL Settings**, select **Require SSL** check box and **Apply** the setting.
Uninstalling a Standalone Installation of WDM

If you have a standalone installation of WDM, where all the components are installed on the same system, then you can follow the steps given below to uninstall WDM.

To uninstall WDM:

1. Click the start menu and select Control Panel.
2. Click Programs → Uninstall a program on the Control Panel screen.
3. Select WDM 5.0 from the program list and click Uninstall.
   The Uninstallation Screen is displayed.
4. Click Next on the Welcome screen.
5. Enter the credentials to access the WDM database.
   You need to specify the SQL Login ID and password for SQL Server or SQL Express depending on where you have installed the WDM database.
   If you specify the wrong credentials, the program displays the following message: Unable to connect to database. Make sure you enter the correct credentials.
6. Click Next to begin the uninstallation process.
7. After the components are uninstalled you are prompted to restart your system. Click Restart Now to complete the uninstallation process.

Uninstalling WDM in a Distributed Setup

If you have installed WDM in a distributed setup, then you need to uninstall the components one by one on the systems where you have installed them.

NOTE: You must uninstall all the other components on the systems where you have installed them, before you uninstall the WDM database.

To uninstall the WDM components:

1. Log in to the system or systems where you have installed the Management Server, Management Console, Other Services, and the Software Repository.
2. Click the start menu and select Control Panel.
3. Click Programs → Uninstall a program on the Control Panel screen.
4. Select WDM 5.0 from the program list and click Uninstall.
   The Uninstallation Screen is displayed.
5. Click Next on the Welcome screen.
6. Click Next to begin the uninstallation process.
7. Log in to the system where you have installed the WDM database.
8. Repeat steps 2 to 5.
9. Enter the credentials to access the WDM database.
   You need to specify the SQL Login ID and password for SQL Server or SQL Express depending on where you have installed the WDM database.

   If you specify the wrong credentials, the program displays the following message: \textit{Unable to connect to database}. Make sure you enter the correct credentials.

10. Click \textbf{Next} to begin the uninstallation process.

11. After the database is uninstalled, restart the system when prompted.
Configuring High Availability Database Clustering for WDM

High-availability clusters (also known as HA clusters or failover clusters) are groups of computers that support server applications that can be reliably utilized with a minimum down-time. They operate by harnessing redundant computers in groups or clusters that provide continued service when system components fail.

If a server running a particular application crashes, then without clustering, the application is unavailable until the crashed server is fixed. HA clustering remedies this situation by detecting hardware/software faults, and immediately restarting the application on another system without requiring administrative intervention. This process is termed **failover**.

HA clusters usually use a heartbeat private network connection which is used to monitor the health and status of each node in the cluster.

The most common size for a HA cluster is a two-node cluster.

![Figure 1. WDM High Availability Database Clustering](image)

This section provides the steps to configure high-availability (HA) database clustering for Dell Wyse Device Manager (WDM) version 5.0 and above.
Components Required for Database Clustering

The high availability environment for WDM consists of the following components:

- **Primary Server or Primary Node** – This is one of the five Virtual Machines (VMs) on which you need to install Microsoft SQL Server 2012 database. This should have two network adapters, one configured for public and one configured for private.
- **Secondary Server or Secondary Node** – This is the second VM and ensures high availability when the primary server fails. This should also have two network adapters, one configured for public and one configured for private.
- **Server for the Quorum folder** – This is the third of the four VMs and is needed to create the Quorum folder.
- **WDM Server** – This is the fourth VM on which you need to install WDM.

Pre-requisites for Database Clustering

Database clustering requires the following:

- 4 VMware Virtual Machines (VMs) out of which 2 VMs should contain 2 network adapters each.
- Supported version of Microsoft SQL Server Database (standalone version). For more information on supported databases, see [Support Information](#).
- All the VMs should be connected to an Active Directory (AD) domain.
- All the four VMs should have Windows Server 2008 R2 installed on them.

**NOTE:** You cannot use SQL Server Express for database clustering.

Configuring the Primary and Secondary VMs

After you create the VMs on the server, you must configure them to support clustering. You must configure both the primary and the secondary nodes by following the steps given below.

