Dell Wyse Device Manager 5.7.2
Installation Guide

Notes, cautions, and warnings

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

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.

2017–02

Rev. A03

Contents

GUID-138DCFA2-F92E-4E1A-831F-BF7752000E32

1

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.

GUID-E9D79B7D-6496-4B19-94AD-A19BD1030087

Installer Matrix

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

			Windows Server 2008 R2 SP1			
RapportDB Authentication		**SQL**			**Windows**	
	Enterprise	**Workgroup**	**Distributed**	**Enterprise**	**Workgroup**	**Distributed**
Windows 2008 R2 SP1 + SQL Express 2014	Yes	Yes	Yes	Yes	Yes	Yes
Windows 2008 R2 SP1 + SQL Server 2008 R2	Yes	Yes	Yes	Yes	Yes	Yes
Windows 2008 R2 SP1 + SQL Server 2008	Yes	Yes	Yes	Yes	Yes	Yes
Windows 2008 R2 SP1 + SQL Server 2012	Yes	Yes	Yes	Yes	Yes	Yes
			Windows Server 2012			

			Windows Server 2008 R2 SP1			
RapportDB Authentication		**SQL**			**Windows**	
Windows 2012 + SQL Express 2014	Yes	Yes	Yes	Yes	Yes	Yes
Windows 2012 + SQL Server 2008 R2	Yes	Yes	Yes	Yes	Yes	Yes
Windows 2012 + SQL Server 2008	Yes	Yes	Yes	Yes	Yes	Yes
Windows 2012 + SQL Server 2012	Yes	Yes	Yes	Yes	Yes	Yes

GUID-601CA685-50C7-4427-8F88-2616CB02148F

Support Information

This section lists out the supported operating systems, the supported databases, and the supported thin client devices for WDM version 5.7.2

Supported Operating Systems for WDM Server	• Windows Server 2008 R2 Enterprise SP1 • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows 7 Enterprise SP1(32-bit) • Windows 7 Enterprise SP1 (64–bit)
Supported Operating Systems to Upgrade all WDM Components	• Windows 2008 R2 SP1 Enterprise • Windows 2008 SP2 32-bit
Supported Databases	• Microsoft SQL Server Express 2014 - English • Microsoft SQL Server 2008 R2 – English • Microsoft SQL Server 2008 Enterprise (32 bit) • Microsoft SQL Server 2012 • Microsoft SQL Server 2012 Enterprise Edition for High Availability.
Supported Thin Client Devices	**Wyse ThinOS:** • Wyse 3010 thin client with ThinOS • Wyse 3020 thin client with ThinOS • Wyse 5010 thin client with ThinOS • Wyse 5040 thin client with ThinOS • Wyse 3030 LT thin client with ThinOS • Wyse 5060 thin client with ThinOS • Wyse 7010 thin client with ThinOS **Wyse ThinOS PCoIP** • Wyse 5040 AIO thin client with PCoIP

	• Wyse 5010 thin client with PCoIP • Wyse 3030 LT thin client with PCoIP • Wyse 5060 thin client with PCoIP **Wyse Enhanced Microsoft Windows Embedded Standard 7 (WES7) build 818 or later:** • Wyse 5010 thin client with WES7 • Wyse 5020 thin client with WES7 • Wyse 7010 thin client with WES7 • Wyse 7020 thin client with WES7 • Wyse 7010 extended chassis thin client with WES7 • Wyse 3030 thin client with WES7 **Wyse Enhanced Microsoft Windows Embedded Standard 7p (WES7p) build 850 or later:** • Wyse 7010 thin client with WES7P • Wyse 7010 extended chassis thin client with WES7P • Wyse 5020 thin client with WES7P • Wyse 7020 thin client with WES7P • Wyse 7040 thin client with WES7P • Dell latitude E7270 mobile thin client • Wyse 5060 thin client with WES7P • Dell latitude 3460 mobile thin client **Wyse Enhanced Microsoft Windows Embedded 8 Standard (64-bit) (WE8S):** • Wyse 5010 thin client with WE8S • Wyse 5020 thin client with WE8S • Wyse 7010 thin client with WE8S • Wyse 7020 thin client with WE8S **Windows 10 IoT Enterprise (64–bit) (WIE10)** • Wyse 5020 thin client with Win10 IoT • Wyse 7020 thin client with Win10 IoT • Wyse 7040 thin client with Win10 IoT **Wyse Enhanced SUSE Linux Enterprise:** • Wyse 5010 thin client with Linux • Wyse 5020 thin client with Linux • Wyse 7010 thin client with Linux • Wyse 7020 thin client with Linux **ThinOS Lite :** • Wyse 3010 zero client for Citrix • Wyse 3020 zero client for Citrix • Wyse 5010 zero client for Citrix • Wyse 3010 thin client with Linux **ThreadX/View Zero Client:** • Wyse 5030 zero client

	- Wyse 7030 zero client - Wyse 5050 AIO zero client with PCoIP **Thin Linux:** - Wyse 3030 LT thin client with ThinLinux - Wyse 7020 thin client with ThinLinux - Wyse 5020 thin client with ThinLinux - Wyse 5060 thin client with ThinLinux
Supported EOL Dell Wyse Thin Client Platforms	**Wyse Enhanced Microsoft Windows Embedded Standard 7 (WES7) build 818 or later:** - C90LE7 - R90L7 - R90LE7 - X90c7 - X90m7 - Z90s7 **Wyse Enhanced Microsoft Windows Embedded Standard 7P (WES7P):** - X90m7P - Z90s7P **Wyse Enhanced Microsoft Windows Embedded 8 Standard (32-bit) (WE8S) :** - Wyse 5010 thin client with WE8S - Wyse 7010 thin client with WE8S - Z90D8E **Wyse Enhanced SUSE Linux Enterprise:** - C50LE - R50L - R50LE - X50c - X50M - Z50S **ThinOS Lite:** - C00X - R00X **ThreadX/ View Zero Client:** - P20 **Wyse ThinOS:** - C10LE - R10L **Wyse Enhanced Microsoft Windows Embedded Standard 2009 (WES2009) build 641 or later:** - C90LEW - 5010 - R90LW

	• R90LEW • V90LEW • X90CW • X90MW • 7010 • Z90SW

GUID-74DD12B0-B05D-498C-9AD7-F0C62A556CB5

Localization Support

For the WDM Server, localization support is provided on Windows 2008 R2 SP1 Enterprise Edition and Windows 2012 Standard R2 for the following languages:

- French
- German
- Spanish
- Japanese
- Simplified Chinese

GUID-5FE389BD-ACDA-439F-A5FA-BEC06DE1A0AD

Dell Wyse technical support

To access technical resources self-service portal, knowledge base, software downloads, registration, warranty extensions/ RMAs, reference manuals, and so on, visit www.dell.com/wyse/support . For Customer Support, visit www.dell.com/support/contents/us/en/19/article/Contact-Information/International-Support-Services/international-contact-center?ref=contactus , and phone numbers for Basic and Pro Support are available at www.dell.com/supportcontacts .

NOTE: Before proceeding, verify if your product has a Dell service tag. For Dell service tagged products, go to www.dell.com/support/contents/us/en/19/article/Product-Support/Dell-Subsidiaries/wyse for more information.

GUID-0FB4A342-C2F9-4AF9-A5D1-CCC84C3270E4

Related documentation and services

Fact sheets containing features of hardware products are available on the Dell Wyse website. Go to http://www.dell.com/wyse and select your hardware product to locate and download the Fact Sheet.

To get support for your Wyse product, check your product Service Tag or serial number.

- For Dell service tagged products, find knowledge base articles and drivers on the Dell Wyse product pages.
- For Non-Dell Service Tagged Products, find all the support needed by accessing the Wyse support domain.

GUID-4D517BA7-FAA9-4B40-9D91-0570FD6D0BB4

Dell Wyse online community

Dell Wyse maintains an online community where users of our products can seek and exchange information about user forums. Visit the Dell Wyse online community forums at: en.community.dell.com/techcenter/enterprise-client/wyse_general_forum/.

GUID-4B94E14A-4924-456B-AAFE-9D1F2BA0DD32

2

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

GUID-6AEACD37-9A9A-412D-972B-73B289DBCB4E

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 Support Information.
- 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.
- The server must be installed with ThreadX 5x components in Windows 2012 and above.

GUID-1E0BCB03-473D-40B5-A137-729BC9694152

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

Category	Minimum Requirements	Recommended Configuration
CPU	2.5 GHz Dual core Intel or AMD	Quad Core Intel or AMD
RAM	4 GB In case of a Virtual Machine, it should be 2 GB initially allocated	4 GB
Minimum Free Space	40 GB	40 GB

Server Hardware Requirements for 64–bit OS

Category	Minimum Requirements	Recommended Configuration
CPU	2.5 GHz Dual core Intel or AMD	Quad Core Intel or AMD
RAM	6 GB	8 GB
Minimum Free Space	40 GB	40 GB

GUID-890DB071-0449-4500-B50B-F96892299BFA

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

WDM Component	Protocol and Corresponding Ports	Port	Function
GUI	HTTP	80	Communicate with the Web Service and Standard Service.

WDM Component	Protocol and Corresponding Ports	Port	Function
		280	
	FTP	21	Register new packages into the Master Software Repository.
	OLE DB	1433 (default) Can be configured during installation.	Communicate with the WDM database.
	VNC	5800 5900	Remote shadows devices.
Web Service	HTTP	80 280	Communicates with the Web Agent, GUI, and Standard Service.
	HTTPS	443 8443	Secure Communication with the Web Agent, GUI, and Standard Service.
	OLE DB	1433 (default) Can be configured during installation	Communicate with the WDM Database.
Web Agent	HTTP	80 280	Communication with the Web Service.
	FTP	21	Read and write files to the master and remote software repositories.
DHCP Proxy and TFTP Services	OLE DB	1433 (default) Can be configured during installation	Communicate with the WDM database.
	HTTP	8008	Communicate with the GUI and Web Service.
DHCP Proxy and TFTP Services and PXE	DHCP	67 68 4011	Process UDP requests from PXE-enabled devices to the Standard Service.
	TFTP	69	Download bootable image to enable management processing.
	HTTP	80	Communicate with the Web Service regarding actions and status of current task.
	FTP	21	Download and upload files to the master and remote software repositories.

WDM Component	Protocol and Corresponding Ports	Port	Function
DHCP Proxy and TFTP Services and legacy support for older WDM agents	UDP	44956 44957	Discover devices using subnet directed broadcasts that have older WDM Agents (5.0.0.x and earlier) installed.
	TCP	44955	Discover devices using IP Range Walking. Upgrade devices that have an older WDM Agent (5.0.0.x and earlier) installed.
ThreadX 4.x Manager Service	TCP	9880 50000	Communicate with ThreadX 4.x devices.
ThreadX 5.x Manager Service	TCP	49159 5172	Communicate with ThreadX 5.x devices. **NOTE: Both the communication ports has to be added to firewall Inbound rules. If required, 49159 port number can be customized. The default port 49159 is customized, this needs to be manually added.**

GUID-0A235F63-E857-4466-B578-235ACE4E9AB3

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 every 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.
- **ThreadX 4.x**:

  Configure FTP if you intend to use the firmware upgrade feature for PCoIP (ThreadX 4.x) 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*.
- **ThreadX 5.x**:

  Configure CIFS if you intend to use the firmware upgrade feature for PCoIP (ThreadX 5.x) devices. You must enable this in the Software Repository. For more information on enabling CIFS in the Software Repository, see the *Dell Wyse Device Manager Administrator's Guide*

  .

GUID-074DE4D6-9D3B-494E-AC6C-35CFD411B76C

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 Express 2014 as the default option, but you can choose another supported version of SQL Server.
- You must install FTP services and it should be active to use FTP for Dell Wyse PCoIP (ThreadX 4.x) devices.
- You must install CIFS services and it should be active to use CIFS for Dell Wyse PCoIP (ThreadX 5.x) 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 Balancing for ThreadX 4.x Devices and Configuring Load Balancing for ThreadX 5.x Devices

GUID-6DAC9ED4-4806-406E-B7A1-1B04E9444C31

3

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
- Web UI

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 upto 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: Workgroup license needs to be activated.

NOTE:

- To run the WDM Installer (Setup.exe), you must log in to the system as an Administrator.
- 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.
- 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.
- The Dell Community Forums supports the WDM Workgroup.
- Threadx 5x management component is supported only in enterprise edition.

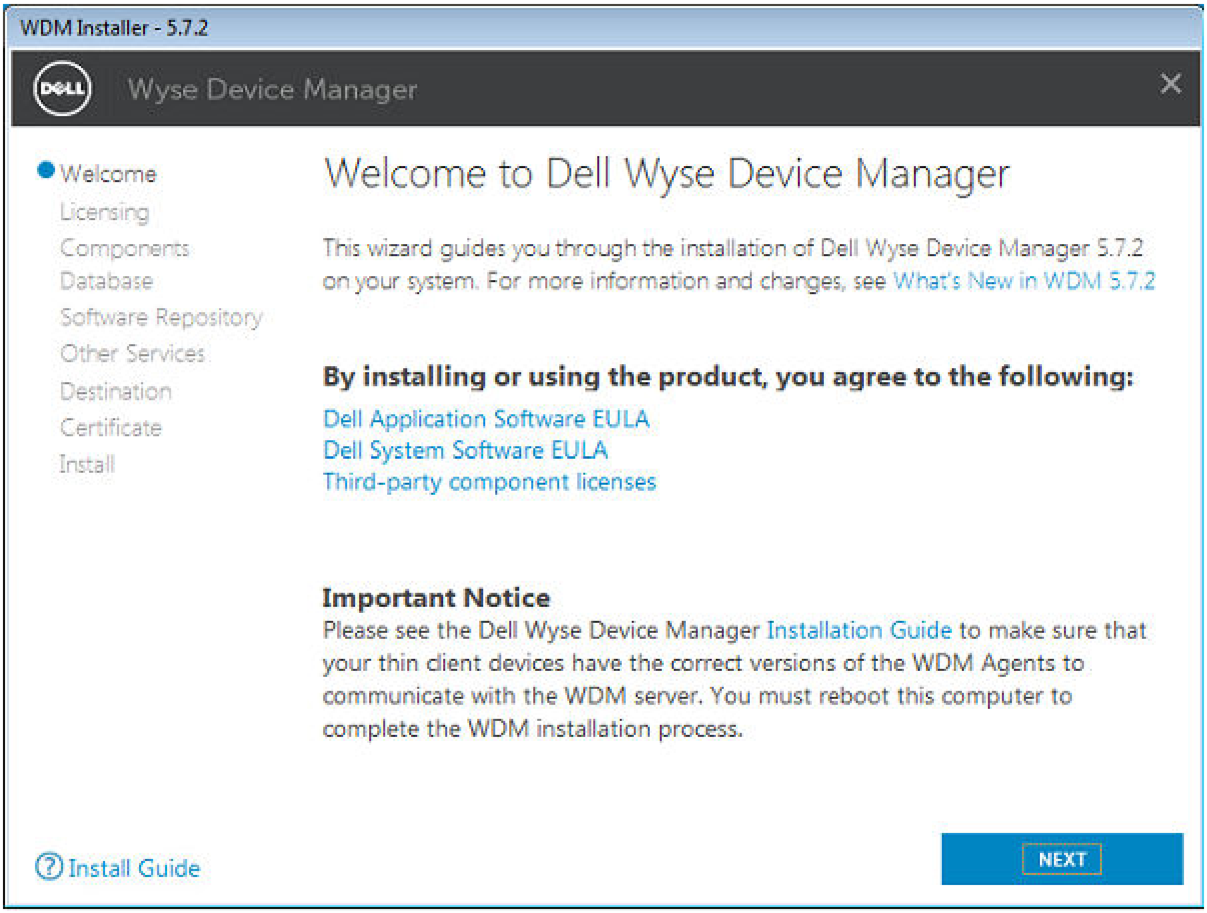
GUID-0B71DF78-674B-4DF0-9868-B2250826321E

Installing the WDM Workgroup Edition

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.



WDM Installer - 5.7.2

Wyse Device Manager

Welcome to Dell Wyse Device Manager

This wizard guides you through the installation of Dell Wyse Device Manager 5.7.2 on your system. For more information and changes, see What's New in WDM 5.7.2

By installing or using the product, you agree to the following:

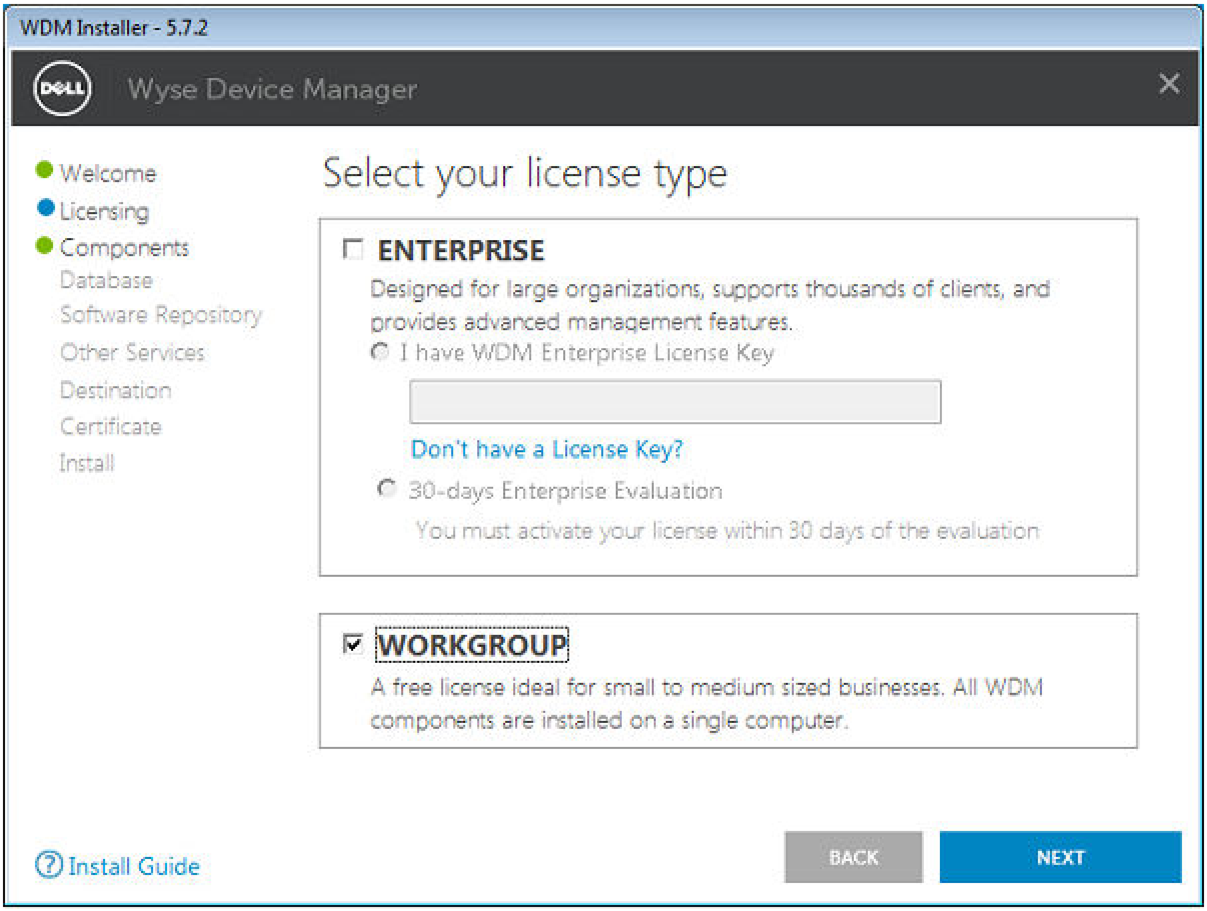
Dell Application Software EULA
Dell System Software EULA
Third-party component licenses

Important Notice

Please see the Dell Wyse Device Manager Installation Guide to make sure that your thin client devices have the correct versions of the WDM Agents to communicate with the WDM server. You must reboot this computer to complete the WDM installation process.

Figure 1. WDM Installer 5.7.2 Screen

3. Click **Next**.
4. Select **Workgroup** as the **License Type** and click **Next**.



Select your license type

☐ **ENTERPRISE**

Designed for large organizations, supports thousands of clients, and provides advanced management features.

○ I have WDM Enterprise License Key

Don't have a License Key?

○ 30-days Enterprise Evaluation

You must activate your license within 30 days of the evaluation

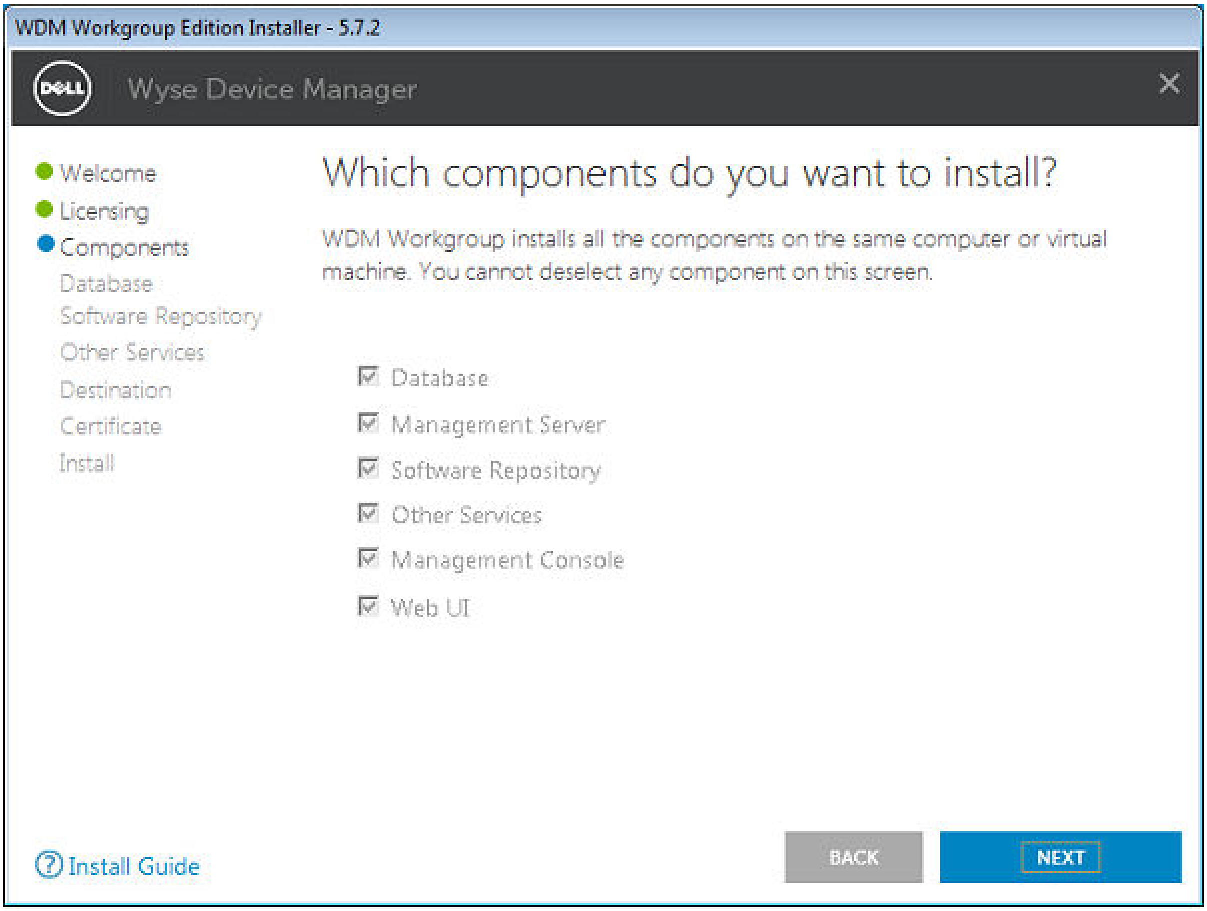
☑ **WORKGROUP**

A free license ideal for small to medium sized businesses. All WDM components are installed on a single computer.

Figure 2. WDM Installer 5.7.2 (Workgroup) Screen

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.**


WDM Workgroup Edition Installer - 5.7.2

Wyse Device Manager

Which components do you want to install?

WDM Workgroup installs all the components on the same computer or virtual machine. You cannot deselect any component on this screen.