To configure the primary and secondary VMs:

1. Launch the vSphere client on any system on the network and select the VM.
2. Right click and select **Edit Settings**. Click **Add** to add one more network adapter (also referred to as node).
3. In the **Add Hardware** screen, select **Ethernet Adapter** and click **Next**.
4. Select the Subnet from the **Network label** drop-down list and click **Next**.
5. Click **Finish**.
6. In the **VM Properties** screen, check that there are two nodes.
7. Launch the **Network Connections** screen from **Control Panel** → **Network and Internet** → **Network Connections** and rename the network connections to **Private** and **Public**.
8. Make sure that the **Public Network** option is first in order in the **Advanced Settings** window.
9. To launch the **Advanced Settings** window, select the **Advanced Settings** option from the **Advanced** menu in the **Network Connections** screen.
10. In the **Network Connections** screen, select the **Public**, right click and select **Properties**.
11. In the **Advanced Settings** window, select **IPv4** and click **Properties**.
12. Enter the IP address, Subnet mask, Default gateway and the Preferred DNS server. Click OK.
13. Repeat steps 10 and 11 for the Private network.
14. Make sure that the Private network contains only the IP address and Subnet mask. The Default Gateway or DNS Servers should not be defined.
15. Make sure that the servers can communicate across this network so that the nodes can communicate with each other across the network.
16. Launch the Server Manager from Start → Administrative Tools. Select Features.
17. Click Add Features to launch the Add Features wizard.
18. Select Failover Clustering and click Next.
19. Make sure that the Failover Clustering option appears in the Confirm Installation Selections screen. Click Install. The installation progress is displayed.
20. After installation completes, check the installation results and click Close.

After the Failover Clustering installation is complete, reboot the server.

Validating a Configuration

After you install Failover Clustering, you must validate the configuration on the primary node. To validate the configuration:

1. Launch the Server Manager of the primary node from Start → Administrative Tools.
2. Select Failover Cluster Manager under Features.
3. Click Validate a Configuration to launch the wizard.
4. Click Next to add the primary and secondary nodes.
5. Enter the hostname of the primary node.
6. Click Add to select the servers. The screen displays the following message while adding the servers: “The operation is taking longer than expected”. You need to wait for a few minutes for the servers to be added.
7. After the servers are selected, they are displayed under Selected Servers. Click Next.
8. A multi-site cluster does not need to pass the storage validation. To skip the storage validation process click Run only the tests I select and click Next.
9. In the Test Selection screen, uncheck the Storage option and click Next to continue. The Confirmation screen is displayed.
10. Click Next to start running the validation tests on the primary and secondary nodes (in this case cluster1 and cluster2). The status of the validation tests are displayed on the screen.
11. View the validation summary and click Finish.

Creating a Cluster on the Primary Node

After you install and validate the Failover Cluster Manager feature on the primary node, you can create a cluster.

To create a cluster on the primary node:

1. Launch Server Manager on the primary node, select Failover Cluster Manager under Features, and click Create a Cluster.
2. Click Next on the wizard.
3. Click Next to continue and in the Select Servers screen, enter the hostname of the primary node, and click Add to add the server.
4. Enter the name of the secondary node and click Add.
5. After the servers are added, click **Next** to continue. You are prompted to validate your cluster. Select **No** since your cluster is validated.

6. Select the second option on the screen and click **Next** to continue.

7. Provide a name for the cluster and an IP for administering the cluster. The name you provide is to administer the cluster. This should not be the same as the name of the SQL Cluster resource that you will create later. Enter **WINCLUSTER** as the name of the cluster and enter the IP address. Click **Next** to continue.

   **NOTE:** This is also the computer name that you need to provide permission for the File Share Majority Quorum, that is described later in this document. For more information, see Implementing a Node and File Share Majority Quorum.

8. Confirm and click **Next**.

   The cluster forming progress is displayed on the screen. If you have performed all the steps correctly, then the cluster formation is successful. If you see the yellow warning symbol on the screen, then it indicates that the cluster formation was successful, but with warnings.

9. Click **View Report** to view the warnings while forming the cluster. The report is displayed with warning messages highlighted in yellow.

10. Ignore the warning messages and click **Finish** to complete the cluster formation process.

### Implementing a Node and File Share Majority Quorum

A quorum is a design to handle the scenario when there is a problem with communication between sets of cluster nodes, so that two servers do not try to simultaneously host a resource group and write to the same disk at the same time. By having this concept of quorum, the cluster will force the cluster service to stop in one of the subsets of nodes to ensure that there is only one true owner of a particular resource group. The Node and File Share Majority quorum configuration is usually used in multi-site clusters. This configuration is used when there is an even number of nodes in the cluster, so it can be used interchangeably with the Node and Disk Majority quorum mode. In this configuration every node gets 1 vote, and additionally 1 remote file share gets 1 vote.

To configure a Node and File Share Majority Quorum:

1. Select the VM identified for creation of the quorum folder, and create a folder called **Quorum** and share the folder location.
2. Right click on the **Quorum** folder and select **Share with → Specific people**.
3. In the **File Sharing** window, select **Everyone**. Select the **Read/Write permission** and click **Share**.
   The folder is shared as `\<Name of the VM>\Quorum`.
4. You now need to change your quorum type. Launch the **Server Manager** on the primary node, and select **Fai**

   8. **Node and File Share Majority (for clusters with special configurations)** option and click **Next**.

   7. Enter the path of the shared folder that you have created on the third VM and click **Next**.

   8. Confirm the shared folder location and click **Next**.

   The quorum settings for the cluster are successfully configured.

9. **Click Finish** to complete the process and view the quorum configuration for the cluster.
Installing .NET Framework on Primary and Secondary Nodes

Microsoft .NET Framework is a pre-requisite to install SQL Server Standalone 2012 (or any other supported version of SQL Server) on the primary and secondary nodes.

To install the .NET Framework:

1. Launch Server Manager on the VMs you have identified for the primary and secondary nodes.
2. Click on Features under Server Manager to launch the Add Features Wizard and select .NET Framework 3.5.1 Features.
3. Click Next and you will prompted to install the required rol services and features to install .NET Framework 3.5.1 features.
4. Click Add Required Role Services. The option .NET Extensibility is selected by default. Click Next to continue.
5. Confirm the installation selections and click Install.
6. After the installation of the selected components is complete, the installation results are displayed.
7. Click Close to complete the .NET Framework installation.

Installing SQL Server on Primary and Secondary Nodes

Installing SQL Server on both the nodes and configuring it to function in a cluster is an important step in the setup of a high availability database cluster. This section provides the steps to install and configure SQL Server 2012 standalone on both the nodes. If you want to install any of the supported versions of SQL Server, see the installation instructions provided by Microsoft.

To install a standalone version of SQL Server 2012 on the both the nodes:

1. Launch the SQL Server 2012 installation media.
2. Click Installation and select New SQL Server stand-alone installation or add features to an existing installation.
3. Make sure that the Setup Support Rules does not display any failures. Click Next to continue.
4. Enter the Product key and click Next.
5. Check the product update and click Next.
6. Accept the license agreement and click Next.
7. Select the SQL Server Feature Installation option and click Next.
8. In the Feature Selection screen, select the Database Engine Services features and all the features under it.
9. Select the Management Tools – Basic feature and the feature under it. Click Next.
10. Make sure that the Installation Rules screen does not display any failures. Click Next.
11. In the Instance Configuration screen, make sure that the Default instance option is checked.
12. Click Next to view the Disk Space Requirements.
13. Click Next to view the Server Configuration.
14. Enter the domain credentials for server configuration and click Next.
15. In the Database Engine Configuration screen, select **Mixed Mode** and enter the SQL Administrator password and click **Add Current User**.
16. Click **Next** on the **Error Reporting** window.
17. Click **Next** and make sure that the installation configuration rules does not display any failures.
18. Click **Install** to begin the installation process.
19. After the installation completes, the installation status is displayed. View the status and click **Close** to complete the installation.

### Installing SQL Server Failover Cluster on Primary Node

After you complete installing SQL Server 2012 on both the primary and secondary nodes, you need to configure both the nodes to support the failover clustering.

To install the SQL Server 2012 failover cluster on the primary node:

1. Launch the SQL 2012 Server Installation media.
2. Click **Installation** and select **New SQL Server failover cluster installation**.
3. Make sure that the **Setup Support Rules** screen does not display any failures. Click **OK**.
4. Enter the product key and click **Next**.
5. Accept the license terms and click **Next**.
6. Check the product updates and click **Next**.
7. Make sure that the **Setup Support Rules** screen does not display any failures or errors. You can ignore the warnings and click **Next**.
8. Select the **SQL Server Feature Installation** option in the **Setup Role** screen and click **Next**.
9. Select all the options under **Instance Features → Database Engine Services**, and **Shared Features → Client Tools Connectivity** on the **Feature Selection** screen. Click **Next**.
10. Make sure that the **Feature Rules** screen does not display any failures. Click **Next**.
11. In the **Instance Configuration** screen, enter the following details:
   - **SQL Server Network Name** – WDMCLUSTER
   - **Named Instance** – WDMCLUST
   - **Instance ID** – WDMCLUST
   Click **Next**.
12. Check the **Disk Space Requirements** and click **Next**.
13. Leave the default settings on the **Cluster Resource Group** screen and click **Next**.
14. Since you have configured a **File Share Majority** clustering, you do not need to select any disk. Click **Next** on the **Cluster Disk Selection** screen.
15. In the **Cluster Network Configuration** screen, enable **IP4** and provide the IP address for the SQL Failover cluster and click **Next** to proceed to the **Server Configuration** screen.
16. Enter the domain credentials for the SQL Server Agent and SQL Server Database Engine and click **Next**.
17. In the **Database Engine Configuration** screen, select the **Mixed Mode** (SQL Server authentication and Windows authentication) option and enter the SQL Administrator password.
18. Click **Add Current User** to add the Administrator user and click **Next**.
19. You will be prompted to install a SQL Failover Cluster. Click **Yes** on the prompt.
20. Click the **Data Directories** tab on the **Database Engine Configuration** screen. In the location for the Data root directory, enter `\<Name of the Quorum VM>\quorum`. Click **Next**.
21. Check the **Error Reporting** screen and click **Next**. You can ignore the warnings.
22. Make sure that there are no failures in the **Cluster Installation Rules** screen. Click **Next**.
23. Click **Install** to begin the installation.
24. The **Installation Progress** screen displays the progress of installation. Click **Next** when the installation completes.
25. Click **Close** to complete the installation. The **Failover Cluster Manager** should be displayed in **Server Manager** under **Features**.