☑ Database

☑ Management Server

☑ Software Repository

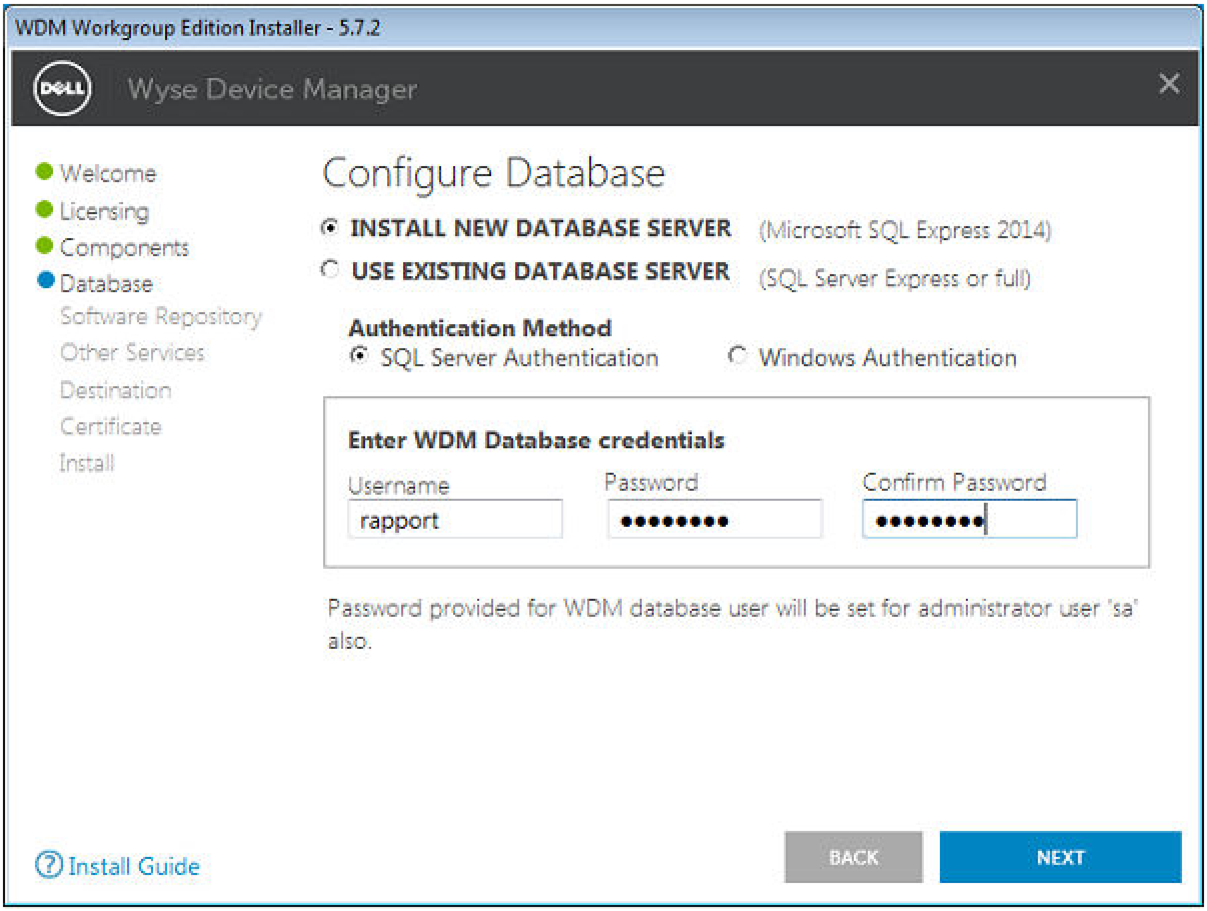
☑ Other Services

☑ Management Console

☑ Web UI

Figure 3. Components Screen

6. In the **Configure Database** screen, you can choose one of the following options:
   - **Install New Database Server (Microsoft SQL Express 2014)** — Select this option if you do not have any supported version of Microsoft SQL Server installed on the system. **Proceed to step 7**.


WDM Workgroup Edition Installer - 5.7.2

Wyse Device Manager

Configure Database

● INSTALL NEW DATABASE SERVER (Microsoft SQL Express 2014)

○ USE EXISTING DATABASE SERVER (SQL Server Express or full)

Authentication Method

● SQL Server Authentication ○ Windows Authentication

Enter WDM Database credentials

Username: rapport

Password: ●●●●●●●●●

Confirm Password: ●●●●●●●●●

Password provided for WDM database user will be set for administrator user 'sa' also.

Figure 4. New Database Configuration

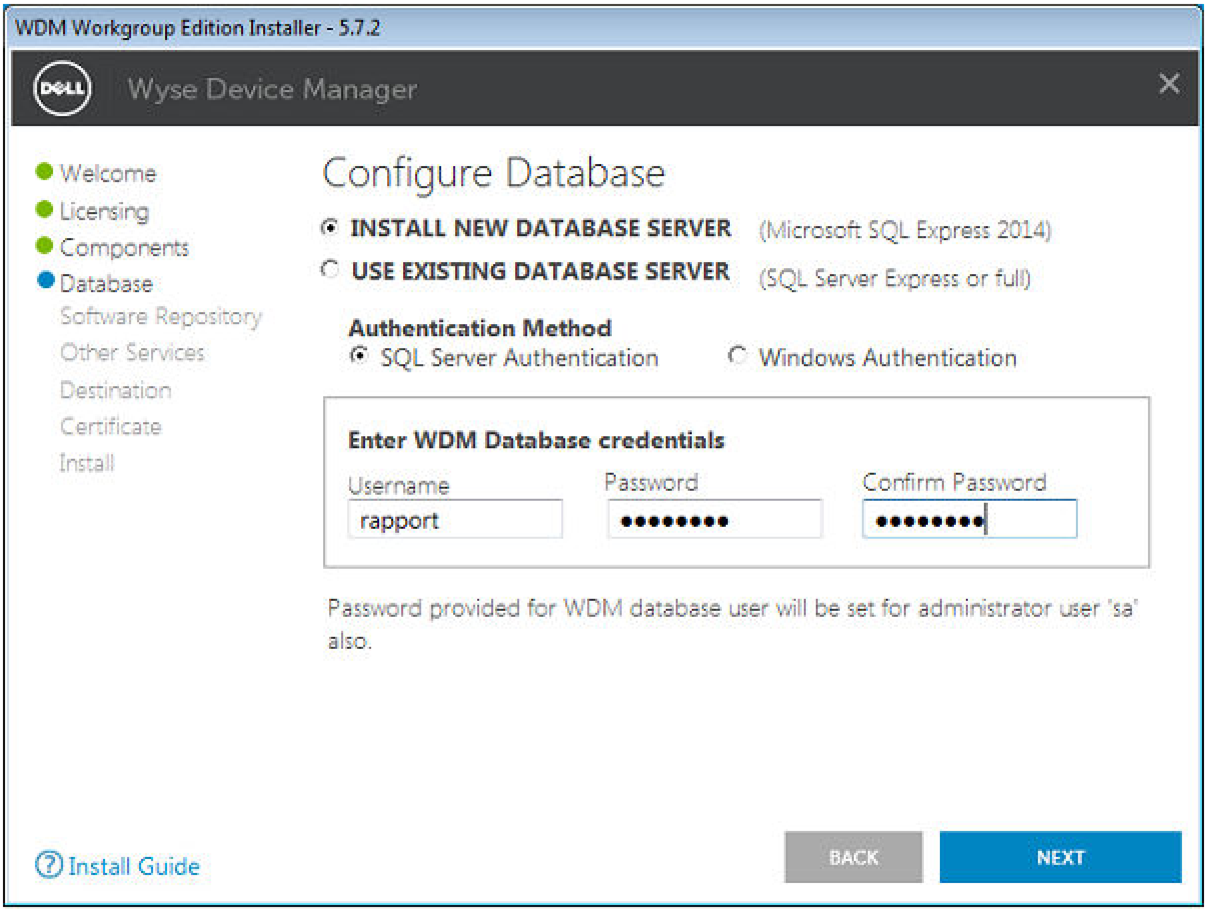
- **Use Existing Database Server (SQL Server Express or full)** — Select this option if you have already installed a supported version of Microsoft SQL Server on the system. **Proceed to step 8**. If you select this option, make sure that the existing database server is on the same system where you are installing WDM Workgroup edition.

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. Enter **Username**, **Password** , and **Confirm Password**. The default username is **rapport**.

   NOTE: Password must match complexity rules of underlying Windows OS.



Configure Database

● INSTALL NEW DATABASE SERVER (Microsoft SQL Express 2014)

○ USE EXISTING DATABASE SERVER (SQL Server Express or full)

Authentication Method

● SQL Server Authentication ○ Windows Authentication

Enter WDM Database credentials

Username: rapport

Password: •••••••••

Confirm Password: •••••••••

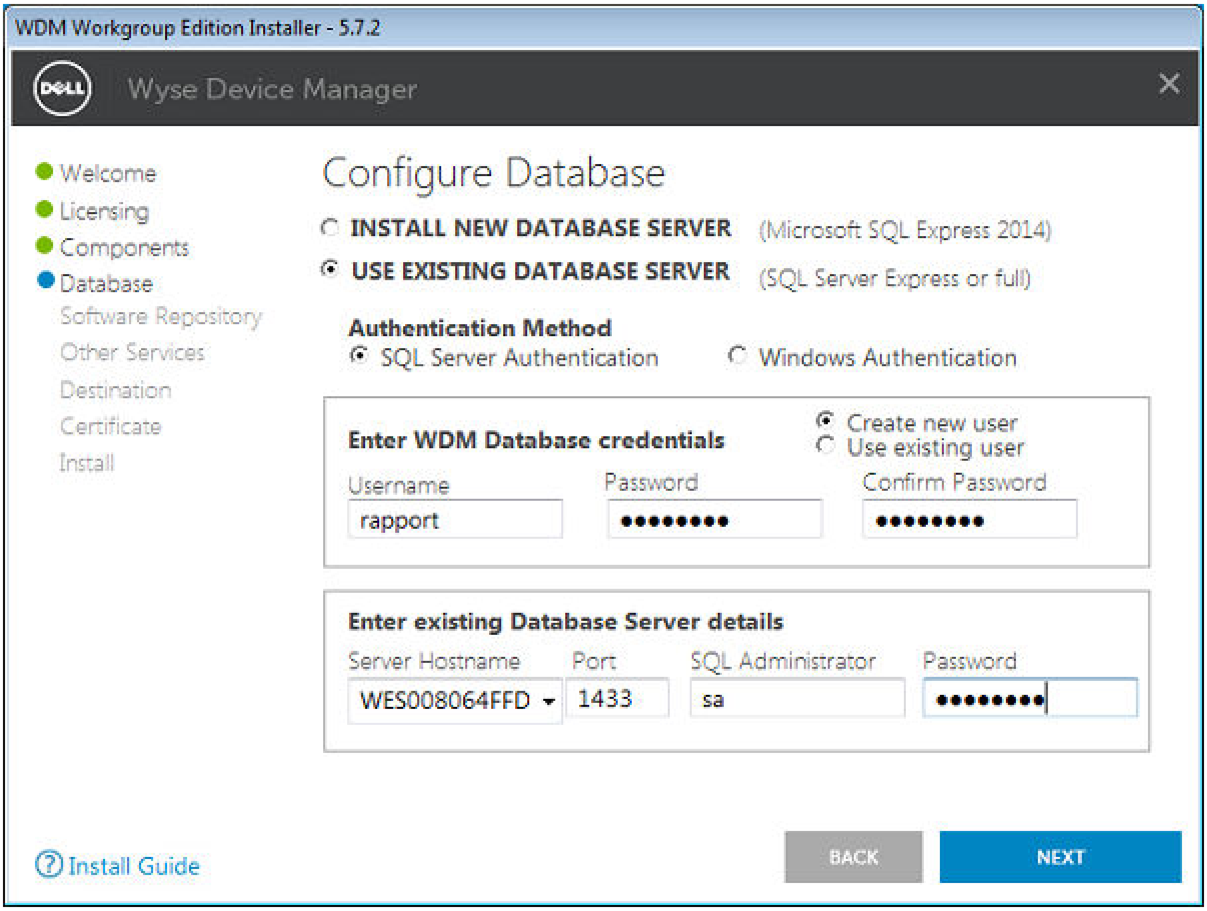
Password provided for WDM database user will be set for administrator user 'sa' also.

Figure 5. New Database Configuration

8. If you have selected the second option in step 6, then provide the following details:

a. Enter **Server Hostname**, **Port**, **Username**, and **Password**. Port number is entered by default and the port number is 1433

NOTE: Password must match complexity rules of underlying Windows OS.


WDM Workgroup Edition Installer - 5.7.2

Wyse Device Manager

Configure Database

○ INSTALL NEW DATABASE SERVER (Microsoft SQL Express 2014)

● USE EXISTING DATABASE SERVER (SQL Server Express or full)

Authentication Method

● SQL Server Authentication ○ Windows Authentication

Enter WDM Database credentials

● Create new user
○ Use existing user

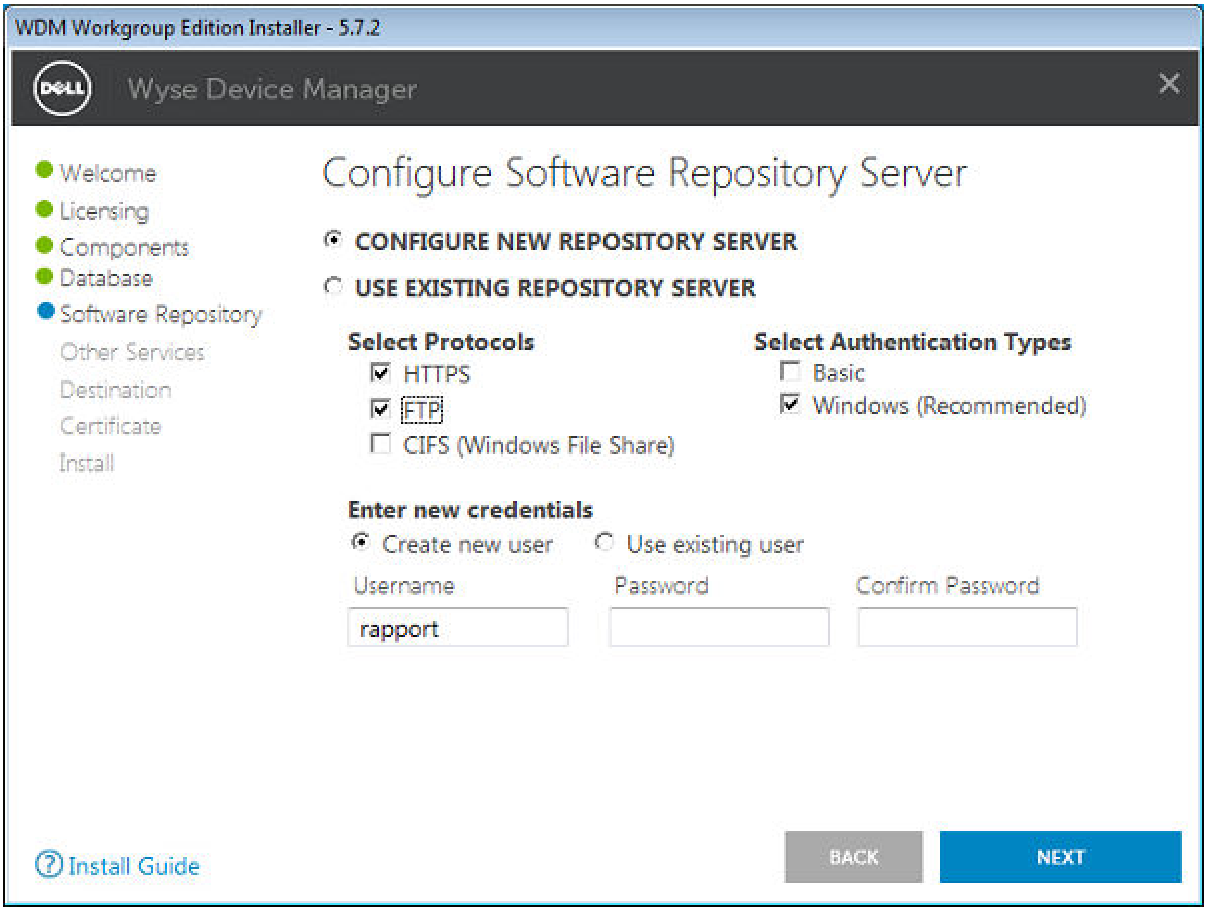
Username: rapport
Password: ••••••••
Confirm Password: ••••••••

Enter existing Database Server details

Server Hostname: WES008064FFD
Port: 1433
SQL Administrator: sa
Password: •••••••••

Figure 6. Existing Database Configuration

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



Configure Software Repository Server

● CONFIGURE NEW REPOSITORY SERVER

○ USE EXISTING REPOSITORY SERVER

Select Protocols

☑ HTTPS

☑ FTP

□ CIFS (Windows File Share)

Select Authentication Types

□ Basic

☑ Windows (Recommended)

Enter new credentials

● Create new user ○ Use existing user

Username: rapport

Password:

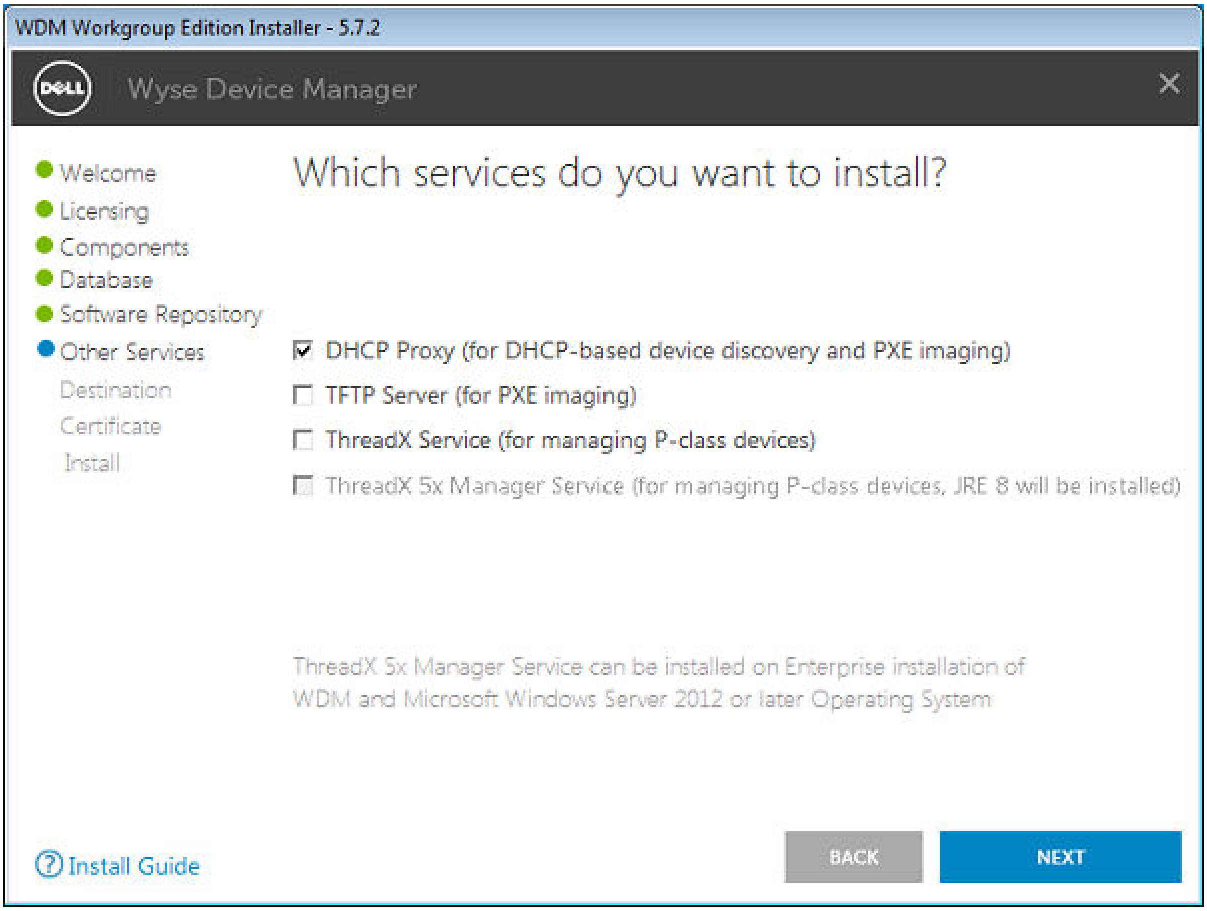
Confirm Password:

Figure 7. Configure Software Repository Server Screen

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** for ThreadX 4.x and **CIFS** for ThreadX 5.x.
    d. **Authentication Type** — Windows is selected by default. You can also select Basic.

       NOTE: Basic authentication is required for Linux.
    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.

       NOTE: Password must match complexity rules of underlying Windows OS.
    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**.



WDM Workgroup Edition Installer - 5.7.2

Wyse Device Manager

- ● Welcome
- ● Licensing
- ● Components
- ● Database
- ● Software Repository
- ● Other Services
- Destination
- Certificate
- Install

Which services do you want to install?

☑ DHCP Proxy (for DHCP-based device discovery and PXE imaging)

□ TFTP Server (for PXE imaging)

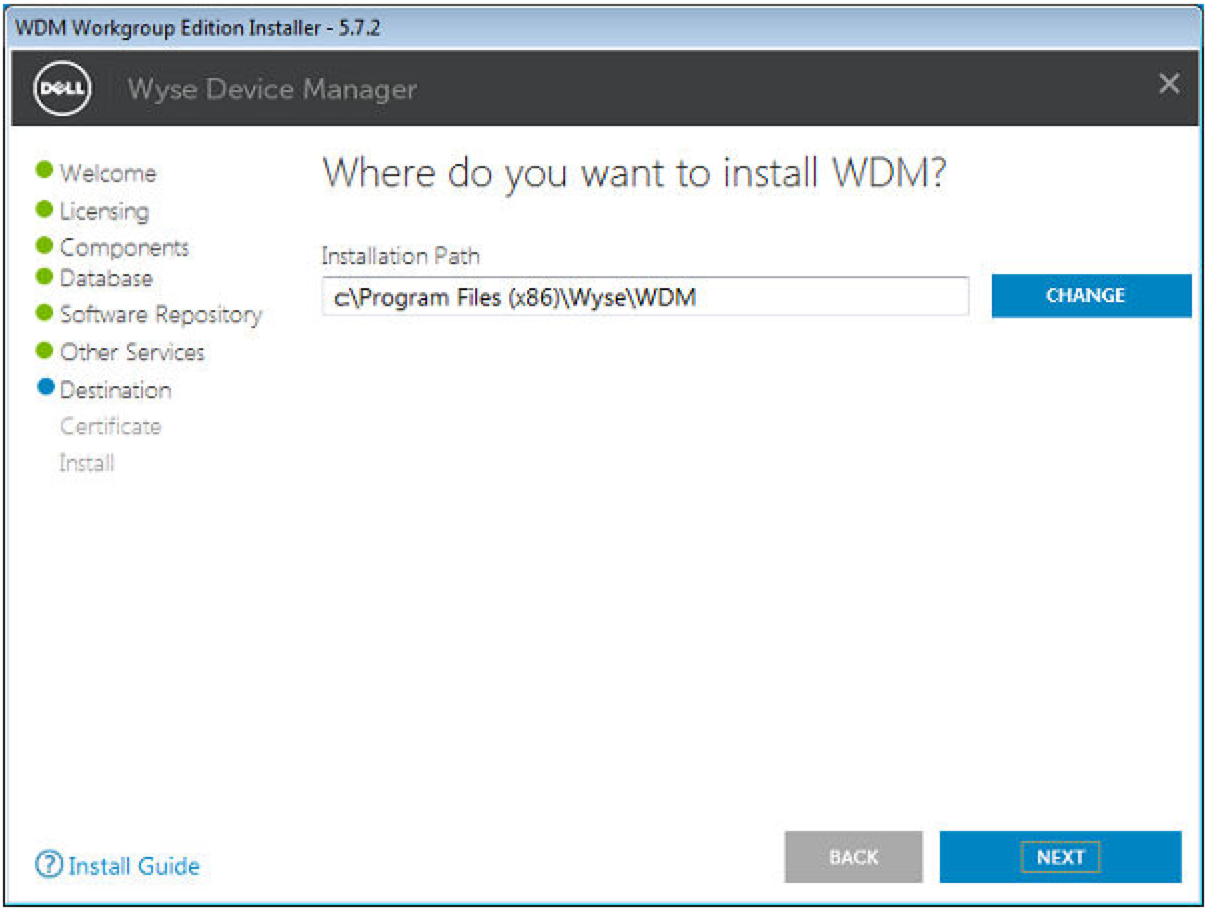
□ ThreadX Service (for managing P-class devices)

□ ThreadX 5x Manager Service (for managing P-class devices, JRE 8 will be installed)

ThreadX 5x Manager Service can be installed on Enterprise installation of WDM and Microsoft Windows Server 2012 or later Operating System

Figure 8. Other Services Screen

13. Provide the installation path and click **Next**.



WDM Workgroup Edition Installer - 5.7.2

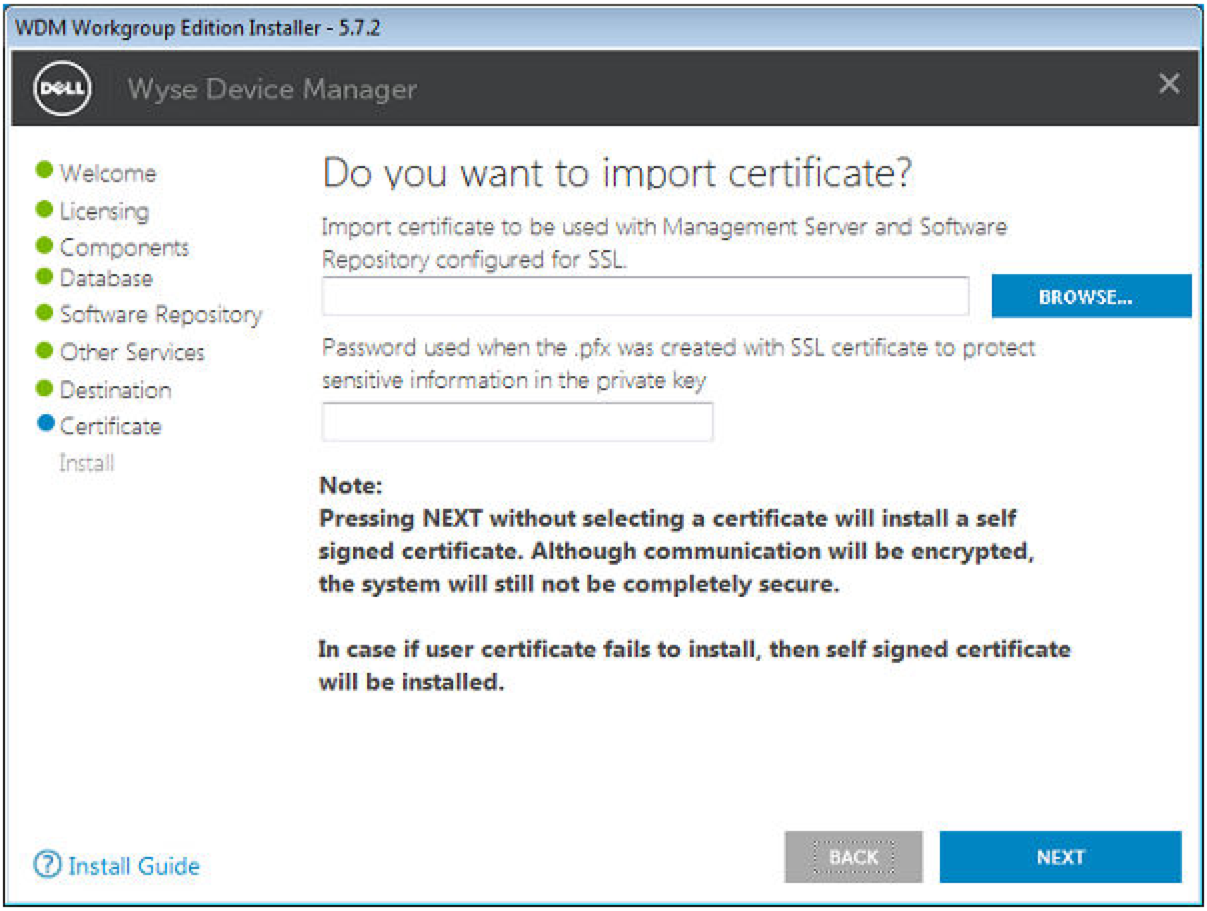
Where do you want to install WDM?