**Adding the Secondary Node to SQL Server Failover Cluster**

After you complete the SQL Server Failover Cluster installation on the primary node, you must add the secondary node to the Failover Cluster.

To add the secondary node to the SQL Server Failover Cluster:

1. Launch the SQL 2012 Server Installation media on the secondary node.
2. Click **Installation** and select **Add node to a SQL Server failover cluster**.
3. Make sure that the Setup Support Rules screen does not display any failures. Click **OK**.
4. The following screen is displayed. If there are failures, resolve them before you proceed. If there are warnings, ignore them and click **Next**.
5. Enter the product key and click **Next**.
6. Accept the License terms and click **Next**.
7. Add the current node to the cluster you created and click **Next**.
8. Select the virtual cluster IP in the **Cluster Node Configuration** screen. Click **Next**.
9. Enter the domain password for the SQL Server database engine and SQL Server Agent. Click **Next**.
10. Check the **Error Reporting** option and click **Next**.
11. Make sure that the **Add Node Rules** does not display any failures. Click **Next**.
12. Click **Install** to add the secondary node to the cluster.
13. The installation progress is displayed on the screen. Click **Next** when the installation completes. The installation summary screen is displayed.
14. Click **Close** to complete adding the node to the cluster. The **Failover Cluster Manager** in the **Server Manager** should display two nodes — Cluster 1 and Cluster 2.

**Post Clustering Procedure**

This section discusses the various steps you need to perform after you complete the cluster setup. These steps enable your cluster to function smoothly without any issues.

Follow the steps given below:

1. In both the cluster nodes, make sure that the SQL Server Services are started up with the domain credentials.
2. Launch the **SQL Server Configuration Manager** and select **SQL Server Services → SQL Server**. Right click and select **Properties**.
3. Check the domain credentials and click **OK**.
4. Click the **AlwaysOn High Availability** tab on both the nodes and select the **Enable AlwaysOn Availability Groups**. Click **OK**.

5. Install the WDM database in only one of the VMs that is one of the nodes of the cluster.

6. Run the following script on the database:
   
   ```
   Use RapportDB
   GO
   Update Install set ServerName='NEWCLUSTER01' where Module='Rapport4DB'
   ```

7. Add the Virtual Hostname of the cluster while installing all the WDM components without the database.

8. Create the same directory structure pointing to the database location both in the primary as well as the secondary node. For example, if the database is present in `C:\WYSE\WDM\Database` in the primary node, create the same structure in the secondary server as well.

9. Launch the SQL Server Management Studio on the primary node. Login with the default SQL user name and password.

10. Right-click on **RapportDB** database and select **Properties**.

11. In the **Database Properties** screen, change the **Recovery Model** to **Full**.

12. Right-click on the RapportDB and select **Tasks → Backup** to take a backup of the RapportDB.

13. Leave the defaults on the **Backup Database** screen and click **OK**.

14. Launch the SQL Server Management Studio, right-click on **AlwaysOn High Availability** and select **New Availability Group Wizard**.

15. The **New Availability Group wizard** is displayed. Click **Next**.

16. Provide a name for the Availability group such as **Rapport_cluster** and click **Next**.

17. Select the database and click **Next**.

18. Click **Add Replica** and select the **Automatic Failover(up to 2)** and **Synchronous commit(up to 3)** check-boxes.

19. Click **Next**.

20. Select the **Full** option and specify the shared folder location as `\<Name of the Quorum Machine>\quorum`. Click **Next**.

21. Make sure that the **Validation** screen does not display any failures. Click **Next**.

22. If you see any warnings on the screen, you can ignore them and proceed with the installation.

23. Click **Finish** to complete installing the **New Availability Group**.

24. The progress window displays the progress of the installation. Click **Next** when installation completes.

25. View the results and click **Close**.

26. The primary and secondary nodes are displayed on the SQL Server Management Studio.

27. Shutdown the secondary node and check to make sure that the primary node is running in the cluster.

28. Launch the SQL Server Management Studio on the primary node. Login with the default SQL user name and password.

29. Click on the **Security** node, select **Login**, right-click and select **New Login** to create the Rapport user. This step is important for WDM to function.