Installation Path: c\Program Files (x86)\Wyse\WDM

Figure 9. Destination Screen

14. Select the certificate and import the same to start the installation.

NOTE: If you click the NEXT without selecting a certificate, the installer installs a self signed certificate. The communications are encrypted, still the system is not completely secure. The certificate must be in the format of .pfx file.



Do you want to import certificate?

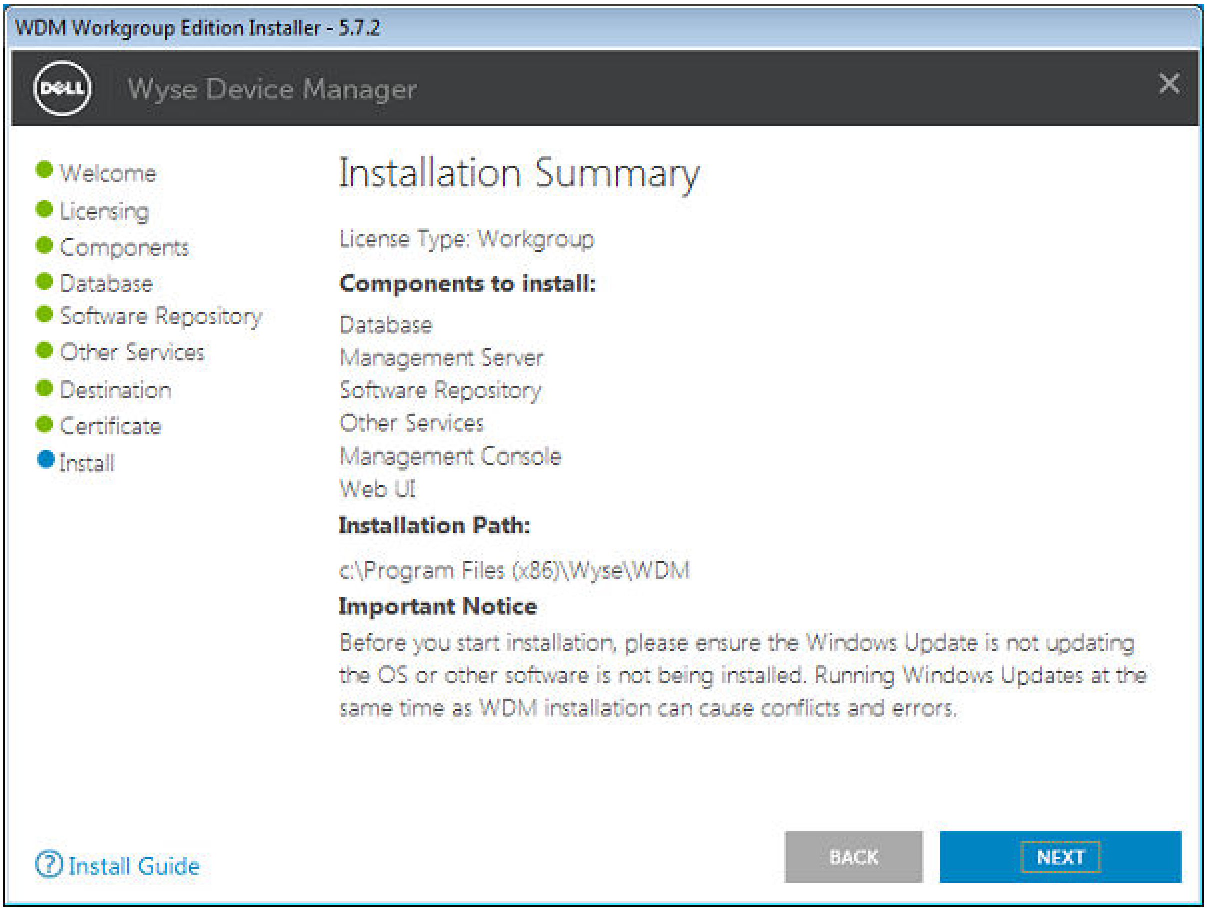
Import certificate to be used with Management Server and Software Repository configured for SSL.

Password used when the .pfx was created with SSL certificate to protect sensitive information in the private key

Note:
Pressing NEXT without selecting a certificate will install a self signed certificate. Although communication will be encrypted, the system will still not be completely secure.

In case if user certificate fails to install, then self signed certificate will be installed.

Figure 10. Certificate Screen


WDM Workgroup Edition Installer - 5.7.2

Installation Summary

License Type: Workgroup

Components to install:

Database
Management Server
Software Repository
Other Services
Management Console
Web UI

Installation Path:

c:\Program Files (x86)\Wyse\WDM

Important Notice

Before you start installation, please ensure the Windows Update is not updating the OS or other software is not being installed. Running Windows Updates at the same time as WDM installation can cause conflicts and errors.

Figure 11. Installation Summary Screen

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.

After installation, ensure that you will meet the following checklists:

- Rapport folder should get created after installing WDM in **C:\Inetpub\ftproot path**.
- WyseDeviceManager 5.7.2 WebUI icon will be created in the Desktop.
- In IIS , HApi Application should be created under Rapport HTTP Server.
- In IIS , MyWDM Application should be created under Rapport HTTP Server.
- In IIS , WebUI Application should be created under Rapport HTTP Server.

GUID-0A61209C-364F-43B4-AFCE-E615CF072D80

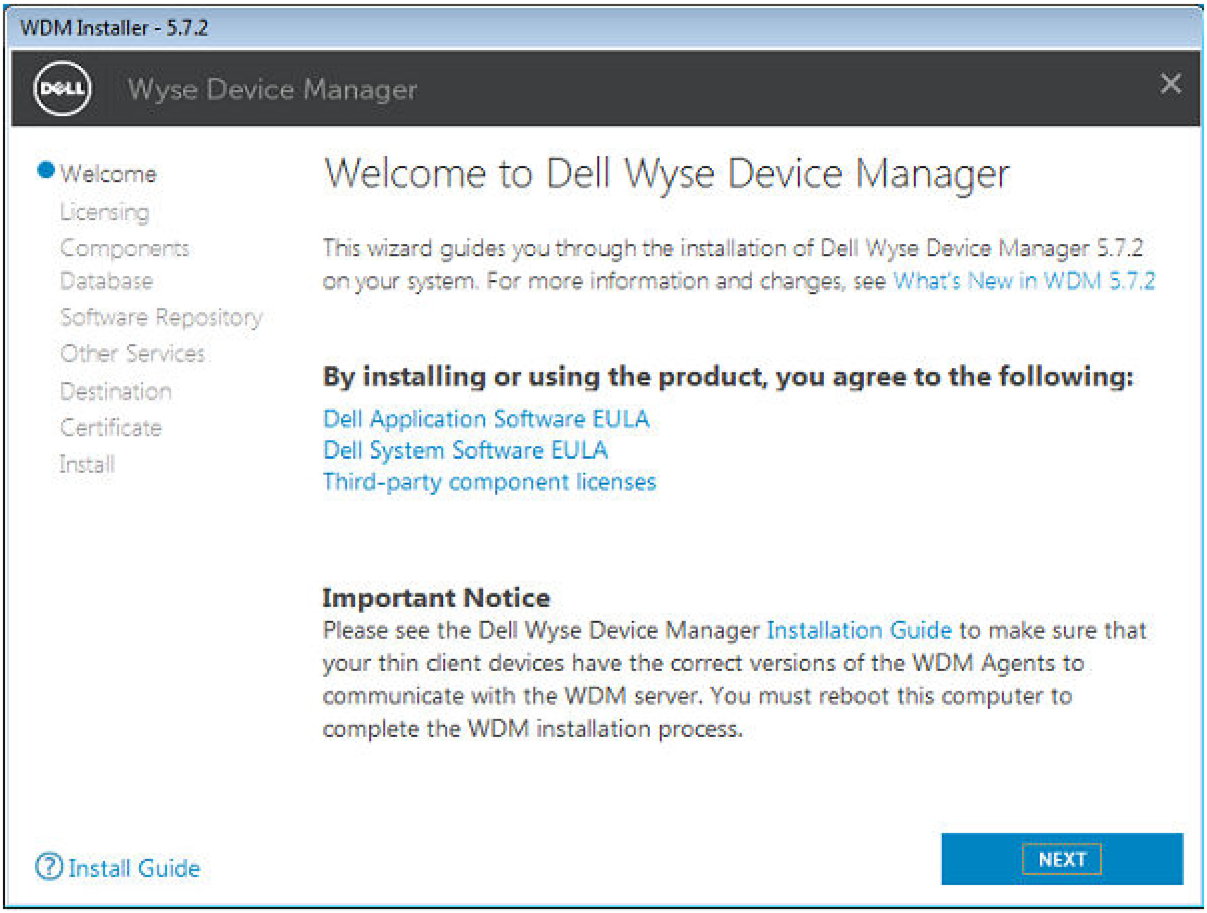
Installing the WDM Enterprise Edition

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.

   If the server does not have .Net framework, then the .Net framework is installed automatically.

   The Welcome screen is displayed.



Welcome to Dell Wyse Device Manager

This wizard guides you through the installation of Dell Wyse Device Manager 5.7.2 on your system. For more information and changes, see What's New in WDM 5.7.2

By installing or using the product, you agree to the following:

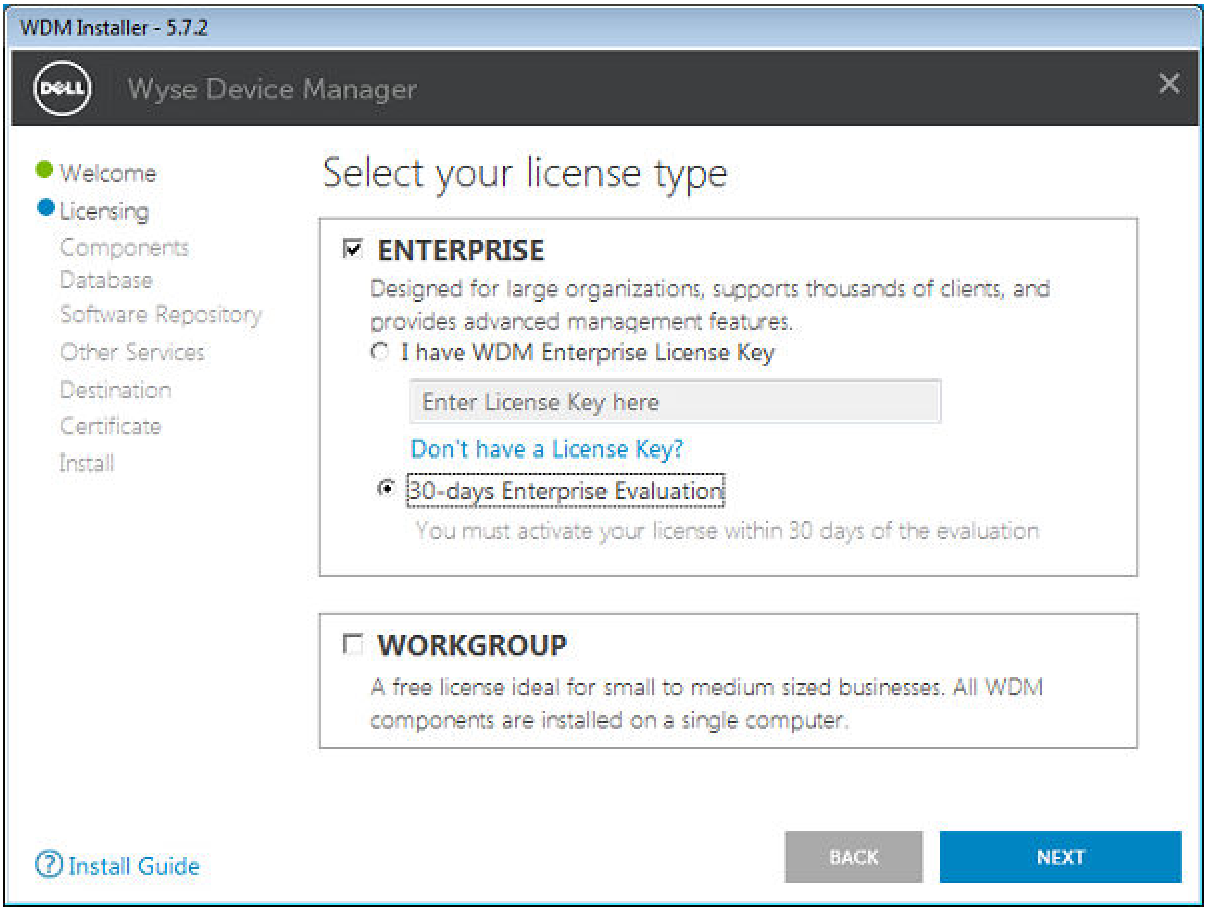
Dell Application Software EULA
Dell System Software EULA
Third-party component licenses

Important Notice

Please see the Dell Wyse Device Manager Installation Guide to make sure that your thin client devices have the correct versions of the WDM Agents to communicate with the WDM server. You must reboot this computer to complete the WDM installation process.

Figure 12. WDM Installer 5.7.2 Screen

3. Click **Next**.
4. Select **Enterprise** as the **License Type**.



Select your license type

☑ **ENTERPRISE**

Designed for large organizations, supports thousands of clients, and provides advanced management features.

○ I have WDM Enterprise License Key

Enter License Key here

Don't have a License Key?

● 30-days Enterprise Evaluation

You must activate your license within 30 days of the evaluation

□ **WORKGROUP**

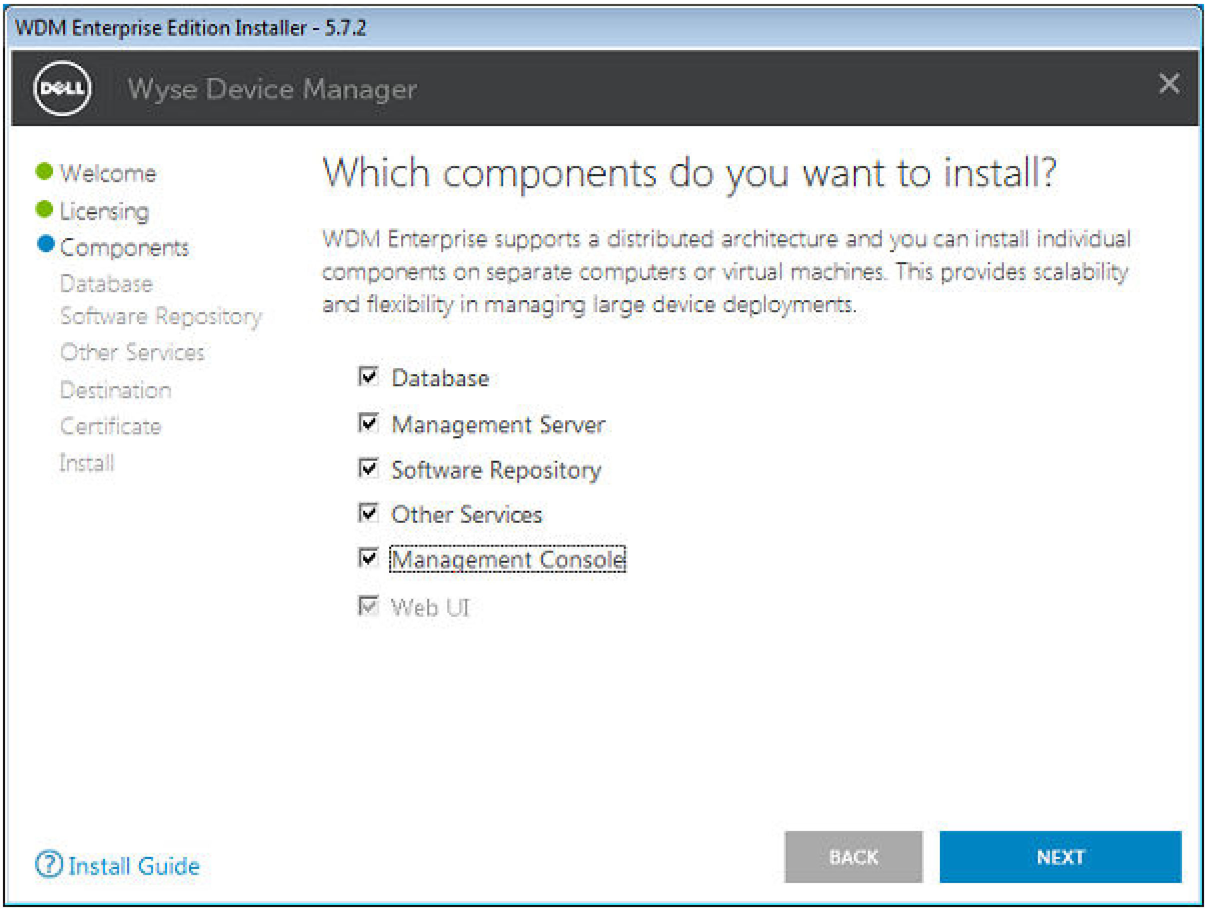
A free license ideal for small to medium sized businesses. All WDM components are installed on a single computer.

Figure 13. License Screen

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**.



WDM Enterprise Edition Installer - 5.7.2

Wyse Device Manager

Which components do you want to install?

WDM Enterprise supports a distributed architecture and you can install individual components on separate computers or virtual machines. This provides scalability and flexibility in managing large device deployments.

☑ Database

☑ Management Server

☑ Software Repository

☑ Other Services

☑ Management Console

☑ Web UI

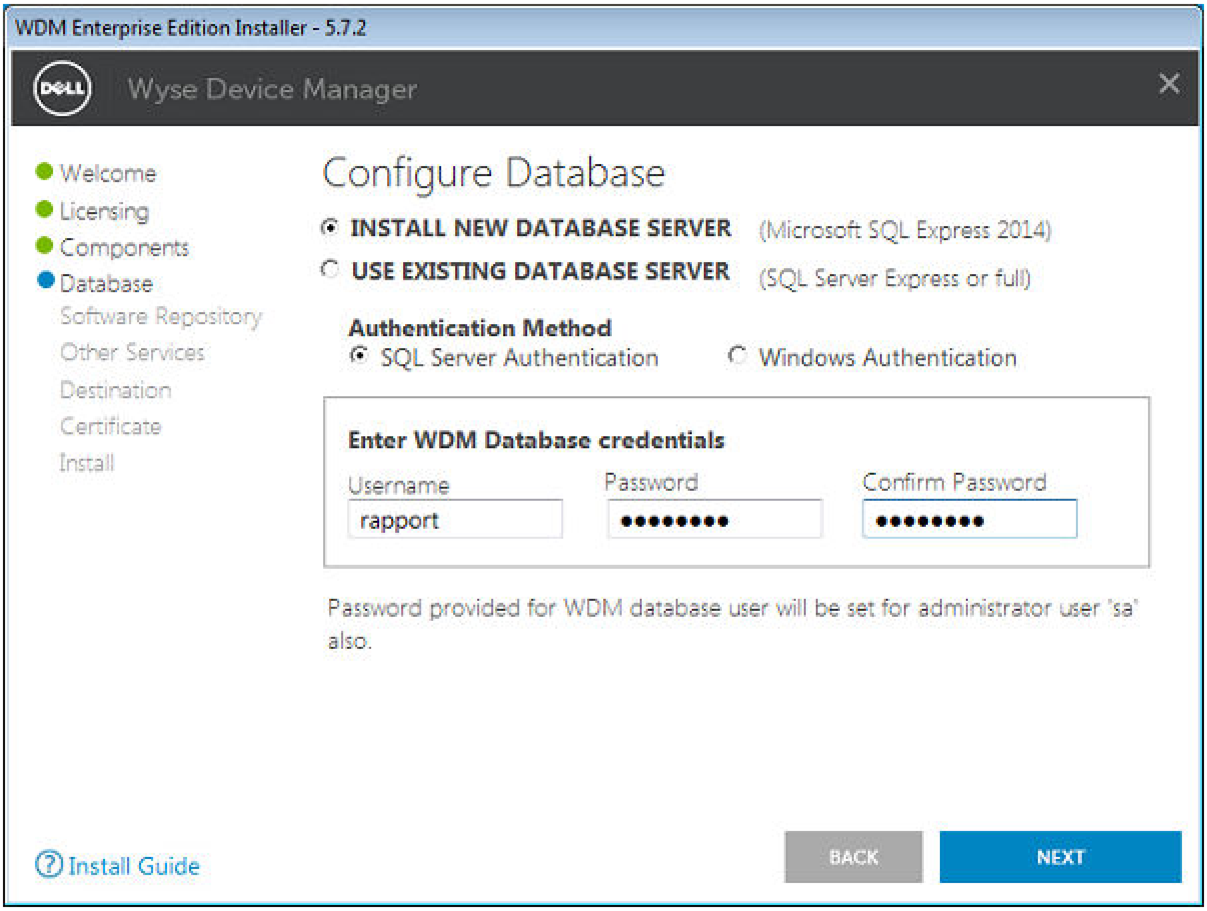
Figure 14. Component Screen

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 2014)** — Select this option if you do not have any supported version of Microsoft SQL Server installed on the system. **Proceed to step 8**.


WDM Enterprise Edition Installer - 5.7.2

Wyse Device Manager

Configure Database

● INSTALL NEW DATABASE SERVER (Microsoft SQL Express 2014)

○ USE EXISTING DATABASE SERVER (SQL Server Express or full)

Authentication Method

● SQL Server Authentication ○ Windows Authentication

Enter WDM Database credentials

Username: rapport

Password: ●●●●●●●●●

Confirm Password: ●●●●●●●●●

Password provided for WDM database user will be set for administrator user 'sa' also.

Figure 15. New Database Screen

- **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**.

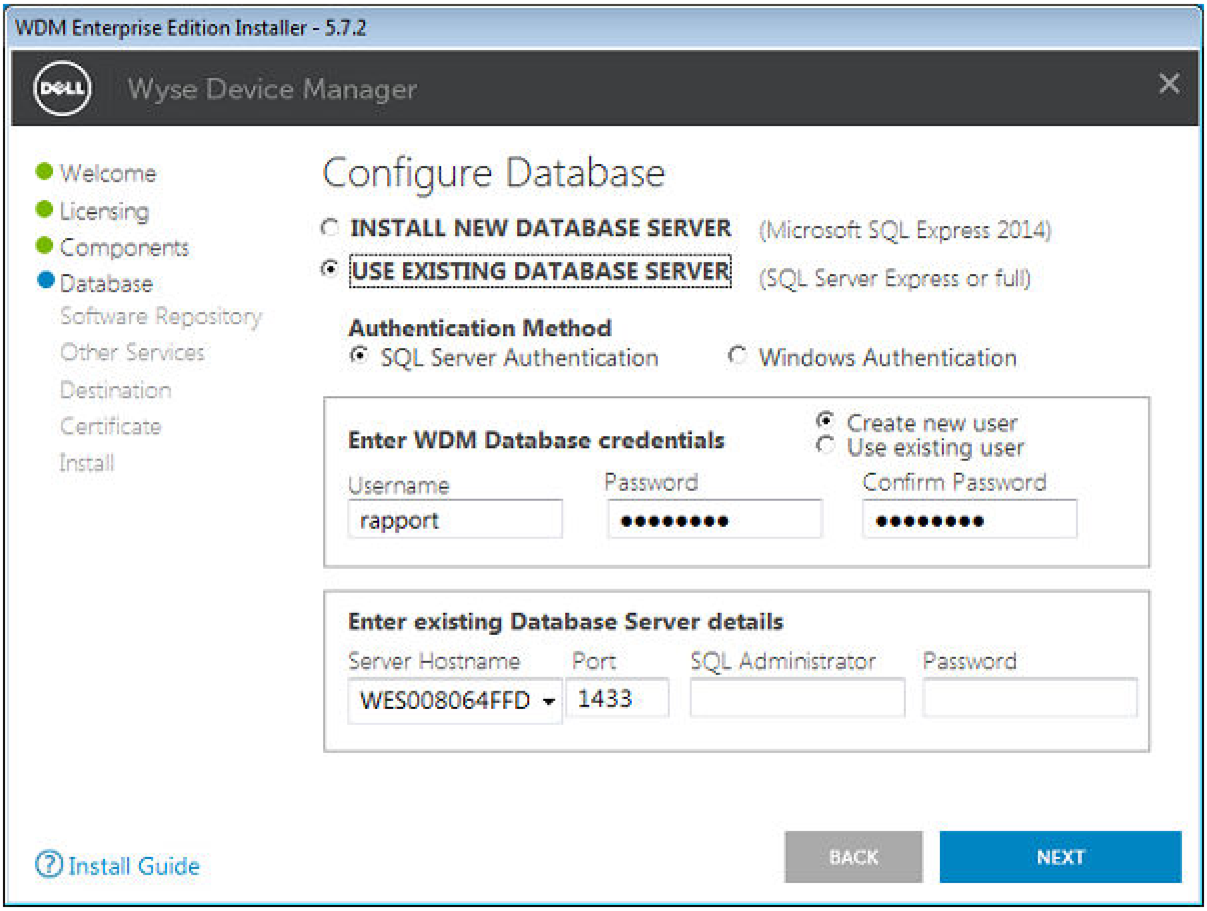
8. Provide the **RapportDB** database credentials. RapportDB is the WDM database instance that is created on SQL Server.

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. 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. Enter **Username**, **Password**, and **Confirm Password**. The default username is **rapport**.

NOTE: Password must match complexity rules of underlying Windows OS.



Configure Database

○ INSTALL NEW DATABASE SERVER (Microsoft SQL Express 2014)

● USE EXISTING DATABASE SERVER (SQL Server Express or full)

Authentication Method

● SQL Server Authentication ○ Windows Authentication

Enter WDM Database credentials

● Create new user
○ Use existing user

Username: rapport
Password: ●●●●●●●●●
Confirm Password: ●●●●●●●●●

Enter existing Database Server details

Server Hostname: WES008064FFD
Port: 1433
SQL Administrator:
Password:

Figure 16. Existing Database Screen

9. If you have selected the second option in **step 7**, then provide the following details:

a. **Server** — Provide the hostname of the system on which you have installed Microsoft SQL Server.

b. **Port** — This is entered by default and the port number is 1433.

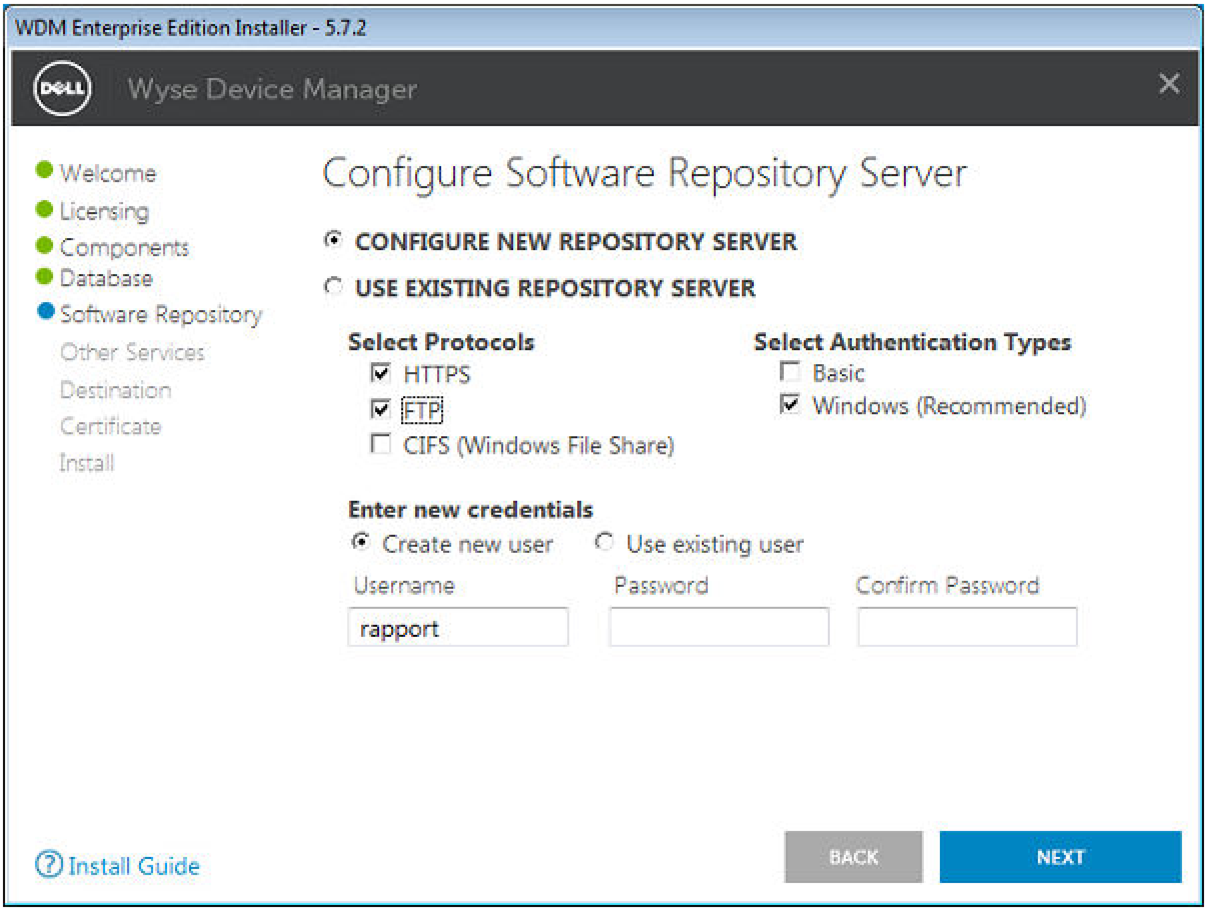
NOTE: You can add five digit custom port for TCP/UDP in the range of 49152 to 65535.

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.



Configure Software Repository Server

● CONFIGURE NEW REPOSITORY SERVER

○ USE EXISTING REPOSITORY SERVER

Select Protocols

☑ HTTPS

☑ FTP

☐ CIFS (Windows File Share)

Select Authentication Types

☐ Basic

☑ Windows (Recommended)

Enter new credentials

● Create new user ○ Use existing user

Username	Password	Confirm Password
rapport		

Figure 17. New Software Repository Screen

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** for ThreadX 4.x and **CIFS** for ThreadX 5.x.

d. **Authentication Type** — Windows is selected by default. You can also select Basic.

NOTE: Basic authentication is required for Linux.

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.

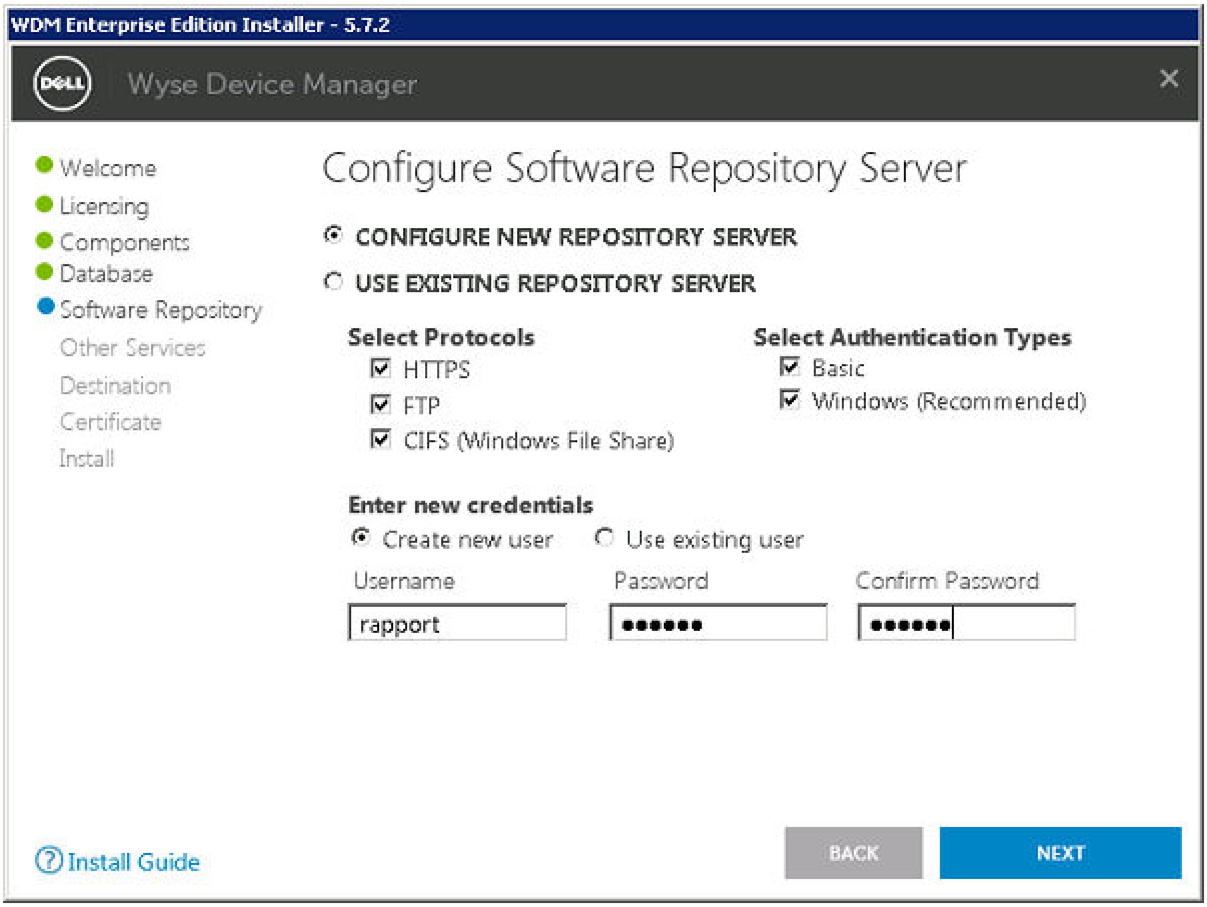
f. **Password** — Enter the password to access the repository.

NOTE: Password must match complexity rules of underlying Windows OS.

g. **Confirm Password** — If you are creating a new user, enter the password again.

12. 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.



Configure Software Repository Server

● CONFIGURE NEW REPOSITORY SERVER

○ USE EXISTING REPOSITORY SERVER

Select Protocols

☑ HTTPS

☑ FTP

☑ CIFS (Windows File Share)

Select Authentication Types

☑ Basic

☑ Windows (Recommended)

Enter new credentials

● Create new user ○ Use existing user

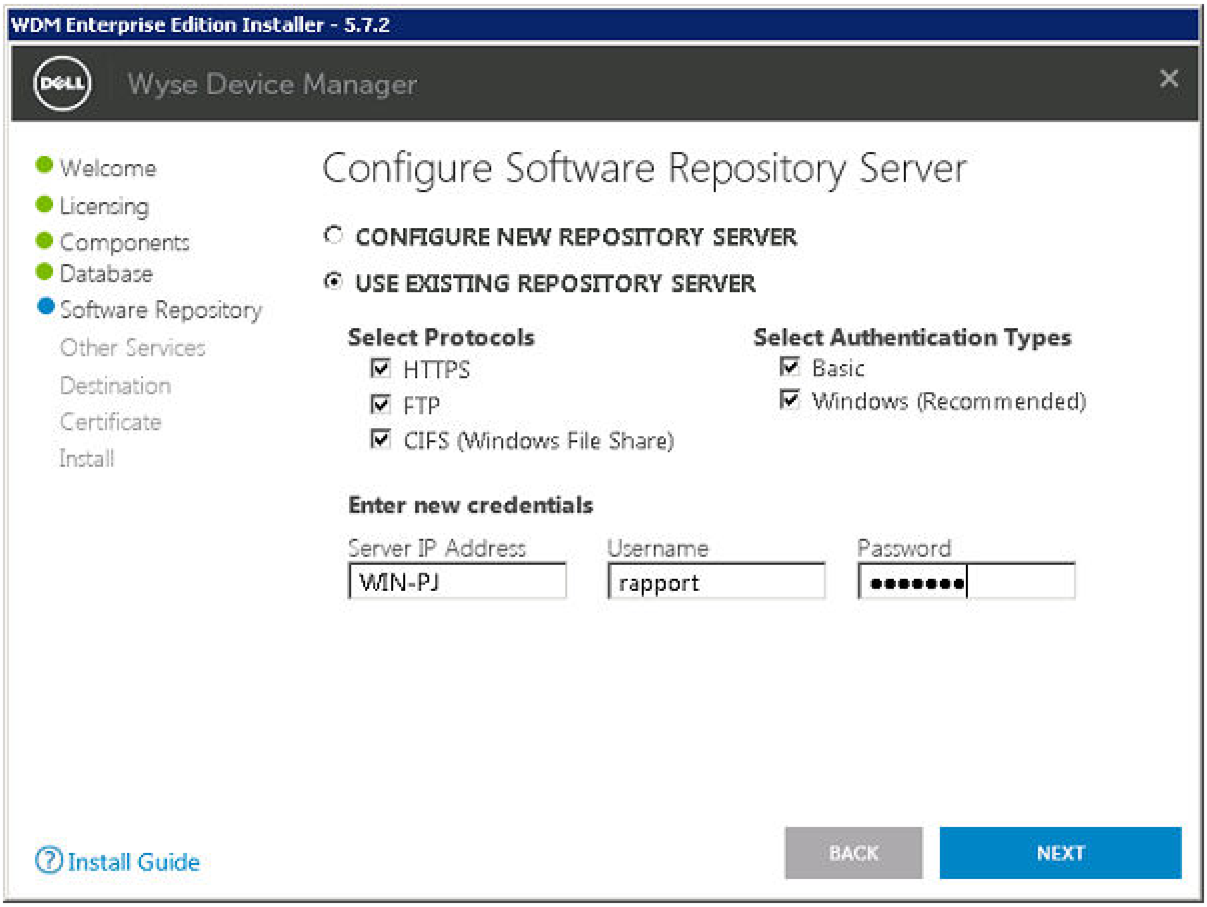
Username: rapport

Password: ●●●●●●

Confirm Password: ●●●●●●

Figure 18. New Software Repository Protocol Screen

b. **Use Existing Repository Server** — select this option if you have already configured the Repository Server.



WDM Enterprise Edition Installer - 5.7.2

Wyse Device Manager

Configure Software Repository Server

○ CONFIGURE NEW REPOSITORY SERVER

● USE EXISTING REPOSITORY SERVER

Select Protocols

☑ HTTPS

☑ FTP

☑ CIFS (Windows File Share)

Select Authentication Types

☑ Basic

☑ Windows (Recommended)

Enter new credentials

Server IP Address: WIN-PJ

Username: rapport

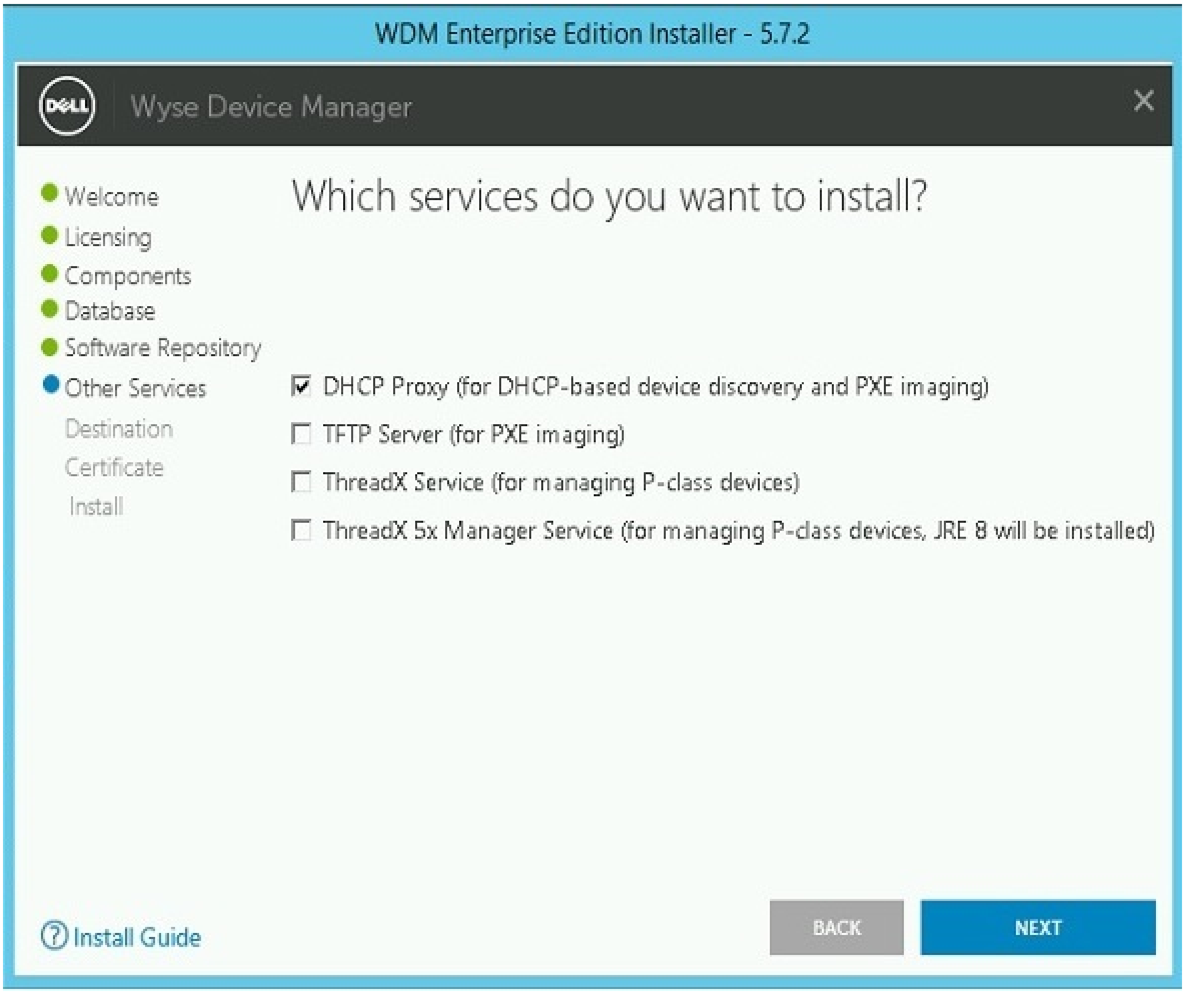
Password: •••••••

Figure 19. Existing Software Repository Screen

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.

13. Click **Next** to install the other services.

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


WDM Enterprise Edition Installer - 5.7.2

Wyse Device Manager

Which services do you want to install?

☑ DHCP Proxy (for DHCP-based device discovery and PXE imaging)

□ TFTP Server (for PXE imaging)

□ ThreadX Service (for managing P-class devices)

□ ThreadX 5x Manager Service (for managing P-class devices, JRE 8 will be installed)

Figure 20. Other Services Screen

NOTE:

- ThreadX 5.0 is supported on the operating system Windows Server 2012 and Windows Server 2012 R2 and above.

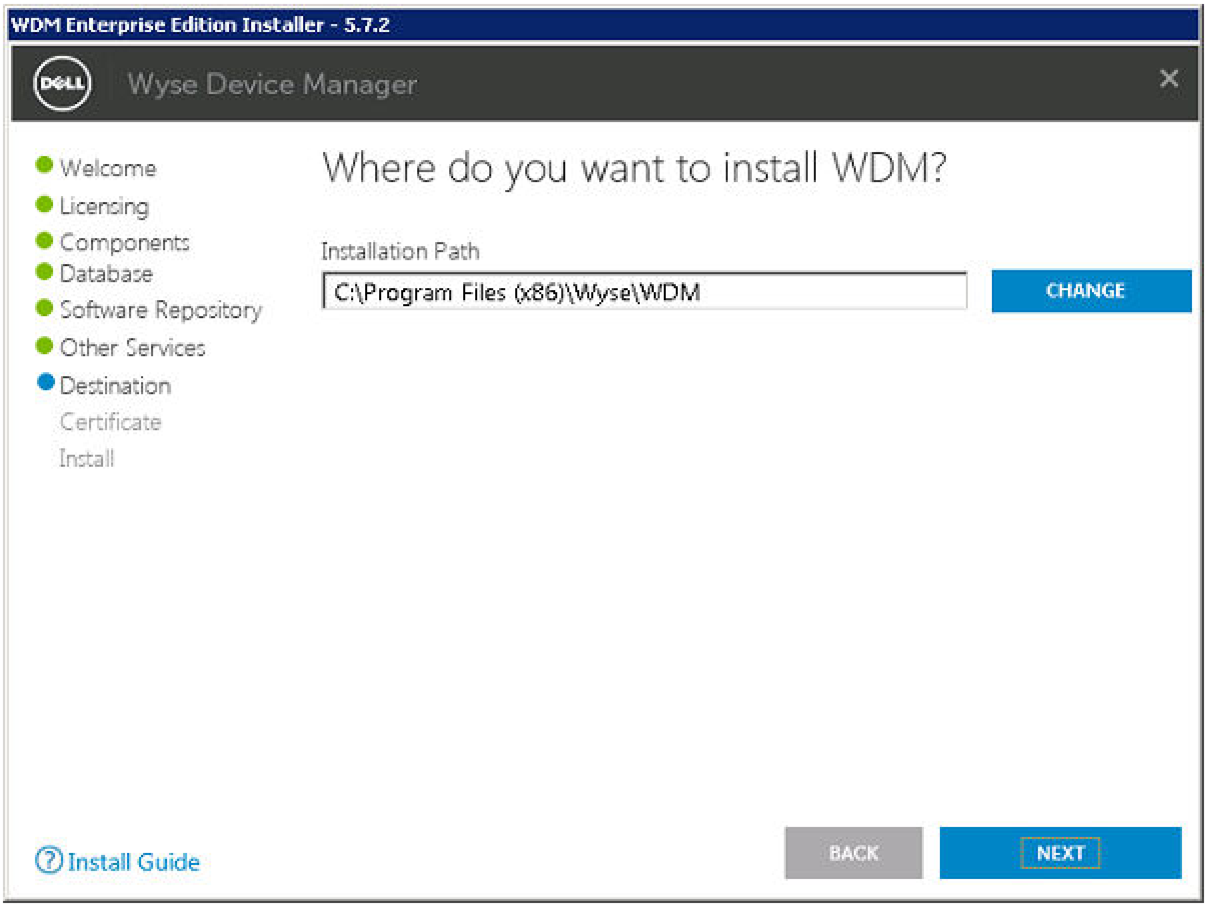
NOTE: Dell recommends you to install all the four services during WDM installation itself. If the WDM installation is completed with only one service installed, then it is not possible to install the remaining services. You must uninstall and then re-install WDM by selecting the remaining services.

NOTE:

- Select DHCP Proxy, to install the services for DHCP-based device discovery and PXE imaging.
- Select TFTP Server, to install the services for PXE imaging.
- Select ThreadX Service, to install the services for managing ThreadX (P- class) devices.
- Select ThreadX 5.x Manager Service, to manage P-class services and to install JRE 8.

15. Provide the installation path and click **Next**.

The Destination screen is displayed.