30. Select **Server Roles**, select the **sysadmin** check-box and click **OK**.

31. View the **Rapport** user on the **SQL Server Management Studio**.

### Running the HA Configuration Utility

WDM needs to connect to the cluster in order to function within the cluster and ensure that there is zero downtime.
The High Availability Configuration Utility is available after you install WDM on the primary and secondary nodes.

1. Launch the High Availability Configuration Utility from Start → All Programs → Dell Wyse Device Manager → Utilities.

2. Enter the following details:
   - **Configure Setup As** – select **Cluster** from the drop-down list.
   - **Database Name** – this is displayed by default and cannot be edited.
   - **Database Server** – Specify the hostname of the database cluster.
   - **Database User Name** – Specify **rapport** as the database user.
   - **Database Password** – Specify the password of the rapport user.

3. Click **Configure**.
   The connection details are displayed on the bottom pane of the utility.

**Adding a License on WDM**

WDM needs a license to function. The licensing code is generated based on the database. WDM is normally installed on a standalone database and then moved to a cluster. Therefore, after your cluster setup is complete, you need to generate the license code again for the cluster.

To add a license on WDM for the WDM server:

1. Launch Wyse Device Manager (WDM). The following error is displayed: “Application Function: Scopeltems_Expand: 13 Type mismatch”.
2. Click **OK** and add the license from the WDM console.
3. To initiate failover, shutdown the database on the primary node and restart the WDM Console.
Configuring Load Balancing

When you use WDM to manage thin client devices in a very large enterprise environment, a single WDM Management Server cannot scale up to manage the large number of devices. There could be problems or delays in client check-ins, schedule execution, or real-time command execution.

Load balancing helps resolve these problems to a great extent. In this setup, you can install and run multiple instances of WDM Management Servers on different systems and configure the load balancing feature between them. WDM uses the Microsoft Application Request Routing (ARR) for IIS 7 feature to perform load balancing between the management servers. This section describes how to setup and configure load balancing.

Setting up the ARR Proxy Server

The Application Routing Request (ARR) Proxy server is the most important component of Load Balancing. This server receives the requests from the thin client systems and routes them to the different WDM Management servers.

Before you set up the ARR Proxy server, you must make sure of the following:

- The entire setup should be on Windows 2008 Server R2 or higher.
- Install all the components of WDM on one server.
• Install only the WDM Management Server and Thread X Service on another server.

**NOTE:** You can set up the ARR Proxy Server and the WDM Management Servers across different subnets in the same domain.

Setting up the ARR Proxy Server consists of the following steps:

1. [Installing IIS](#).
2. [Installing the ARR Module](#).
3. [Configuring the Application Pool Process Model for ARR](#).
4. [Creating a Server Farm of WDM Management Servers](#).
5. [Configuring SSL](#).
6. [Configuring Server Farm Properties for ARR](#).
7. [Configuring Request Filtering](#).
8. [Setting up the Proxy FQDN in WDM Preferences](#).

### Installing Internet Information Services (IIS)

Install Windows 2008 Server R2 on any of the systems that you identify to be the ARR Proxy Server. To install IIS:

1. Log in to the system as an administrator and launch the Server Manager.
2. Select **Roles** under Server Manager and click **Add Roles** on the right-hand pane. The **Add Roles Wizard** is displayed.
3. Select **Server Roles** and check **Web Server (IIS)** and click **Next**.

4. Select the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Sub-options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common HTTP Features</strong></td>
<td>• Static Content</td>
</tr>
<tr>
<td></td>
<td>• Default Document</td>
</tr>
<tr>
<td></td>
<td>• HTTP Errors</td>
</tr>
<tr>
<td></td>
<td>• Directory Browsing</td>
</tr>
<tr>
<td><strong>Health and Diagnostics</strong></td>
<td>• HTTP Logging</td>
</tr>
<tr>
<td></td>
<td>• Request Monitor</td>
</tr>
<tr>
<td></td>
<td>• Logging Tools</td>
</tr>
<tr>
<td></td>
<td>• Tracing</td>
</tr>
</tbody>
</table>

5. Click **Next** to view the summary.

6. Click **Install** to install IIS.
Installing the ARR Module

You must install the Application Request Routing version 3.0 on the system you have identified to be the ARR Proxy Server. The installer is available on the Microsoft download site at http://www.microsoft.com/web/gallery/install.aspx?appid=ARRv3_0. Download the ARRv3_0.exe file and install it.

Configuring the Application Pool Process for ARR

All HTTP requests and responses for the content sites go through Application Request Routing. For this to function correctly you must make sure that the worker process of the Default Web Site on ARR is always running.

To configure the application pool process:

1. Log in to the ARR Proxy Server, and launch the IIS manager.
2. Select Application Pools under the root node.
   The right-hand pane displays DefaultAppPool as the application pool for the Default Web Site.
4. Select **Advanced Settings** to display the **Advanced Settings** window.