WDM Enterprise Edition Installer - 5.7.2

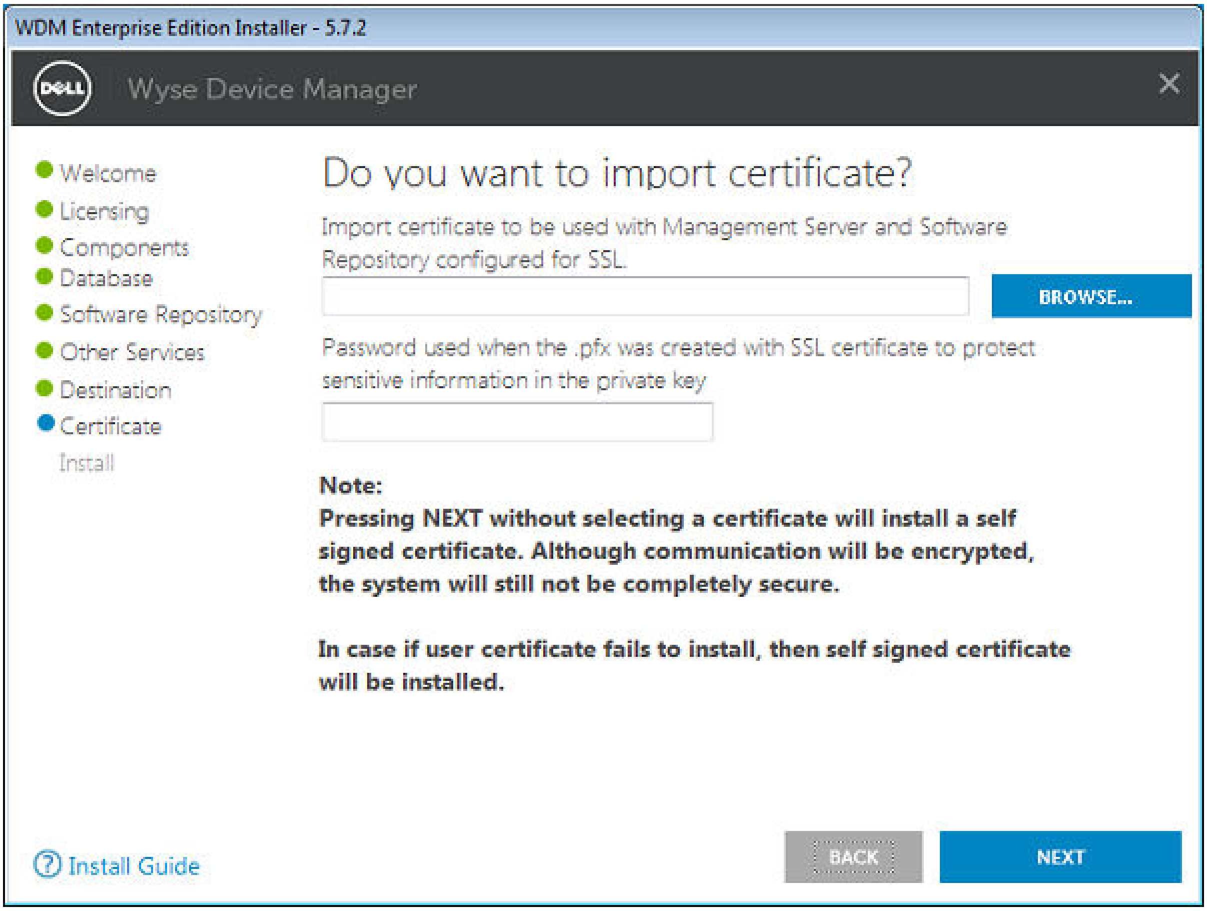
Where do you want to install WDM?

Installation Path: C:\Program Files (x86)\Wyse\WDM

Figure 21. Destination Screen

16. Select the certificate and import the same to start the installation.

NOTE: If you click the NEXT without selecting a certificate, the installer installs a self signed certificate. The communications are encrypted, still the system is not completely secure. The certificate must be in the format of .pfx file.



Do you want to import certificate?

Import certificate to be used with Management Server and Software Repository configured for SSL.

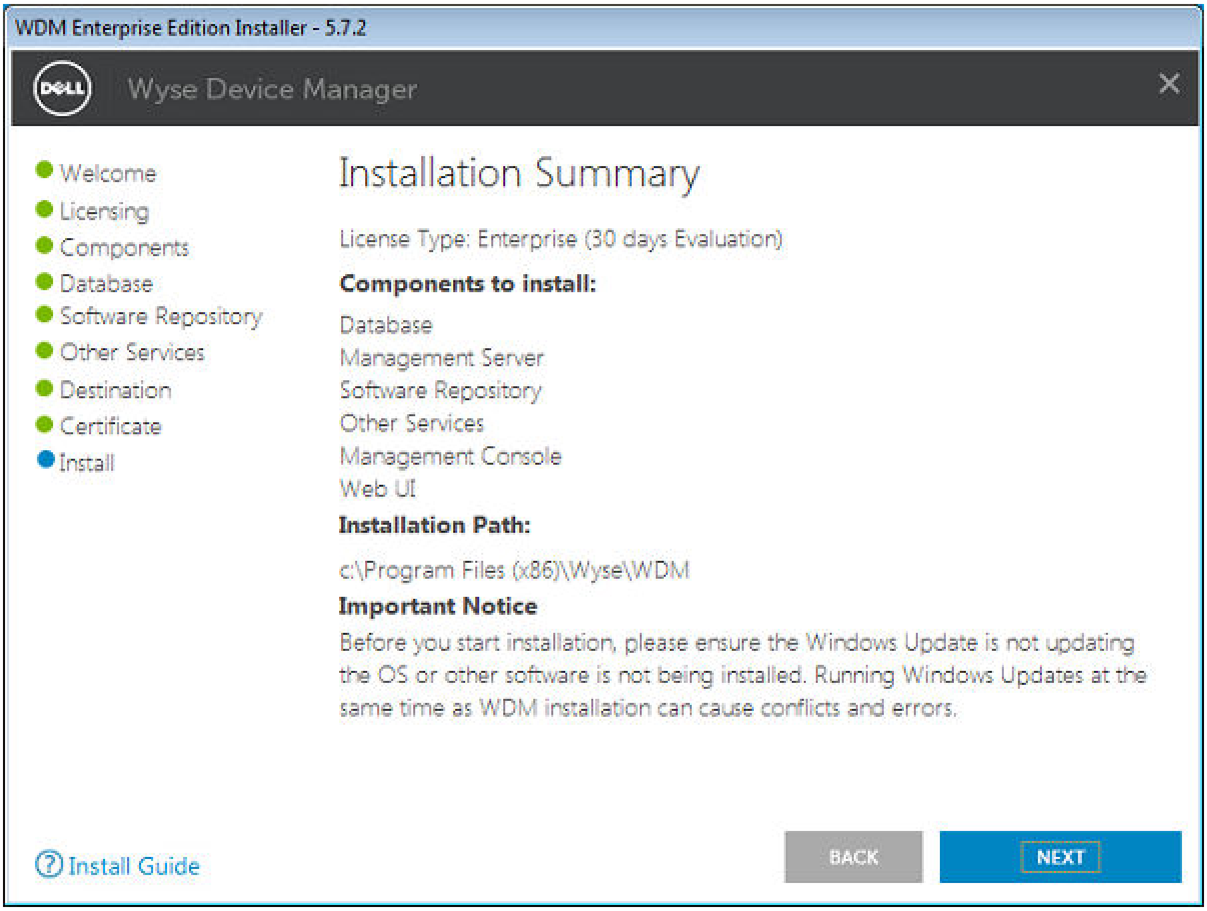
Password used when the .pfx was created with SSL certificate to protect sensitive information in the private key

Note:
Pressing NEXT without selecting a certificate will install a self signed certificate. Although communication will be encrypted, the system will still not be completely secure.

In case if user certificate fails to install, then self signed certificate will be installed.

Figure 22. Certificate Screen

17. Click **Next** to begin the installation.


WDM Enterprise Edition Installer - 5.7.2

Wyse Device Manager

Installation Summary

License Type: Enterprise (30 days Evaluation)

Components to install:

Database
Management Server
Software Repository
Other Services
Management Console
Web UI

Installation Path:

c:\Program Files (x86)\Wyse\WDM

Important Notice

Before you start installation, please ensure the Windows Update is not updating the OS or other software is not being installed. Running Windows Updates at the same time as WDM installation can cause conflicts and errors.

Figure 23. Installation Summary

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.

GUID-E1664207-9B43-43B2-AAAC-629B85E8E347

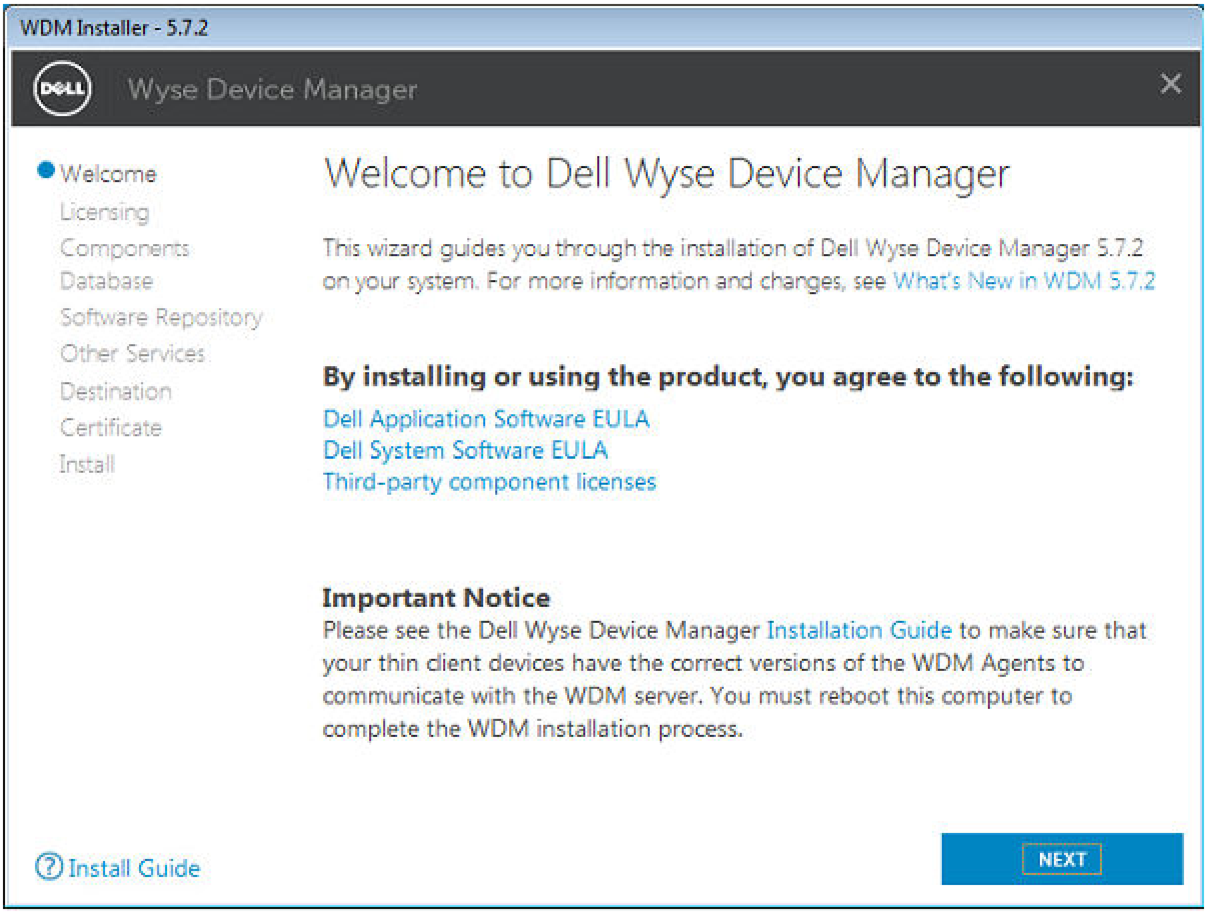
Installing the WDM on Cloud Environment

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.

   If the server does not have .Net framework, then the .Net framework is installed automatically.

   The Welcome screen is displayed.



WDM Installer - 5.7.2

Welcome to Dell Wyse Device Manager

This wizard guides you through the installation of Dell Wyse Device Manager 5.7.2 on your system. For more information and changes, see What's New in WDM 5.7.2

By installing or using the product, you agree to the following:

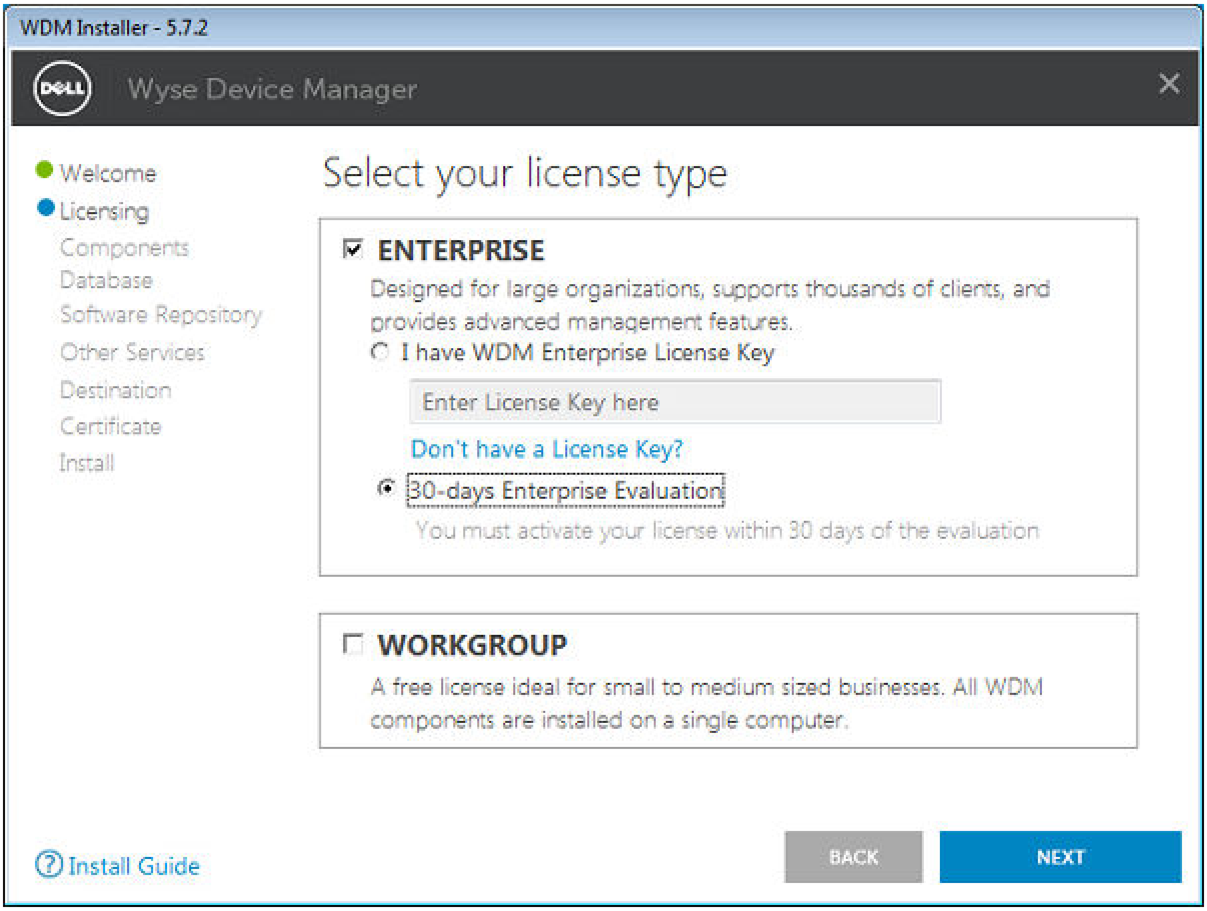
Dell Application Software EULA
Dell System Software EULA
Third-party component licenses

Important Notice

Please see the Dell Wyse Device Manager Installation Guide to make sure that your thin client devices have the correct versions of the WDM Agents to communicate with the WDM server. You must reboot this computer to complete the WDM installation process.

Figure 24. Welcome Screen

3. Click **Next**.
4. Select **Enterprise** as the **License Type**.



Select your license type

☑ **ENTERPRISE**

Designed for large organizations, supports thousands of clients, and provides advanced management features.

○ I have WDM Enterprise License Key

Enter License Key here

Don't have a License Key?

● 30-days Enterprise Evaluation

You must activate your license within 30 days of the evaluation

☐ **WORKGROUP**

A free license ideal for small to medium sized businesses. All WDM components are installed on a single computer.

Figure 25. License Screen

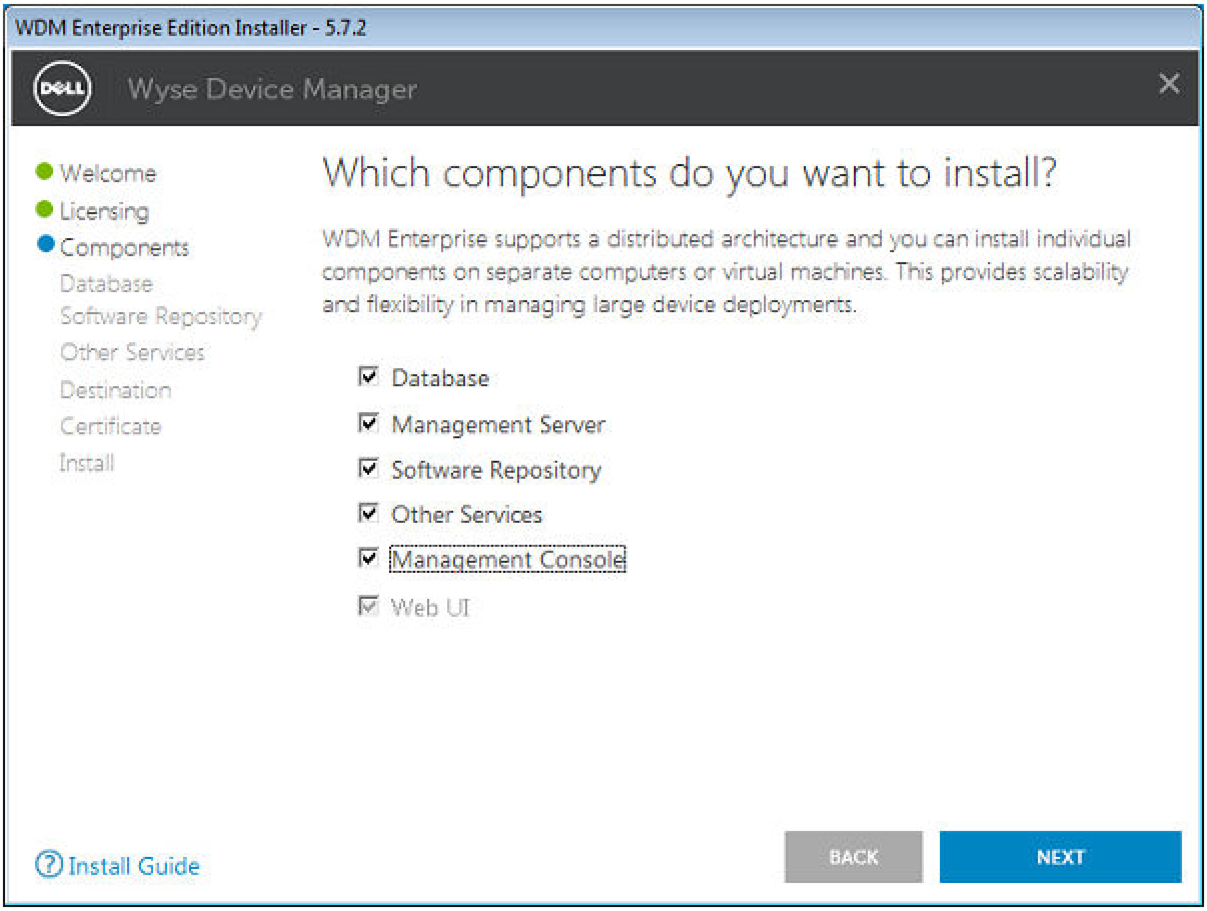
a. If you have the WDM License key, select the **I have WDM Enterprise License Key** option and enter the license key in the space provided.

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**.



Which components do you want to install?

WDM Enterprise supports a distributed architecture and you can install individual components on separate computers or virtual machines. This provides scalability and flexibility in managing large device deployments.

☑ Database

☑ Management Server

☑ Software Repository

☑ Other Services

☑ Management Console

☑ Web UI

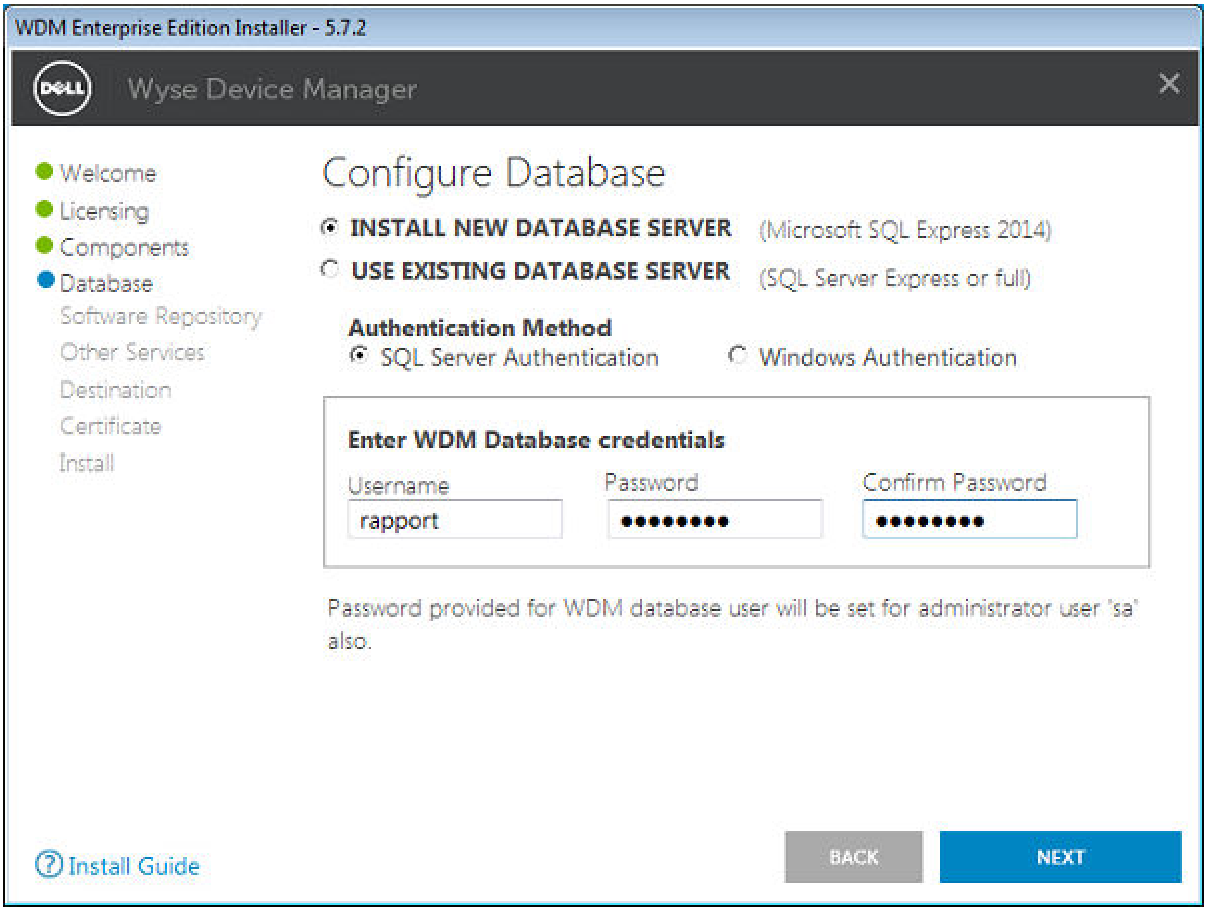
Figure 26. Components Screen

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 2014)** — Select this option if you do not have any supported version of Microsoft SQL Server installed on the system. **Proceed to step 8**.



Configure Database

● INSTALL NEW DATABASE SERVER (Microsoft SQL Express 2014)

○ USE EXISTING DATABASE SERVER (SQL Server Express or full)

Authentication Method

● SQL Server Authentication ○ Windows Authentication

Enter WDM Database credentials

Username	Password	Confirm Password
rapport	●●●●●●●●	●●●●●●●●

Password provided for WDM database user will be set for administrator user 'sa' also.

Figure 27. New Database Server Screen

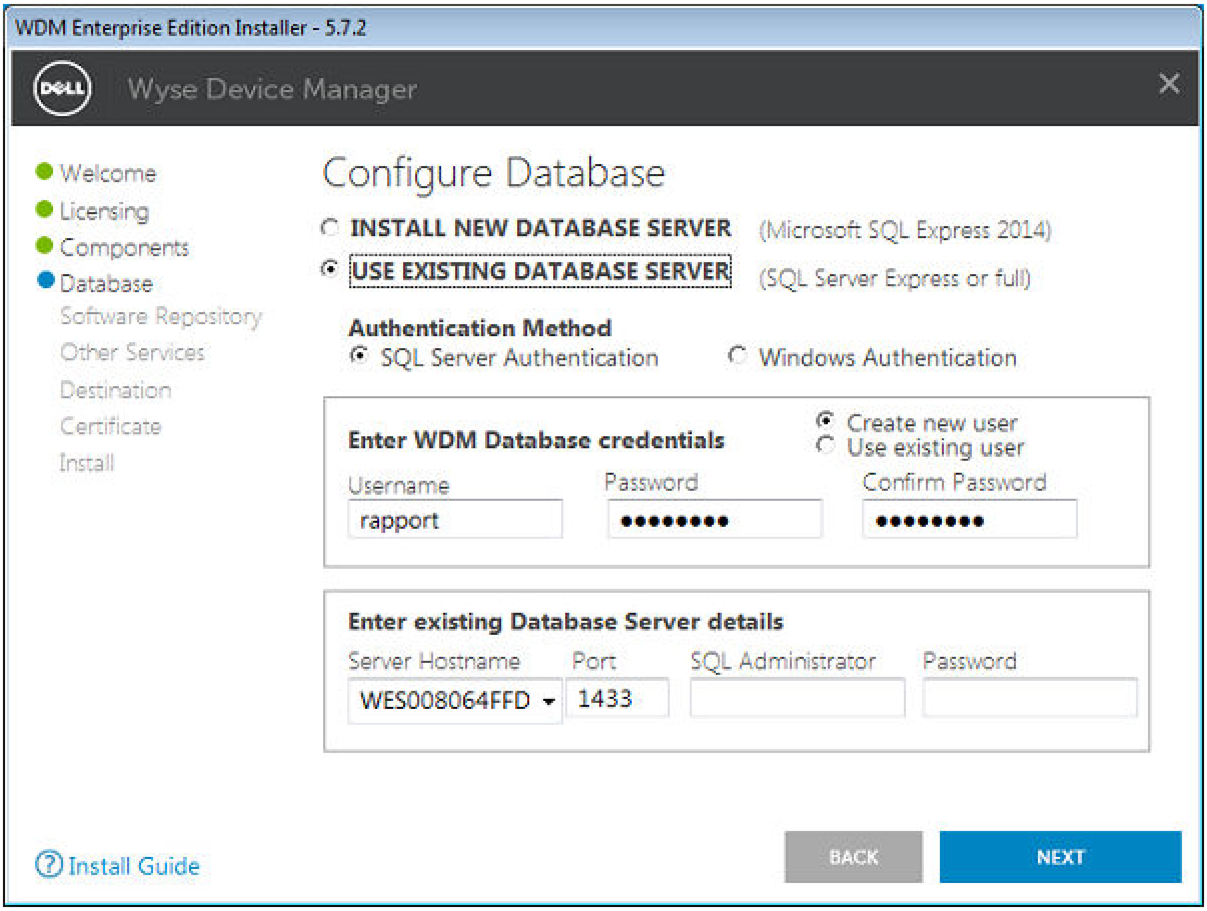
- **Use Existing Database Server (SQL Server Express or full)** — Select this option if you have already installed a supported version of Microsoft SQL Server on the system. **Proceed to step 9**.

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. 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. Enter **Username**, **Password**, and **Confirm Password**. The default username is **rapport**.



Configure Database

○ INSTALL NEW DATABASE SERVER (Microsoft SQL Express 2014)

● USE EXISTING DATABASE SERVER (SQL Server Express or full)

Authentication Method

● SQL Server Authentication ○ Windows Authentication

Enter WDM Database credentials

● Create new user
○ Use existing user

Username	Password	Confirm Password
rapport	●●●●●●●●	●●●●●●●●

Enter existing Database Server details

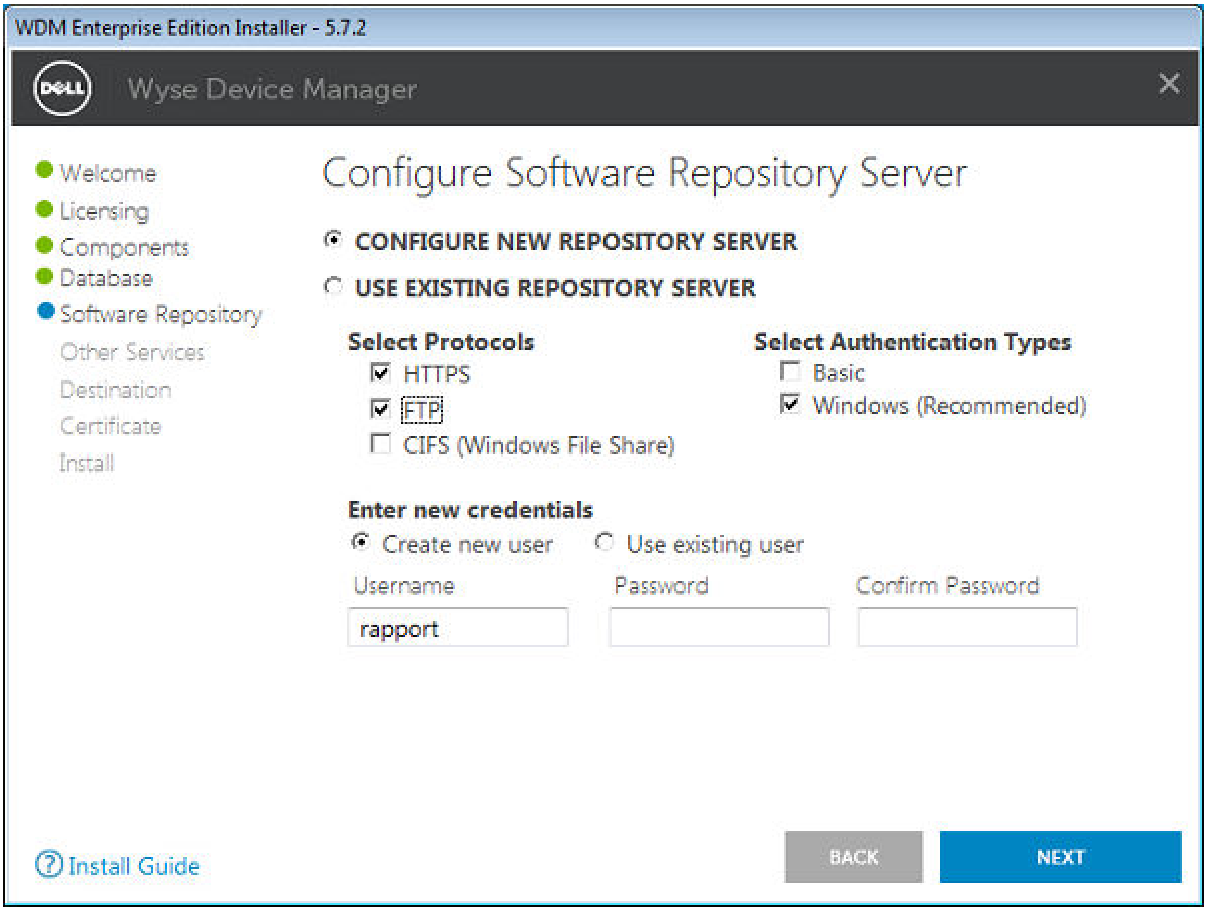
Server Hostname	Port	SQL Administrator	Password
WES008064FFD	1433		

Figure 28. Existing Database Screen

9. If you have selected the second option in **step 7**, then provide the following details:
   a. **Server** — Provide the hostname of the system on which you have installed Microsoft SQL Server.
   b. **Port** — This is entered by default and the port number is 1433.

   NOTE: You can use user dynamic port for TCP/UDP in the range of 49152 to 65535 while installing WDM on cloud environment.

   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.



WDM Enterprise Edition Installer - 5.7.2

Wyse Device Manager

Configure Software Repository Server

● CONFIGURE NEW REPOSITORY SERVER

○ USE EXISTING REPOSITORY SERVER

Select Protocols

☑ HTTPS

☑ FTP

□ CIFS (Windows File Share)

Select Authentication Types

□ Basic

☑ Windows (Recommended)

Enter new credentials

● Create new user ○ Use existing user

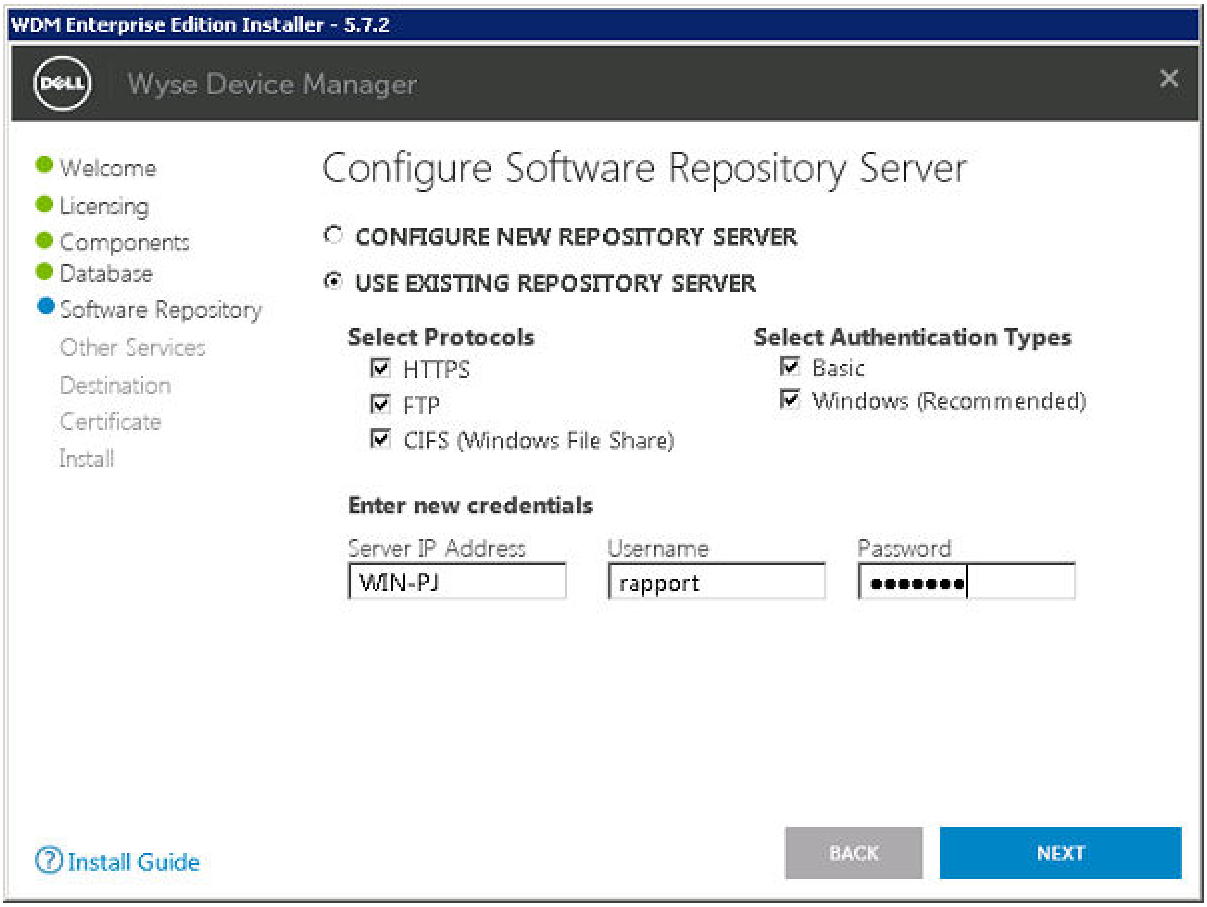
Username	Password	Confirm Password
rapport		

Figure 29. Software Repository Screen

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.



Configure Software Repository Server

○ CONFIGURE NEW REPOSITORY SERVER

● USE EXISTING REPOSITORY SERVER

Select Protocols

- ☑ HTTPS
- ☑ FTP
- ☑ CIFS (Windows File Share)

Select Authentication Types

- ☑ Basic
- ☑ Windows (Recommended)

Enter new credentials

Server IP Address: WIN-PJ

Username: rapport

Password: •••••••

Figure 30. Existing Software Repository Screen

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.

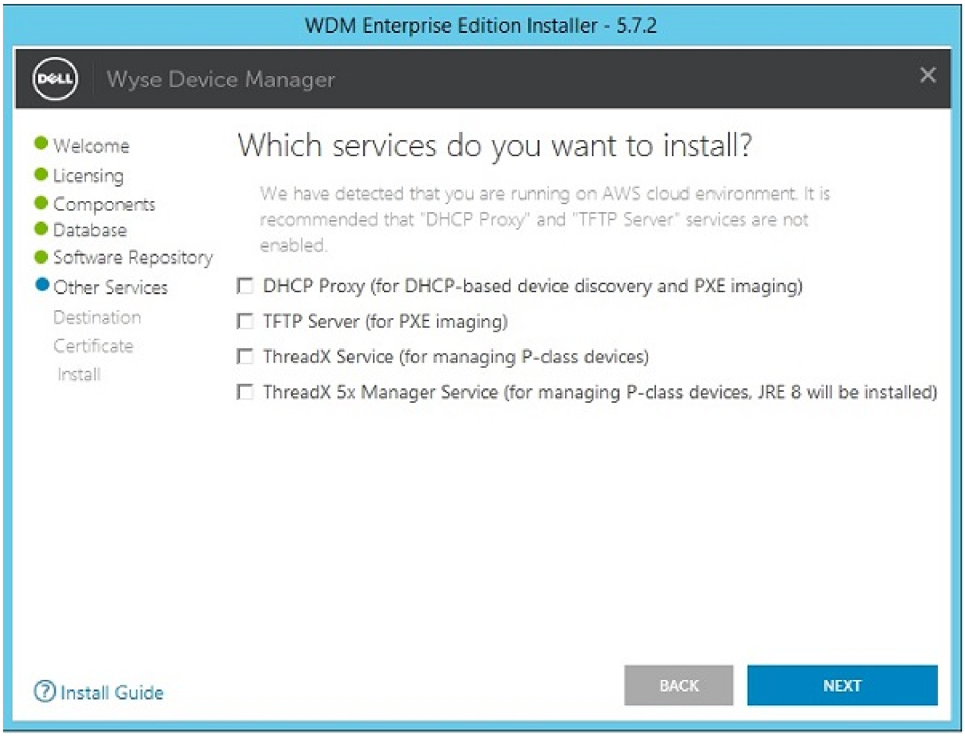
e. **Username** — Rapport is displayed by default. You can change this. If you select the **Use Existing Repository User** option, enter the user name of the existing user.

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.

- If you are working on the AWS cloud environment, the following screen is displayed. Click **Next** to continue.


WDM Enterprise Edition Installer - 5.7.2

Wyse Device Manager

Which services do you want to install?

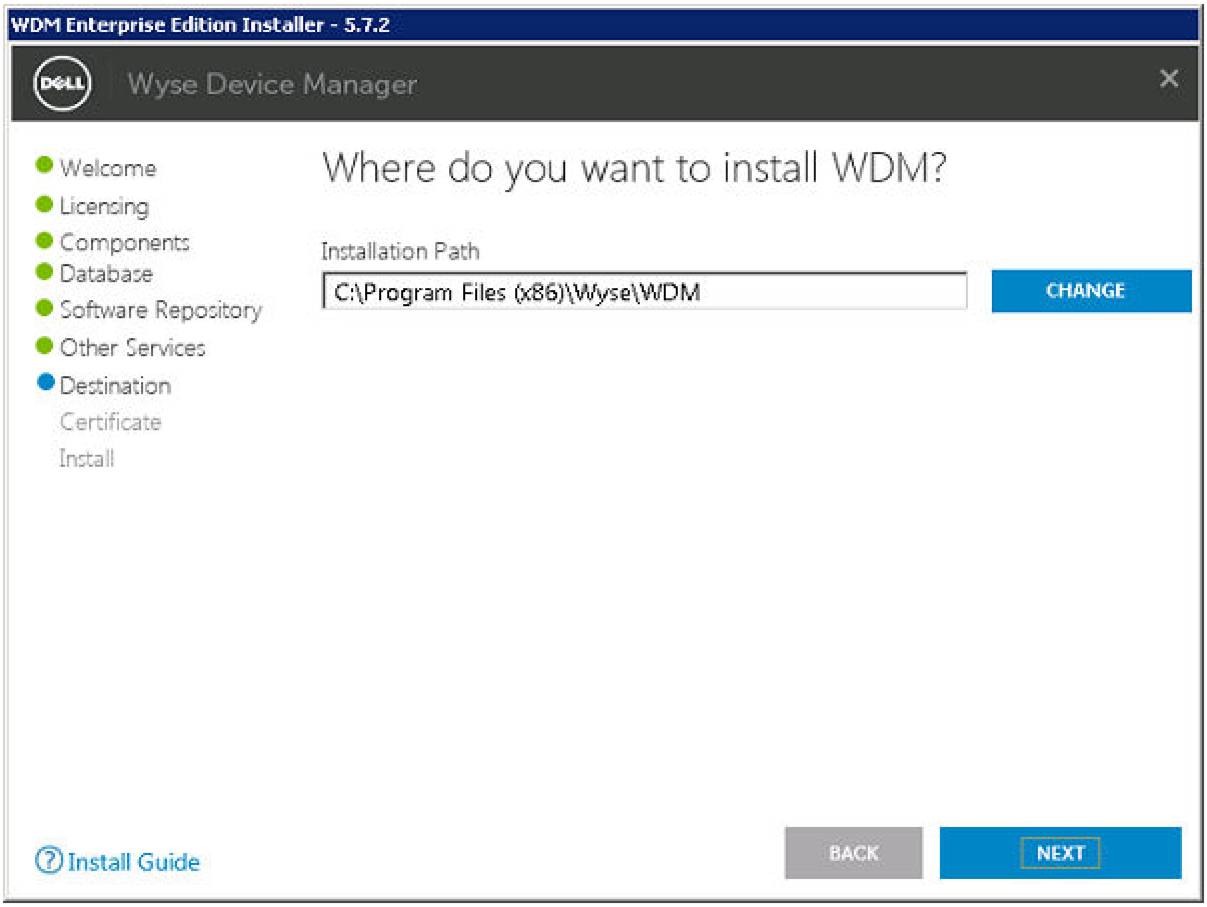
We have detected that you are running on AWS cloud environment. It is recommended that "DHCP Proxy" and "TFTP Server" services are not enabled.

- □ DHCP Proxy (for DHCP-based device discovery and PXE imaging)
- □ TFTP Server (for PXE imaging)
- □ ThreadX Service (for managing P-class devices)
- □ ThreadX 5x Manager Service (for managing P-class devices, JRE 8 will be installed)

Figure 31. Other Services Screen

NOTE: ThreadX 5.0 is available only for Windows Sever 2012 , Windows Server 2012 R2 and above.

13. Provide the destination path and click **Next**. The destination screen is displayed.



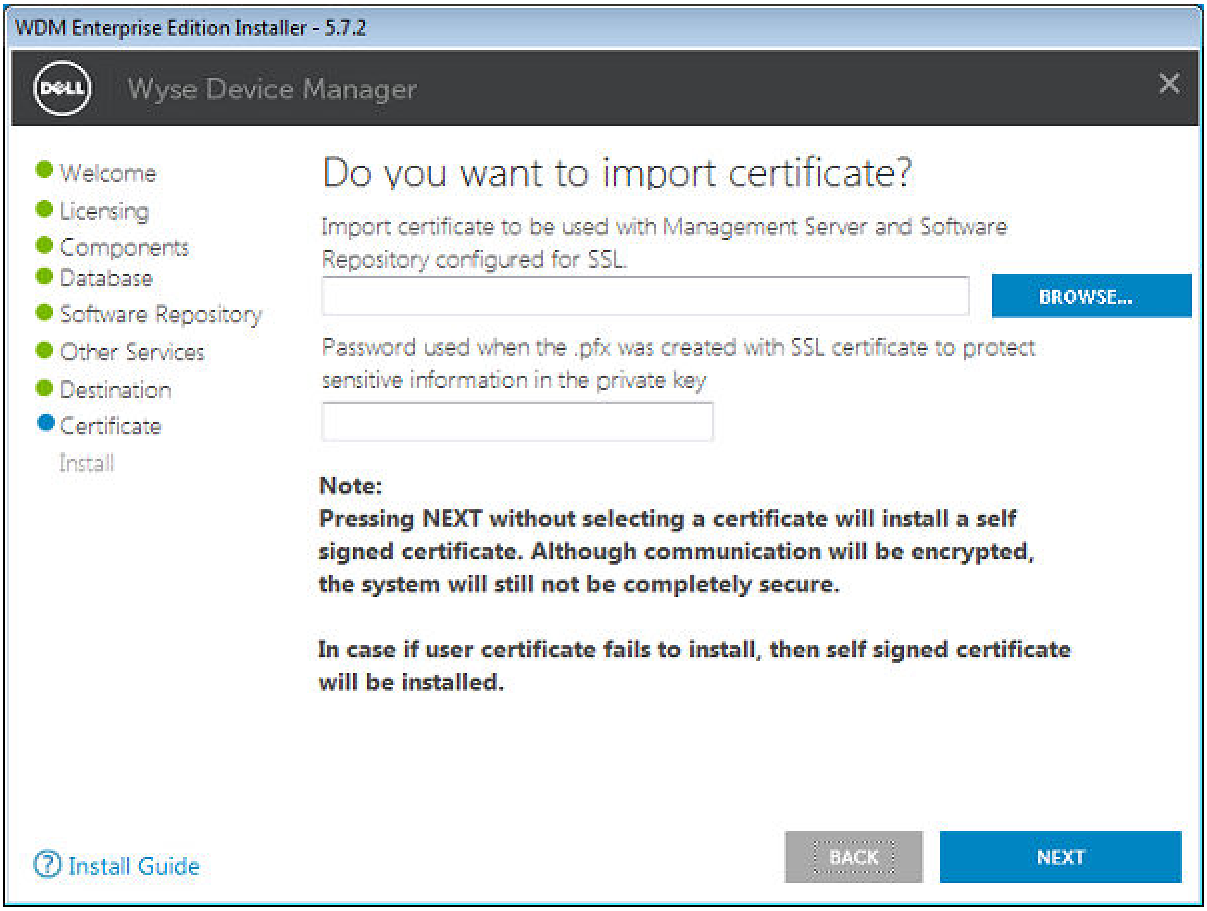
Where do you want to install WDM?

Installation Path: C:\Program Files (x86)\Wyse\WDM

Figure 32. Destination Screen

14. Select the certificate and import the same to start the installation.

   NOTE: If you click the NEXT without selecting a certificate, the installer installs a self signed certificate. The communications are encrypted, still the system is not completely secure. The certificate must be of in the format of .pfx file.



Do you want to import certificate?

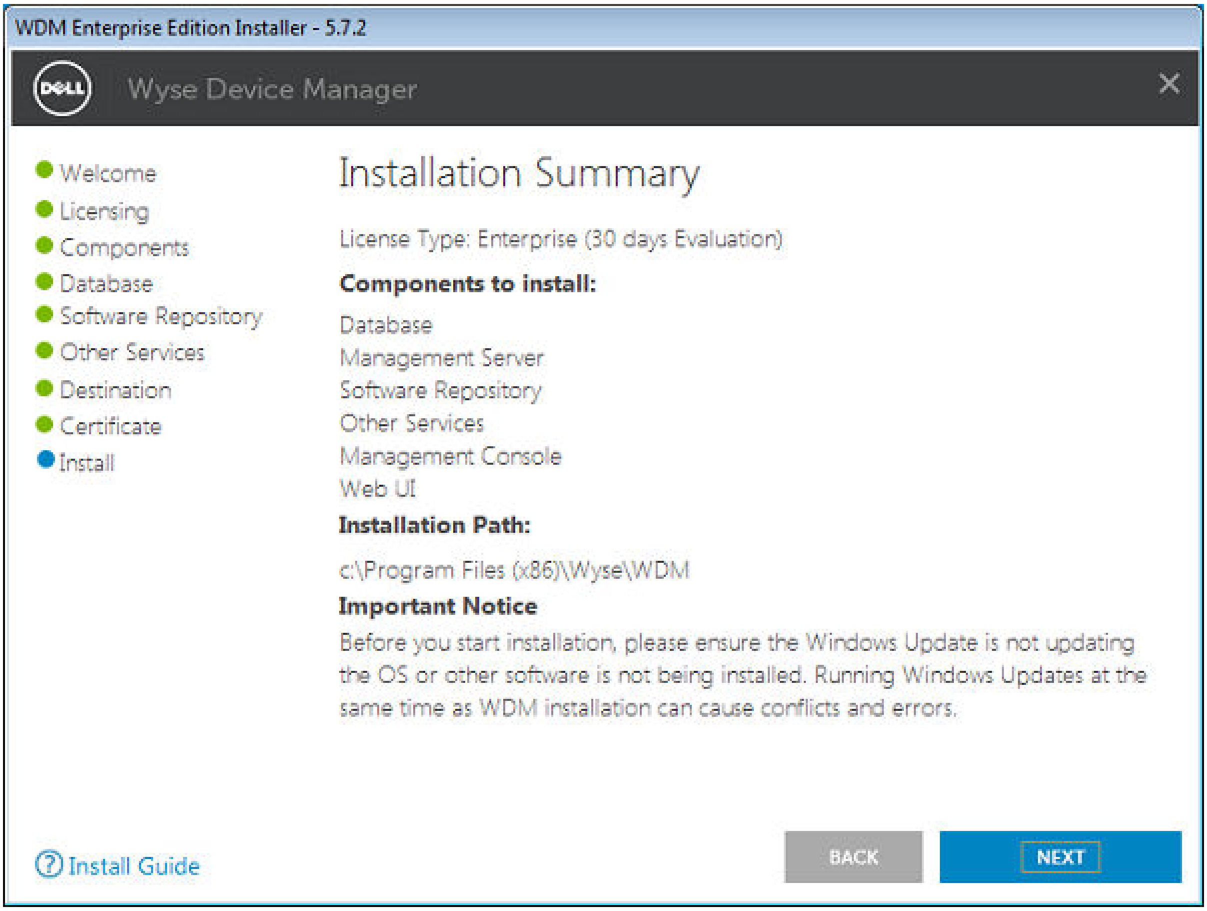
Import certificate to be used with Management Server and Software Repository configured for SSL.