5. Under **Process Model** change the value of **Identity** from **LocalSystem** to **ApplicationPoolIdentity**.

6. Change the **Idle Time-out (minutes)** to 0 to disable the setting. Click **OK** to save the changes.

**Creating a Server Farm of WDM Management Servers**

To create and define a server farm:

1. Log in to the ARR Proxy Server system and launch the IIS Manager.
2. Select **Server Farms** under the root node. This option is available only after you install the ARR Proxy module.
3. Right-click and select **Create Server Farm** from the menu. The **Create Server Farm** screen is displayed.

![Create Server Farm Screen](image)

- **Specify Server Farm Name**
  - **Server farm name:** WEMServer
  - **Online**

[Previous] [Next] [Finish] [Cancel]
4. Enter a name for the server farm. For example, **WDMServerFarm**. Click **Next** to add the WDM Management servers.

5. Type the host name of the WDM Server and click **Add**. You can add all the servers where you have installed the WDM Management Server.

6. Click **Finish** to add all the servers to the farm.

7. Click **Yes** so that IIS manager can create a URL rewrite rule to route all incoming requests to this server farm.

**Configuring SSL**

One of the features in ARR is **SSL off-loading**. This is a feature in which the communications between the clients and the ARR Proxy Server are done via SSL, and the communications between the ARR Proxy Server and the WDM Management Servers are done via clear text. By enabling this feature, you can help to maximize the server resources on the WDM Management Servers.

You first need to create the SSL Certificate on the ARR Proxy Server.

To create and configure the SSL Certificate:

1. Log in to the ARR Proxy Server and launch the IIS Manager.
2. Select the root node and open the **Server Certificates** page from the right-hand pane.
3. Click **Create Domain Certificate** on the Action pane.
4. Provide the name of the ARR Proxy Server in the Create Certificate wizard.
5. Click Next to complete creation of the certificate.
6. Select Default Web Site under Sites and click Bindings on the Actions pane.
7. Assign the certificate to HTTPS binding.
8. Double click on Routing Rules and select the Enable SSL offloading option if you want the communication between the ARR Proxy Servers and the WDM Management Servers to be in plain text. You also need to add both the HTTP and HTTPS ports to the Default Web Site Bindings on the individual WDM Management Server systems.

**NOTE:**
If you want the communication between the ARR Proxy Server and the WDM Management Servers also to be on the HTTPS protocol, then you must disable the SSL off-loading feature and configure SSL on the individual WDM Management Servers. If you use a self-signed certificate setting up SSL on the WDM Management Server, then import this certificate to the Trusted Root Certificate Authorities store for a local computer on the ARR Proxy Server by following the steps available on Microsoft website: [http://technet.microsoft.com/en-us/library/cc754841.aspx#BKMK_addlocal](http://technet.microsoft.com/en-us/library/cc754841.aspx#BKMK_addlocal)

### Configuring Server Farm Properties for ARR

After the server farm has been created and defined, you need to set additional properties to manage the behavior of ARR.

To configure server farm properties:

1. Log in to the ARR Proxy Server and launch the IIS Server Manager.
2. Select the Server Farm you created. The following options are displayed on the right-hand pane:
   - Caching
   - Health Test
   - Load Balance
   - Monitoring and Management
   - Proxy
   - Routing Rules
   - Server Affinity
3. Select Caching.
   a. De-select the Enable disk cache option to disable caching.
   b. Set the Memory cache duration to 0.
4. Select Health Test.
   a. Enter the fully qualified domain name (FQDN) of the ARR proxy server in the URL field. The value should be: `http(s)://<ProxyFQDN>/hserver.dll?&V93`. This is the URL, which ARR uses to send requests to the WDM Management Server to check the Health for a particular server farm.
   b. Set the Interval time period after which the ARR Health Test repeats the Health Check. The default is 30 seconds. You can set it to 180 seconds.
   c. Set the time out period of the URL you specified. This is the time period during which if the server does not respond, it is marked as Unhealthy.
   d. Set the Acceptable Status codes to 200–399. If the health URL returns a status code that does not match with the value in the Acceptable Status Codes, then ARR marks that server as unhealthy.
   e. Set the text value Server Healthy in the Response Match field. The text in Response Match is verified against the response entity from each server and if response from server does not contain the string specified in response match then that server is marked as unhealthy.
   f. Click Verify URL. This should pass for all the WDM Management Servers in the server farm.
5. Change the **Load Balance** algorithm.
   a. Select **Weighted Round Robin** from the **Load balance algorithm** drop-down list.
   b. Select **Even distribution** from the **Load distribution** drop-down list.
   c. Click **Apply**.

6. Double click the **Monitoring and Management** option to view the WDM Management Server health status and other statistics.

7. Double click **Proxy** to configure the proxy settings:
   a. Change the **Response buffer threshold** value to 0.
   b. De-select the **Keep Alive** option.
   c. Change the **HTTP version** to **HTTP/1.1**.
   d. Select the **Reverse rewrite host in response headers** option.

8. Double click **Routing Rules**.
   a. Click **URL Rewrite** on the **Actions** pane.
   b. In the **Edit Inbound Rule** page, set the **Pattern** to *hserver.dll*.

   This step ensures that the ARR Proxy Server forwards only the URL requests meant for the WDM Management Server to the Server Farm.

The Server Farm properties are now configured.

### Configuring Request Filtering

To configure request filtering:

1. Log in to the ARR Proxy Server and launch the IIS Manager.
2. Select **Default Web Site** under **Sites** and on the right-hand pane double click on **Request Filtering**.
3. Click **Edit Feature Settings**.
4. Set the **Request Limits** as shown below:

![Edit Request Filtering Settings](image)

- **General**
  - Allow unlisted file name extensions
  - Allow unlisted verbs
  - Allow high-bit characters
  - Allow double escaping

- **Request Limits**
  - Maximum allowed content length (Bytes): 4294967295
  - Maximum URL length (Bytes): 40960
  - Maximum query string (Bytes): 40960

5. Click **OK** to apply the settings.

**Setting up Proxy FQDN in WDM Preferences**

To complete the Load Balancing setup, you need to specify the Proxy server details in WDM. To setup the Proxy FQDN in WDM:

1. Log in to the system where you have installed WDM and launch the WDM Console.
2. Select **Configuration Manager → Preferences**.
3. Double click on **Service Preferences** and in the **Preferences** window, select **Serv/Port Settings**.
4. Enter the FQDN of the ARR Proxy Server in the **Alias Server Name** field. For example, **WIN2K8–Ent-N.test-blr.com**
5. Click **OK** to save the settings.

The ARR Proxy Server is now recorded in the WDM database, and this completes the Load Balancing setup.

**Installing WDM Components**

The load balancing setup needs multiple installations of WDM Management Servers. However, you must make sure that one of the systems in this setup has a complete installation of WDM. You can then install only the Management Server and the ThreadX Service on the other systems. For more information on installing only the selected components, see [Installing Management Server](#).
Configuring Load Balancing for ThreadX Devices

When you want to manage a large number of PCoIP (ThreadX) devices, then a single ThreadX Manager Service may not scale up to manage the large number of ThreadX devices. Configuring load balancing for ThreadX devices helps you to manage a large number of such devices.

Before you configure Load Balancing for ThreadX devices, you first need to identify a Windows 2008 R2 system and install the Domain Name Server (DNS) on the system.


The load balancing mechanism uses the DNS Round Robin method to share and distribute the network resource loads.

To set up the DNS Round Robin:

1. Log in to the DNS Server and launch the DNS Manager.
2. Select the server name on the tree in the left pane, right-click and select **Properties** from the menu. The **Properties** window is displayed.
3. Click the **Advanced** tab on the **Properties** window.
4. In the **Server Options** pane, make sure that the options **Enable round robin** and **Secure cache against pollution** are checked.
5. If you require netmask ordering, then select the **Enable netmask ordering** option. This feature tries to prioritize local resources for the clients.
6. Click the **View** menu on the DNS Manager and select the **Advanced** option.
7. Expand the **Domain** node and under **Forward Lookup Zones**, select the domain. For example, WDMSQA11.com.
8. Right-click and select **New Host (A or AAAA)....** The **New Host** window is displayed.
9. Enter the virtual host name of the ThreadX Server Farm that will participate in the load balancing. For example, ThreadXServer1. The FQDN of the server is displayed automatically.
10. Enter the IP address of the server.
11. Click **Add Host**.
12. Repeat steps 8–11 to add as many ThreadX Servers as you want.
13. Select the **Domain** node on **DNS Manager**, right-click and select **Other New Records**.
14. In the **Resource Record Type** dialog box, select **SRV Location** and click **Create Record**.
15. In the New Resource Record dialog box, enter the following values:
   - **Service Name** – _PCOIP-broker
   - **Protocol** – _tcp
   - **Port Number** – 50000.
   - **Host Offering this Service** – enter the hostname of the ThreadX Server Farm.
16. Repeat steps 13–15 to add the _PCOIP-tool SRV record.
17. Configure DNS Caching:
   a. On the DNS Manager, expand the Domain node and under it select the _tcp node.
   b. Select PCOIP-tool on the right-hand pane, right-click and select Properties.
   c. In the Properties window, check the Time to live (TTL) value. The caching interval is called the Maximum TTL value and the default is 1 hour. You can change this if you want.
      The TTL field is displayed only if you have selected Advanced View in the View menu of the DNS Server.

The load balancing is now configured for ThreadX devices and you can use your WDM Management Servers to manage a large number of ThreadX devices.
Troubleshooting

This section describes how to troubleshoot the issues that you may encounter while installing or upgrading WDM.