Password used when the .pfx was created with SSL certificate to protect sensitive information in the private key

Note:
Pressing NEXT without selecting a certificate will install a self signed certificate. Although communication will be encrypted, the system will still not be completely secure.

In case if user certificate fails to install, then self signed certificate will be installed.

Figure 33. Certificate Screen



WDM Enterprise Edition Installer - 5.7.2

Wyse Device Manager

Installation Summary

License Type: Enterprise (30 days Evaluation)

Components to install:

Database
Management Server
Software Repository
Other Services
Management Console
Web UI

Installation Path:

c:\Program Files (x86)\Wyse\WDM

Important Notice

Before you start installation, please ensure the Windows Update is not updating the OS or other software is not being installed. Running Windows Updates at the same time as WDM installation can cause conflicts and errors.

Figure 34. Installation Summary Screen

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

GUID-B179116D-40E1-48E5-BC8C-4D723138FF93

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
- Web UI

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 and Web UI.
- Installing the Software Repository.

GUID-93A09892-AB21-4335-8463-3EEA054C6CF6

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 2014 that comes packaged with the WDM installer.

NOTE:

If you are installing the WDM database on an existing SQL Server database, make sure that port 1433 is available on the system.

To install the WDM database, you must select **Database** on the **Components** screen, and then continue with the Installation process.

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 2014)** — 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: If a custom Active directory user is required to be added post installation of Database then manually add the Custom user in to the database and provide required Security rights. Later install Remaining components.
   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 hostname of the system on which you have installed Microsoft SQL Server.
   b. **Port** — This is entered by default and the port number is 1433.

      NOTE: You can add five digit custom port and also use dynamic port while installing WDM database. The dynamic port rage for TCP/UDP is 49152 to 65535.
   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.

For Manual Installation of WDM Database using Scripts, see Manual installation of WDM database using scripts

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.

GUID-BBAD361F-18CC-49A6-8056-48C58E4E24CD

Installing Management Server/Other Services/Management Console/ Web UI

You can install the Management Server, Other Services, Management Console, and Web UI 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**, **Management Console**, and **Web UI**. 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 **DHCP Proxy** 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. Select the certificate and import the same and click **Next**.

    The summary screen is displayed with the components you have selected.
12. 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.

NOTE: In distributed environment, Web UI cannot be installed on a multiple console.

GUID-7D881CF3-3856-4599-9F6A-6629FF876DAC

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. Select the Certificate and import the same and click **Next**.

    NOTE: Same certificate should be used while installing the management server.

    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.

GUID-C1F6041B-968F-444C-8497-E5C4ED36B9BF

Upgrading WDM

The current version of WDM supports an upgrade from WDM version 5.7/5.7.1. You cannot upgrade from any other version. If you are running an older version of WDM, you must first upgrade to version 5.7/5.7.1 and then upgrade to the latest version.

NOTE: After you upgrade to WDM version 5.7.2, you must upgrade all devices with the latest Agents packages available to make sure your devices can be managed using WDM. For more information, see the *WDM 5.7.2 Release Notes*.

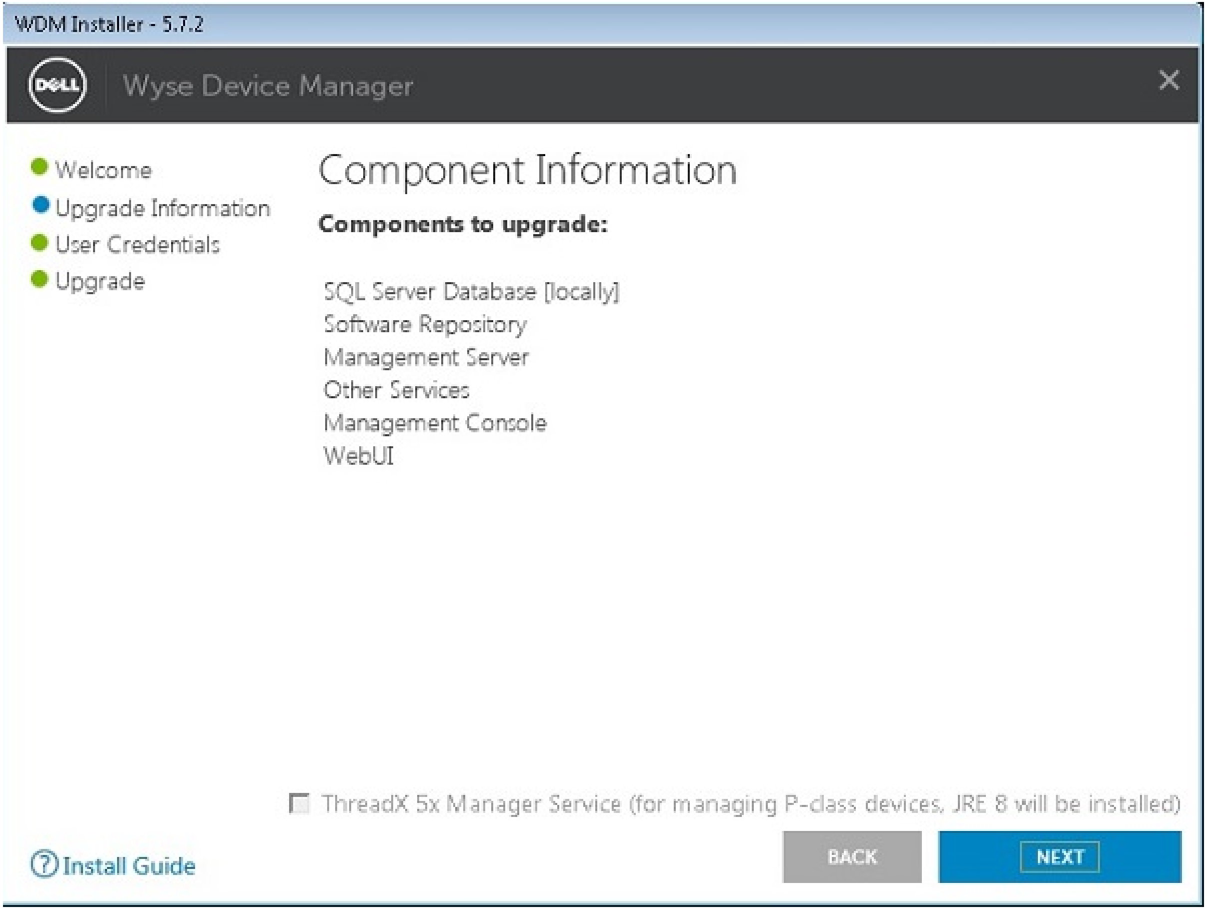
To upgrade to WDM version 5.7.2:

1. Extract the contents of the WDM installer on the system where you have installed WDM version 5.7/5.7.1.

2. Navigate to the folder where you have extracted the installer and run **Setup.exe**.

   The Welcome screen is displayed.

3. Click **Next**. The **Upgrade Information** screen is displayed.



Component Information

Components to upgrade:

SQL Server Database [locally]
Software Repository
Management Server
Other Services
Management Console
WebUI

□ ThreadX 5x Manager Service (for managing P-class devices, JRE 8 will be installed)

Figure 35. Component Information

4. Click **Next** to continue. **User Credentials** screen is displayed. Enter the password.

   Important: The Password field is disabled for SQL Authentication. You are required to enter the password only for Windows Authentication.

5. Click **Next**.

   The Important Information screen is displayed.

6. Read the **Important Information** carefully and click **Next**.

   The upgrade process begins.

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

NOTE: ThreadX 5.x is installed automatically if ThreadX 4.x is already installed on the system with windows 2012 and above versions.

GUID-F5F22152-4BC0-445E-9FB0-A0AEB86B1672

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.