.NET Framework Installation Error in Windows 2012

Issue: .NET Framework 3.5 installation fails on Windows Server 2012 with error code 0x800F0906

Resolution:

Method 1:
1. Log in to the system where you have installed Windows Server 2012 and launch the Server Manager.
2. Install .NET Framework 3.5 features using the Add Roles and Features wizard in Server Manager.
3. While installing specify an alternate source path using the link at the bottom of the wizard.

Method 2:
Using DISM from the command prompt, specify the source files path parameter:

For example, if D: is the Windows Server DVD media, the source files path would be: DISM /Online / Enable-Feature /FeatureName:NetFx3ServerFeatures /FeatureName:NetFx3 /Source:D:\Sources\sxs

Method 3:
1. Log in to the system where you have installed Windows Server 2012 and launch the Server Manager.
2. Install Server Role Windows Server Update Services (WSUS) using Add Roles and Features Wizard in Server Manager.
3. Using DISM from the command prompt, specify the source files path parameter: DISM /Online / Enable-Feature /FeatureName:NetFx3ServerFeatures /FeatureName:NetFx3
4. Make sure Windows Update Service is running, and Windows Update store can be connected from where the necessary components can be retrieved.

Failure While Attaching the Database

Issue: Failure while attaching the database on Windows 2012 Server, with SQL Server 2012.

Resolution:

Run SQL Service ‘MSSQLSERVER’ using the ‘LocalSystem’ account on the system where WDM installation is targeted.
Retry WDM installation.

Database Installation Failure After Manual Uninstallation of SQL Server Express 2008

**Issue:** The WDM database installation fails after you manually uninstall the existing SQL Server Express 2008, and use the **Install New Database** option in the installer.

**Resolution:** To resolve this issue:

1. Uninstall SQL Server Express 2008 R2 from Add\Remove Programs.
2. Launch the **Services** window from **Control Panel → Administrative Tools**.
3. Delete the **MSSQL$RapportDb** Service
4. Delete **MSSQL10_50.RAPPORTDB** from the SQL Server Express Installation folder.
5. Delete the **RapportDB** registry entry from **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Microsoft SQL Server\Instance Names\SQL**.
6. Delete the **MSSQL10_50.RAPPORTDB** registry entry from **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server**.
7. Delete the **RAPPORTDB** registry entry from **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Microsoft SQL Server**.
8. Restart the WDM Installer.

Troubleshooting Load Balancing Issues

This section describes how to troubleshoot some issues that you may encounter in the Load Balancing setup.

**Health Test Feature in ARR Proxy (with SSL) Fails with Error Code 80072F8F**

**Issue:** If the ARR Proxy does not trust the backend server’s Digital Certificate, the health test may fail with the Error Code 80072F8F.
Resolution: Import the certificate that is used to setup SSL on the WDM management server onto the Trusted Root Certificate Authorities store for a local computer on the ARR Proxy system by referring to http://technet.microsoft.com/en-us/library/cc754841.aspx#BKMK_addlocal.

ARR Proxy Returns HTTP Error Code 502.3

Issue: The ARR Proxy returns the HTTP Error Code 502.3 for older WDM Agents (HAgents) that do not send the HTTPHEADSUPP=2 tag when they are checking in. If the HAgent does not send the HTTPHEADSUPP=2 tag while checking in, then the Management Server does not send the HTTP status code header (200 OK) in response and the ARR proxy returns the error. Only the clients sending the value 2 are supported in load balancer setup.

Resolution: You can run the following query on the WDM Database and read the value:

SELECT [HttpHeadSupp]
FROM    [ClientNetwork]
where  [MAC] = <ClientMac>

ARR Proxy Returns HTTP Error Code 502.4

Issue: The ARR Proxy server could return the HTTP Error Code 502.4 when any of the Management Servers (HServers) are not available. The Health Status of all the HServers in the Server Farm may be set to Unhealthy because the configured Health Tests have failed.

Resolution: To correct this:

1. Log in to the ARR Proxy Server and launch the IIS Server Manager.
2. Select the Server Farm you created and on the right-hand pane, select Monitoring and Management.
3. Select the HServers and in the Action pane, select Set Server as Healthy.
4. If the load on the HServer is high then try to increase the interval and time-out values in the Health Test feature.

Enabling SSL Offloading on Proxy

Load Balancing is only supported in HTTPS setup. For debugging, if you want to see the Management Server (HServer) response in Wireshark capture, then you can change the HServer-Proxy communication to HTTP.

1. Log in to the ARR Proxy Server and launch the IIS Manager.
2. Double click the Routing Rules feature and select Enable SSL offloading setting.
3. Enable both HTTP and HTTPS binding in the website on the HServer machines and do not select Require SSL in the SSL Settings.

..