Configure 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. e.g. SelfSSL7.exe /Q /N
cn="TestCert.TestLab.com" /I /S "Default Web Site"
```

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 **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.
14. In **Configure Certificate Database** window, select the **Certificate database location** and **Certificate database log location** and click **Next** to open **Add Roles Wizard** window for IIS.
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 **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 **Server Certificates**.
20. In the right pane of **Server Certificates**, double click **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 the **Server** and on the right pane double click **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 **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.

Installing Root Certificate Authority in IIS 7 on Windows Server 2012 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

  Install the certificate on Domain Controller server:

Use the following guidelines:

1. Go to the Server Manager.
2. In the **Dashboard** >> select option 2 **Add Roles and features**.
3. In Add Roles and Features wizard, select Installation Type as >> Role-based or feature-based installation.
4. In Server Selection >> Select a server from the server pool (By default local server will be selected).
5. Then in Server Role window, select Active Directory Certificate Services' Role.
6. Selecting Active Directory Certificate Services Role will launch the Add Role and Features Wizard' will auto launch with sub-features>> Click on Add Features button.
7. Click Next->Next. Then in Features window, leave the default values as it is and click Next.
8. Then in AD CS window appears and click Next button.
9. In Role Service window, select the options Certification Authority and Certificate Authority Web Enrolment.
10. After selecting the option Certificate Authority Web Enrolment, if IIS is not installed in the server, another window Add Features that are required for Certification Authority Web Enrollment sub-window will appear.
11. On the above window, click on Add Feature button and click Next to Confirmation window.
12. Then click on 'Install' button to install the AD Certificate role.
13. In the Results window, Feature installation progress can be viewed.
14. After Installation succeeds for AD Certificate Authority role, click on 'Close' button.

15. Then in the Server Manager>> Dashboard console under notifications' find the Post-deployment Configuration message.
16. In Post-deployment Configuration message click on link "Configure Active Directory Certificate Services on the local server".
17. Then AD CS Configuration>> Credentials window will open get launched; provide the required appropriate credentials and click on 'Next' button.
18. Then under Role Services>> select the options Certification Authority and Certificate Authority Web Enrolment and click 'Next' button.
19. Then in the Setup Type window, depending on the requirement select either Enterprise or Standalone radio button and click Next to open CA Type window.
20. In CA Type window, depending on the requirement select either Root CA or Subordinate CA radio button and click Next to open Private Key window.
21. In 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.
22. In Configure Cryptography for CA window,
    - depending on the requirement select the value for field Select a cryptographic service provider (CSP) from the combo drop down box,
    - Provide the Key length from the next combo box
    - Select the value for field Select the Hash algorithm for signing certificate issued by this CA
    - and then 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.
23. In CA Name window, provide the values for Common name for this CA and Distinguished name suffix fields and click Next to open Validity Period window.
24. In the Specify Validity Period window, select the validity period for the certificate generated for this CA and click Next to open Certificate Database window.
25. In Certificate Database window, select the Certificate database location and Certificate database log location and click Next to open Confirmation window.
26. Then in Confirmation window, click on Configure button which will launch the progress window.
27. Then in the Results window, Certification Authority and Certification Authority Web Enrollment Configuration succeeded message will appear.
28. Click on Close button to finish the configuration of AD CS.
29. 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. Click on Create Domain Certificate link on right most pane and 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 (created in your AD Controller machine or in your setup) 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 -> 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 Type as HTTPS, and select Certificate Authority under IP Address, select the recently created certificate from SSL Certificate combo drop down 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 ‘Require’ radio button for Client certificate and Apply the settings.

GUID-95673E02-37F2-4DE5-AD34-9AF746A637BC

4

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 5.7.2 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.

After the Uninstallation, ensure that you meet the following checklists :

- WyseDeviceManager 5.7.2 **WebUI** icon should be removed from the Desktop.
- In IIS , HApi Application should be deleted under Rapport HTTP Server.
- In IIS , MyWDM Application should be deleted under Rapport HTTP Server.
- In IIS , WebUI Application should be deleted under Rapport HTTP Server.

GUID-1D85EF8E-B5B7-4B29-B568-BC9E22318E54

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, Software Repository, and the Web UI.
2. Click the start menu and select Control Panel.
3. Click **Programs** → **Uninstall a program** on the Control Panel screen.
4. Select WDM 5.7.2 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: *Unable to connect to database.* Make sure you enter the correct credentials.
10. Click **Next** to begin the uninstallation process.
11. After the database is uninstalled, restart the system when prompted.

GUID-2E7ACC0A-9A35-4ABC-A35B-DBA0AB8388F7

5

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.

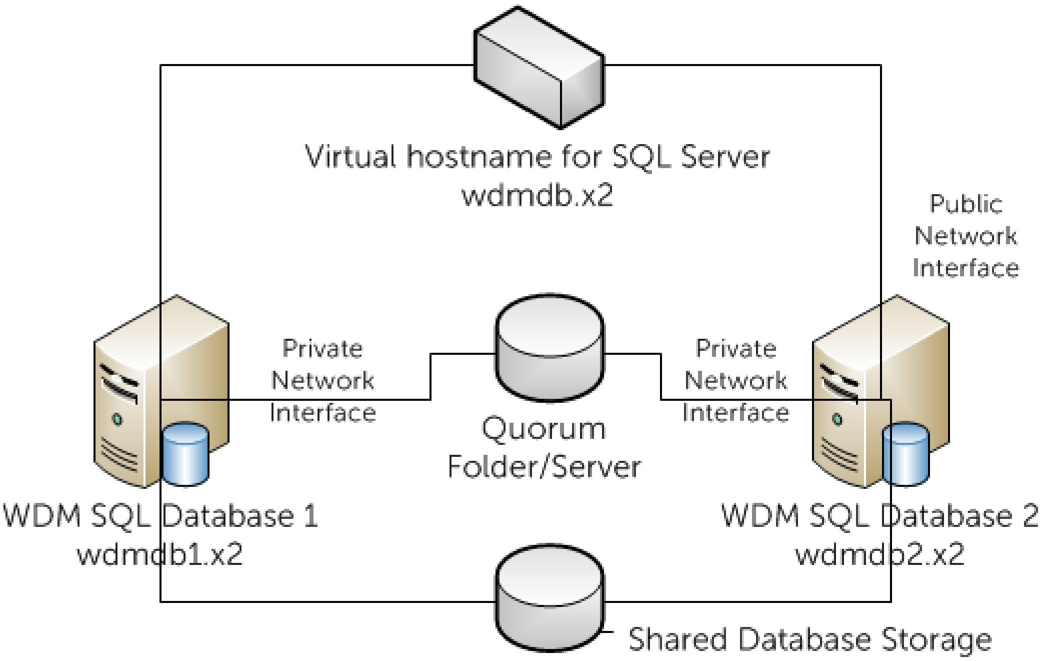


Figure 36. WDM High Availability Database Clustering

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

GUID-DC2CC4B7-E9EB-4289-B8CA-2F7B86D81BAB

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 four 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.

GUID-258A85F8-180E-410D-A87B-7D749BA0FEA2

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.

  NOTE: The steps for database clustering discussed in this guide are performed on Microsoft SQL Server 2012. However database clustering is supported on other supported versions of SQL Server.

  All the VMs should be connected to an Active Directory (AD) domain.
- All the four VMs should have Windows Server 2008 R2 Enterprise installed on them.

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

GUID-75FFD5C6-F71B-4C88-B43F-3526A43B4307

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**.

   NOTE: There must be two subnets for two network cards i.e. one subnet for the Public network (PDB) and one subnet for the Private network (PDB), and the same for the two network cards on the SDB server
8. Make sure that the **Public Network** option is first in order in the **Advanced Settings** window.
9. To launch the **Advanced Settings** window, press the Alt button to access the **Advanced** menu in the **Network Connections** screen and select the **Advanced Settings** option.
10. In the **Network Connections** screen, select **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 acoss 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.

GUID-034F12D6-8E93-4756-A713-6A039EA4CC28

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**.

GUID-A66249CB-34E4-4776-8570-864D13FCB118

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.

GUID-1B55B283-632C-473C-A560-B32F12C17C62

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 **Failover Cluster Manager** under **Features**.
5. Right click on your cluster and select **More Actions → Configure Cluster Quorum Settings**.
6. Select the **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.

GUID-615CA07D-D96F-4320-B68C-2D3A3995D762

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.

GUID-DFD0336F-6144-44F0-83E5-AE8FD1E7CDB5

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.

NOTE: If you encounter the Windows Firewall Warning while installing SQL Server, you can ignore the warning and continue with the installation. If required, you can add port 1433 to the SQL Server firewall exception.

GUID-A127E83C-EB04-4170-9E32-2205E1EDF2D5

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**.

GUID-5E5187F6-F2BD-47E6-A228-6F900CE85849

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 on VMs that you have identified as the primary and secondary nodes of the cluster.

6. Run the following script on the database:

   ```
   Use RapportDB
   GO
   Update Install set ServerName='NEWCLUSTER01' where Module='Rapport4DB'
   ```
7. When you install the WDM components without the database, make sure you provide the name of the SQL Database Cluster name in the Server IP Address field.
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:\Program Files\WYSE\WDM\Database** in the primary node, create the same structure in the secondrary 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. Right-click on **AlwaysOn High Availability** in the Object Explorer and select **New Availability Group Wizard**.
15. Click **Next** on the **New Availability Group Wizard** screen.
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.

    Repeat the step for the secondary node.
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 the **Security** node, select **Login**, right-click and select **New Login** to create the Rapport user. This step is important for WDM to function as you are creating the SQL Server Authentication user.
30. Select **Server Roles**, select the **sysadmin** check-box and click **OK**.
31. View the **Rapport** user on the **SQL Server Management Studio**.
32. Repeat steps 28 — 31 on the secondary node.

NOTE: If there is a fail-over from the primary database to the secondary database, you must restart the WDM UI.

GUID-29EA3E95-3905-4306-9E74-02BDCD898FED

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 a separate node other than the primary and secondary nodes.

1. Log in to the system where you have installed WDM.
2. Launch the **HAConfigureUtility** from **Start** → **All Programs** → **Dell Wyse Device Manager** → **Utilities**.
3. 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. For example, **WDMCLUSTER**.
- **Database User Name** – Specify **rapport** as the database user.
- **Database Password** – Specify the password of the rapport user.

4. Click **Configure.**

   The connection details are displayed on the bottom pane of the utility.

GUID-17004940-5904-45F0-AC6A-0065DF001DE9

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: ScopeItems_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.

GUID-410FD7CB-0208-40F2-98FB-208BB21C8782

6

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.

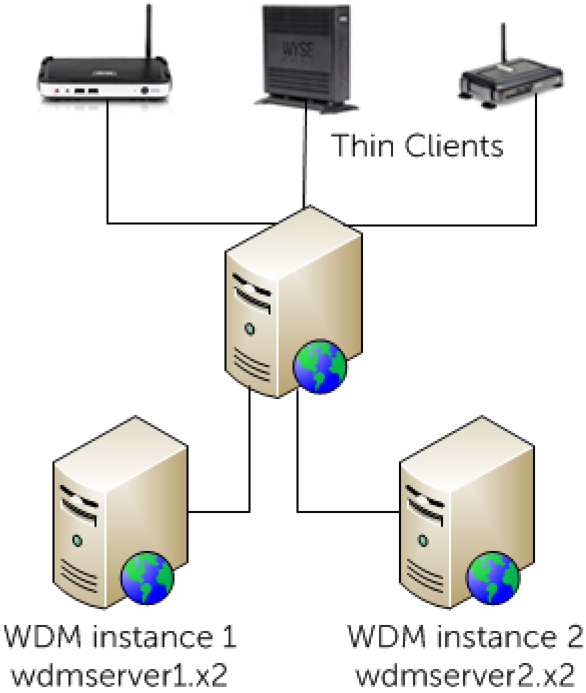


Figure 37. WDM Load Balancing Setup

GUID-28479843-0299-4AD7-8D43-077519D3092A

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 ThreadX 4.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 doamin.

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 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.

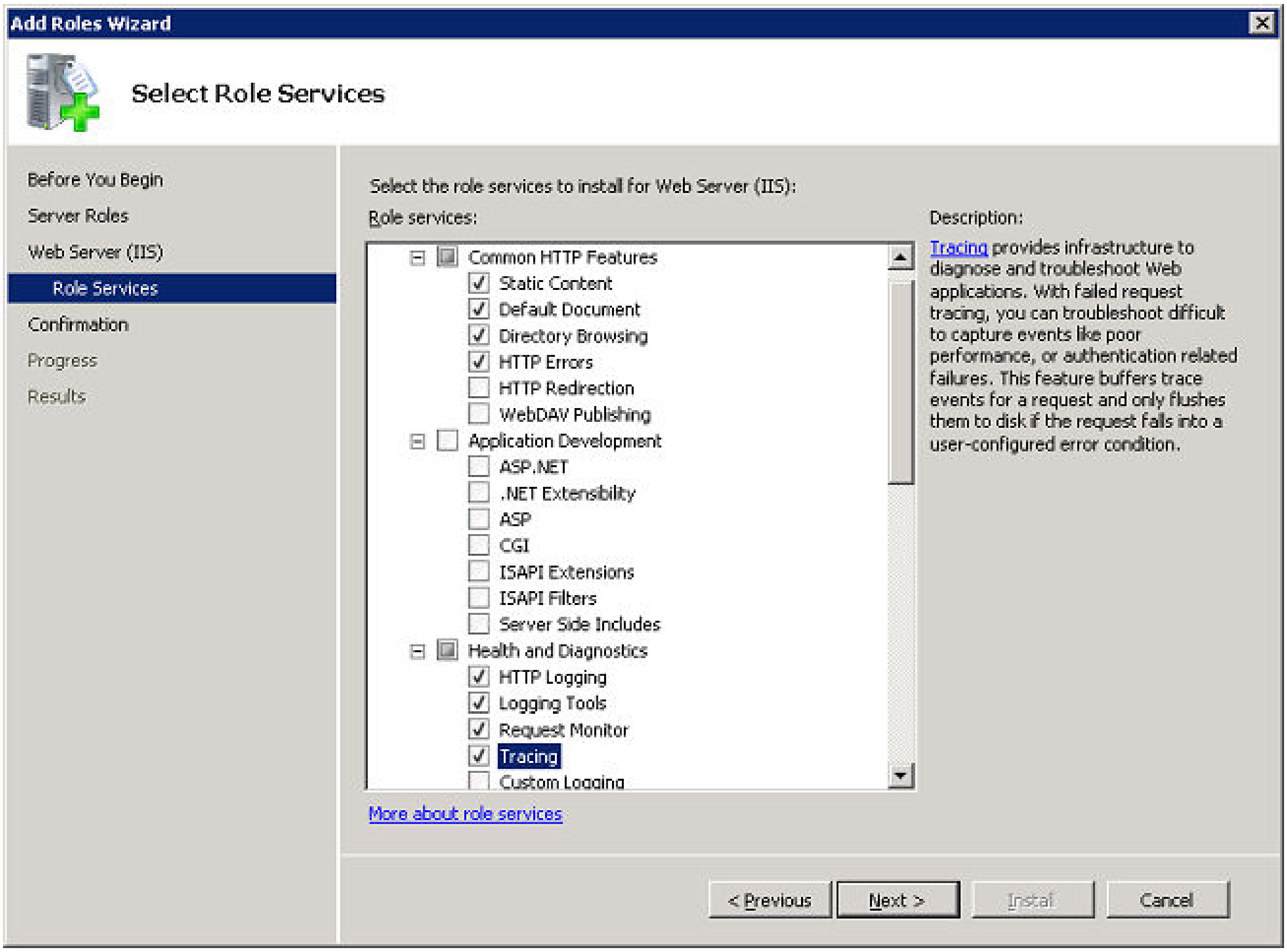
GUID-C3E1333E-CFEF-426D-AA0B-20BC88BBBDFA

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**.



Select the role services to install for Web Server (IIS):

Role services:

- ▣ Common HTTP Features
  - ☑ Static Content
  - ☑ Default Document
  - ☑ Directory Browsing
  - ☑ HTTP Errors
  - ☐ HTTP Redirection
  - ☐ WebDAV Publishing
- ☐ Application Development
  - ☐ ASP.NET
  - ☐ .NET Extensibility
  - ☐ ASP
  - ☐ CGI
  - ☐ ISAPI Extensions
  - ☐ ISAPI Filters
  - ☐ Server Side Includes
- ▣ Health and Diagnostics
  - ☑ HTTP Logging
  - ☑ Logging Tools
  - ☑ Request Monitor
  - ☑ Tracing
  - ☐ Custom Logging

Description:

Tracing provides infrastructure to diagnose and troubleshoot Web applications. With failed request tracing, you can troubleshoot difficult to capture events like poor performance, or authentication related failures. This feature buffers trace events for a request and only flushes them to disk if the request falls into a user-configured error condition.

4. Select the following options:

Option	Sub-options
Common HTTP Features	· Static Content · Default Document · HTTP Errors · Directory Browsing
Health and Diagnostics	· HTTP Logging · Request Monitor · Logging Tools · Tracing
Management Tools	Select all the sub-options.

5. Click **Next** to view the summary.
6. Click **Install** to install IIS.

GUID-BB2CB293-04D3-4353-B051-391E3A55917F

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 https://www.microsoft.com/en-us/download/details.aspx?id=47333. Download the **ARRv3_0.exe** file and install it.

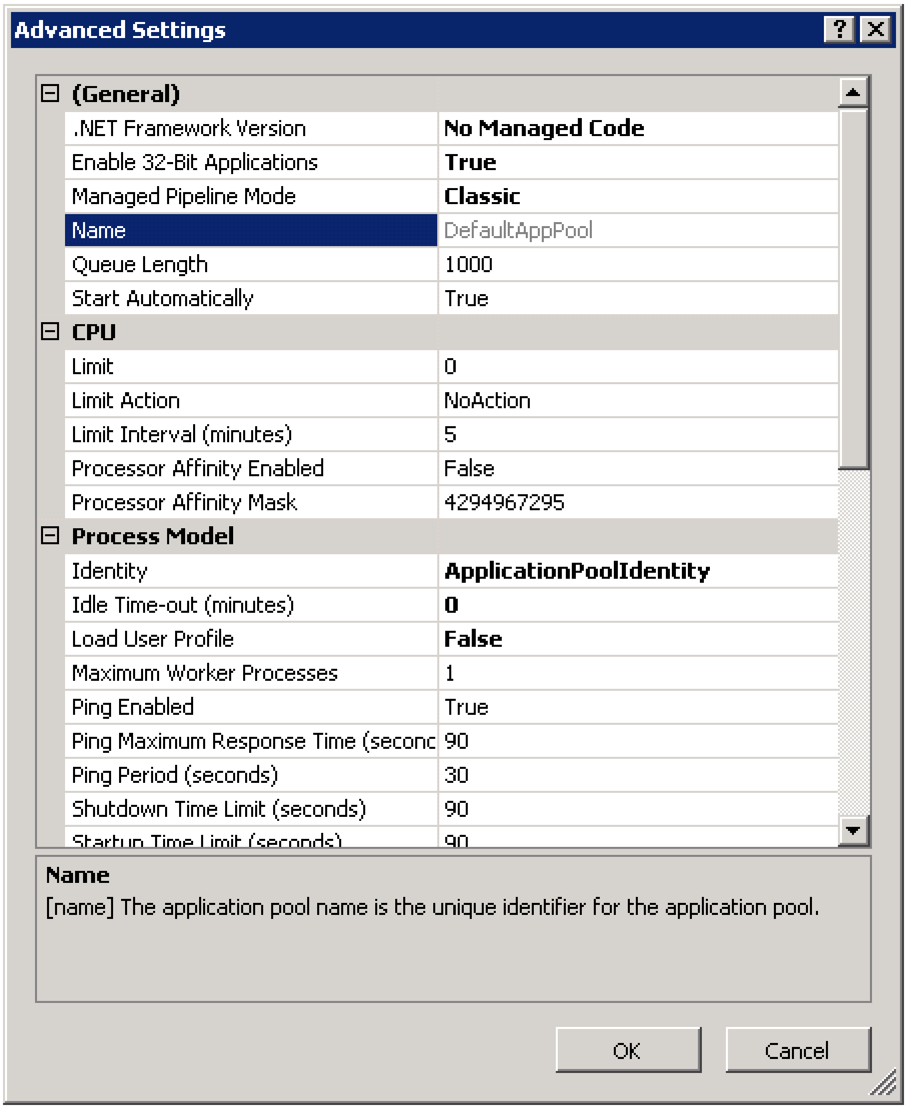
GUID-661B7B7A-F16A-4B1D-8FC6-49CE418EEDF7

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.
3. Select **DefaultAppPool** and click **Edit Application Pool** on the **Action** pane.
4. Select **Advanced Settings** to display the **Advanced Settings** window.



⊟ **(General)**	
.NET Framework Version	**No Managed Code**
Enable 32-Bit Applications	**True**
Managed Pipeline Mode	**Classic**
Name	DefaultAppPool
Queue Length	1000
Start Automatically	True
⊟ **CPU**	
Limit	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
⊟ **Process Model**	
Identity	**ApplicationPoolIdentity**
Idle Time-out (minutes)	**0**
Load User Profile	**False**
Maximum Worker Processes	1
Ping Enabled	True
Ping Maximum Response Time (seconc	90
Ping Period (seconds)	30
Shutdown Time Limit (seconds)	90
Startup Time Limit (seconds)	90

Name
[name] The application pool name is the unique identifier for the application pool.

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.

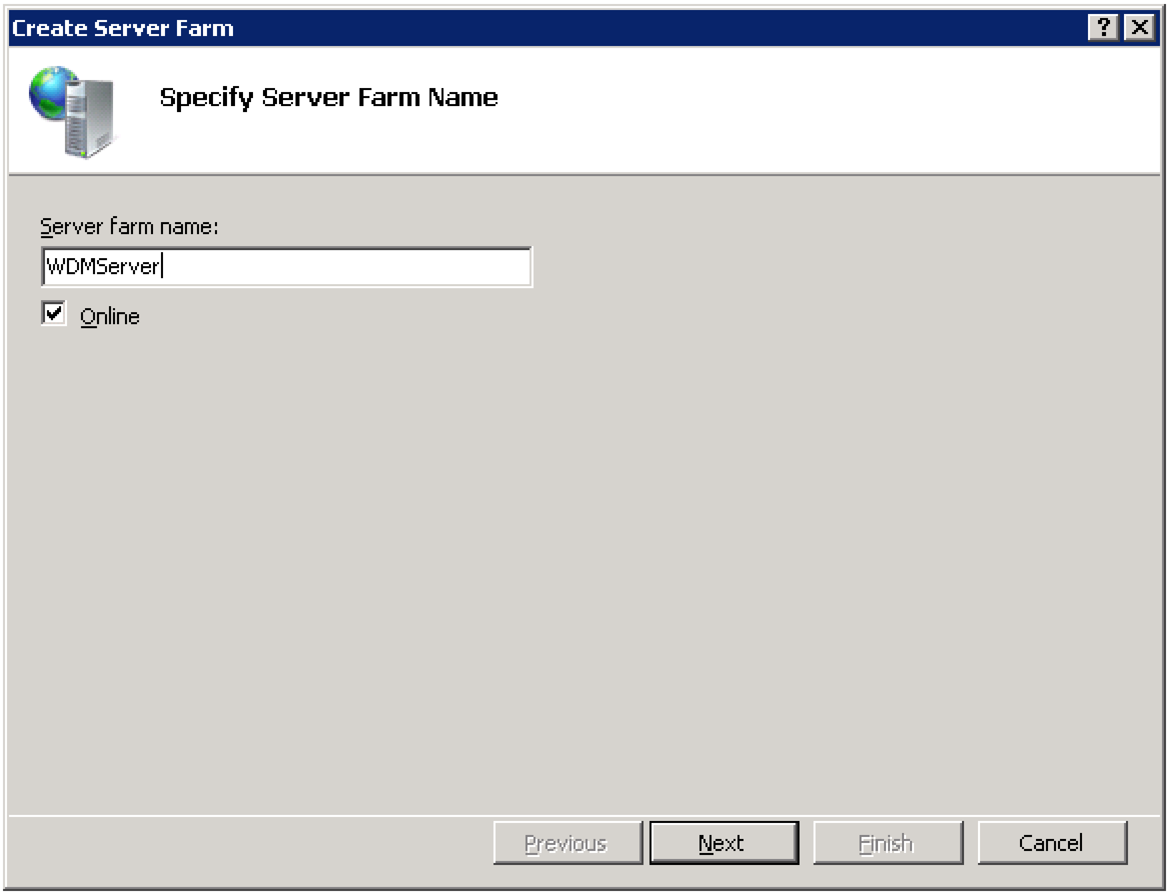
GUID-5C922BF6-6F2D-4B4A-987D-8A3485666705

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.



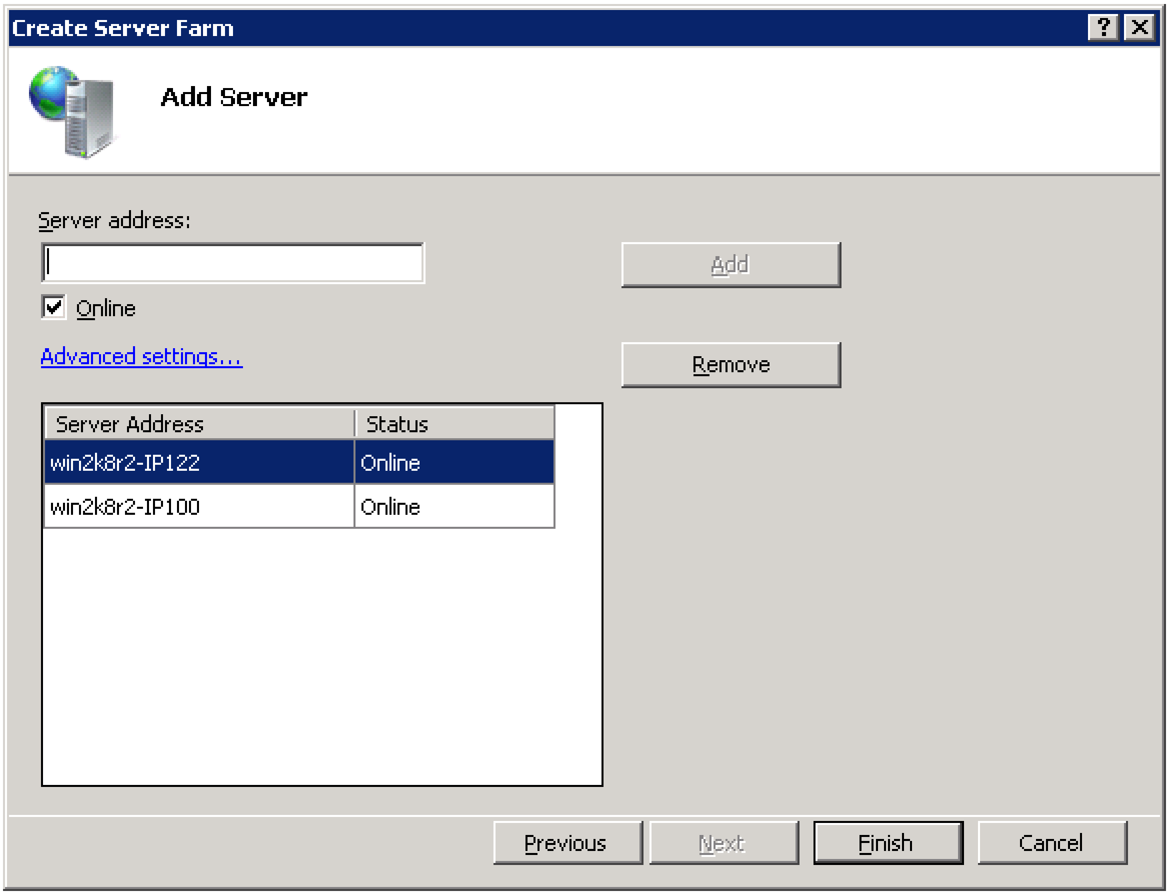
Create Server Farm

Specify Server Farm Name

Server farm name: WDMServer

☑ Online

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



Server address:

☑ Online

Server Address	Status
win2k8r2-IP122	Online
win2k8r2-IP100	Online

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.

   After the servers are added and the server farm is created you are prompted with a message to rewrite the routing rules for all requests to automatically come to the server farm.
7. Click **Yes** so that IIS manager can create a URL rewrite rule to route all incoming requests to this server farm.

GUID-821FA42D-B3CE-45E0-97EA-521DE023882E

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. Go to the **Server Farm** and double click the **Created Farm**.

9. 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

GUID-80509A6E-5817-4336-8942-FAEF7BCCE109

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 Hhealth 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.

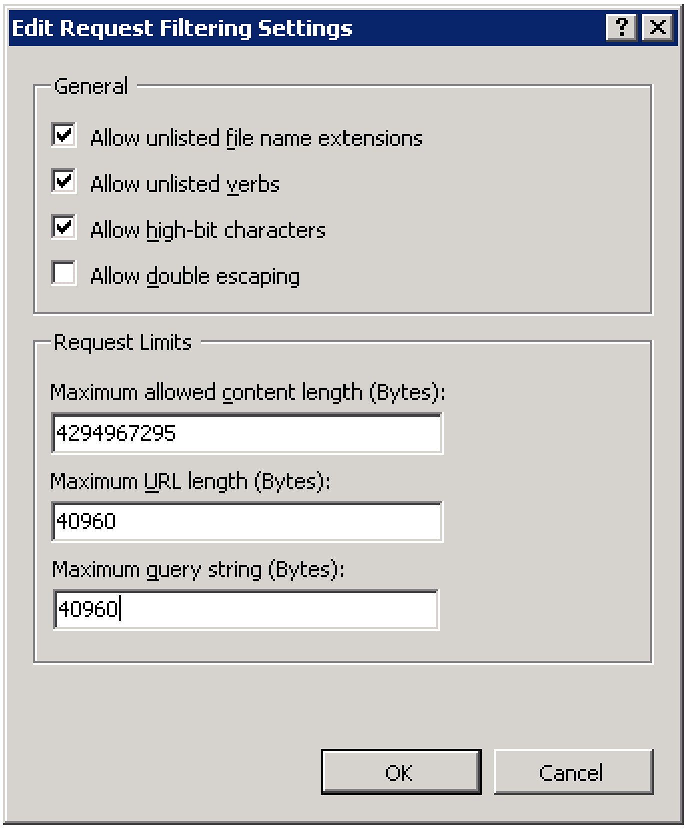
The Server Farm properties are now configured.

GUID-900447C9-A856-4699-8B66-B21F70F6FEDF

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

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.

GUID-11D581EA-57D1-4F1F-AC18-BFCF9417C6ED

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 start the WDM WEb UI Console.
2. Select **System** → **Comsole**.
3. Under Manager Server Alias Name , enter the FQDN of ARR Proxy Server.
4. Click **Save** to save the settings.

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

GUID-E4AA88FE-9B3C-43F6-B592-18BD995B4118

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

GUID-F0318D55-AC3F-4897-9BF0-210AA92D7E8B

Configuring Load Balancing for ThreadX 4.x 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.

For more information on installing DNS on a Windows 2008 Server, go to http://technet.microsoft.com/en-us/library/cc725925.aspx.

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 the your WDM Management Servers to manage a large number of ThreadX devices.

GUID-DE70A0F7-5557-4C02-8A29-689D18578745

Configuring Load Balancing for ThreadX 5.x Devices

When WDM is used to manage ThreadX 5.x devices in a large enterprise environment, a single Teradici Device Proxy Server which is used to manage ThreadX 5x devices from WDM cannot scale up to manage more than 18 thousand devices. There could be problems or delays in client check-ins, schedule execution, and/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 Teradici Device Proxy Servers on different systems and balance the load between them using a proxy as described below.

The components of the load balancer are as follows:

- Teradici Device Proxy Server
- HA Proxy Server

WDM uses the HAProxy hosted on the Ubuntu server 16.04.1 LTS to perform load balancing between the Teradici Device Proxy servers. HAProxy is a load balancer proxy that can also provide HA based on how it is configured. It is a popular open source software for TCP/HTTP Load Balancer, and proxying solution which can be run on Linux. The most common use is to improve the performance and reliability of a server environment by distributing the workload across multiple servers.

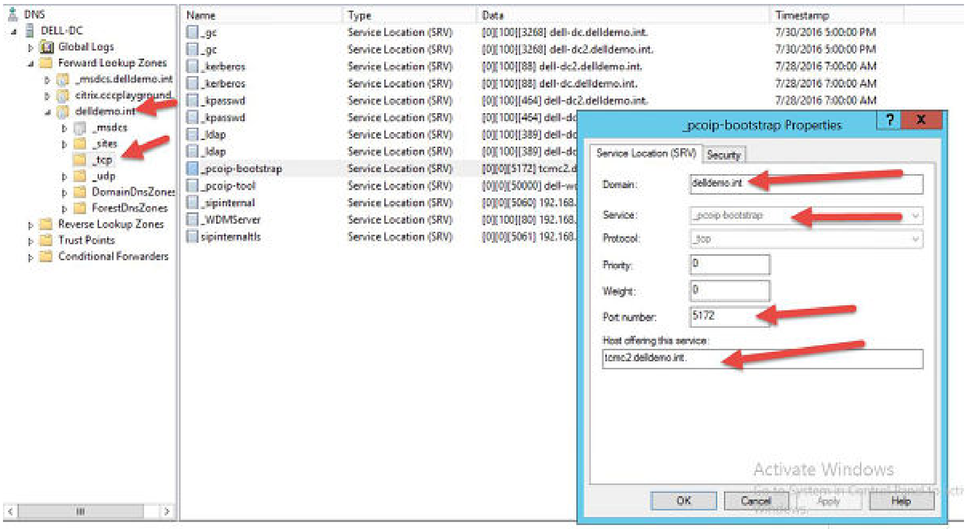
This section describes how to set up and configure load balancing of the HA Proxy Server.

Steps to create DNS_SRV Record:

Firmware 5.x uses a DNS_SRV record in addition to the text record that contains the thumbprint of the SSL certificate to use in the management console.

WDM 5.7.2 supports Teradici 5.x firmware with comprehensive features.

1. The first record required is a DNS_SRV record for _pcoip-bootstrap. The record must point to the name of the Teradici Device Proxy (HAProxy).



Name	Type	Data	Timestamp
_gc	Service Location (SRV)	[0][100][3268] dell-dc.delldemo.int.	7/30/2016 5:00:00 PM
_gc	Service Location (SRV)	[0][100][3268] dell-dc2.delldemo.int.	7/30/2016 5:00:00 PM
_kerberos	Service Location (SRV)	[0][100][88] dell-dc2.delldemo.int.	7/28/2016 7:00:00 AM
_kerberos	Service Location (SRV)	[0][100][88] dell-dc.delldemo.int.	7/28/2016 7:00:00 AM
_kpasswd	Service Location (SRV)	[0][100][464] dell-dc2.delldemo.int.	7/28/2016 7:00:00 AM
_kpasswd	Service Location (SRV)	[0][100][464] dell-dc	
_ldap	Service Location (SRV)	[0][100][389] dell-dc	
_ldap	Service Location (SRV)	[0][100][389] dell-dc	
_pcoip-bootstrap	Service Location (SRV)	[0][0][5172] tcmc2.d	
_pcoip-tool	Service Location (SRV)	[0][0][50000] dell-w	
_sipinternal	Service Location (SRV)	[0][0][5060] 192.168.	
_WDMServer	Service Location (SRV)	[0][100][80] 192.168.	
sipinternaltls	Service Location (SRV)	[0][0][5061] 192.168.	

_pcoip-bootstrap Properties

Service Location (SRV) | Security

Domain: delldemo.int

Service: _pcoip-bootstrap

Protocol: _tcp

Priority: 0

Weight: 0

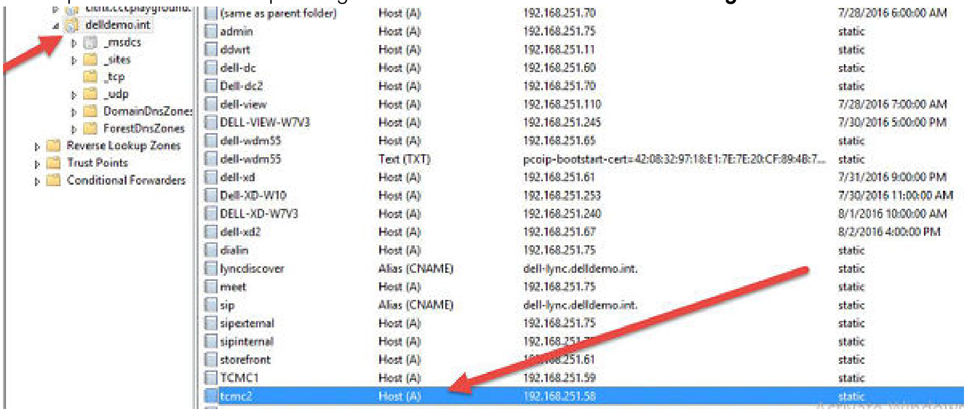
Port number: 5172

Host offering this service:

tcmc2.delldemo.int.

Figure 38. DNS_SRV record for _pcoip-bootstrap

2. The second record required is an A record pointing to the name used in the **Host offering this service** field.



(same as parent folder)	Host (A)	192.168.251.70	7/28/2016 6:00:00 AM
admin	Host (A)	192.168.251.75	static
ddwrt	Host (A)	192.168.251.11	static
dell-dc	Host (A)	192.168.251.60	static
Dell-dc2	Host (A)	192.168.251.70	static
dell-view	Host (A)	192.168.251.110	7/28/2016 7:00:00 AM
DELL-VIEW-W7V3	Host (A)	192.168.251.245	7/30/2016 5:00:00 PM
dell-wdm55	Host (A)	192.168.251.65	static
dell-wdm55	Text (TXT)	pcoip-bootstart-cert=42:08:32:97:18:E1:7E:7E:20:CF:89:4B:7...	static
dell-xd	Host (A)	192.168.251.61	7/31/2016 9:00:00 PM
Dell-XD-W10	Host (A)	192.168.251.253	7/30/2016 11:00:00 AM
DELL-XD-W7V3	Host (A)	192.168.251.240	8/1/2016 10:00:00 AM
dell-xd2	Host (A)	192.168.251.67	8/2/2016 4:00:00 PM
dialin	Host (A)	192.168.251.75	static
lyncdiscover	Alias (CNAME)	dell-lync.delldemo.int.	static
meet	Host (A)	192.168.251.75	static
sip	Alias (CNAME)	dell-lync.delldemo.int.	static
sipexternal	Host (A)	192.168.251.75	static
sipinternal	Host (A)	192.168.25[illegible]	static
storefront	Host (A)	192.168.251.61	static
TCMC1	Host (A)	192.168.251.59	static
tcmc2	Host (A)	192.168.251.58	static

Figure 39. Host Record

3. The third record required is a Txt record. The txt record is the thumbprint of the SSL certificate in use by the management console.

Complete the following steps to create A record for Host as well as Txt record:

1. Click the domain node (delldemo.int) and select the **Other New Records** and then select Host (A or AAAA), the name is the A record of the management console.

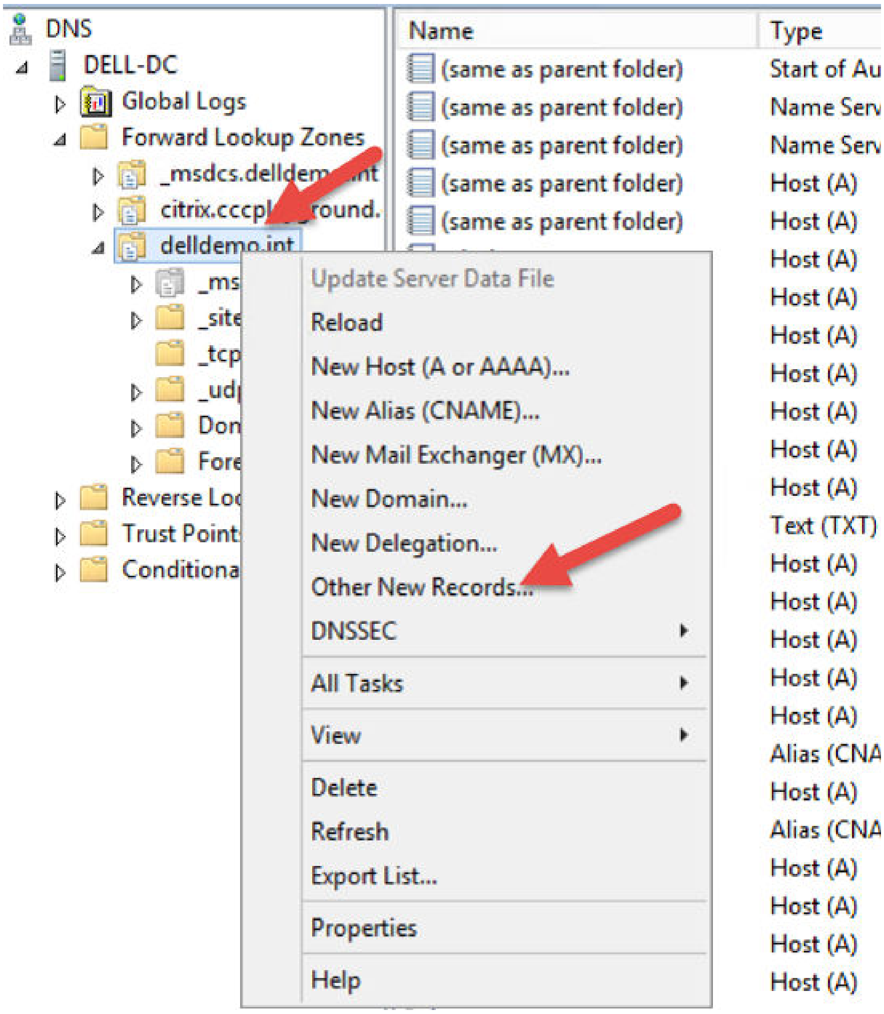
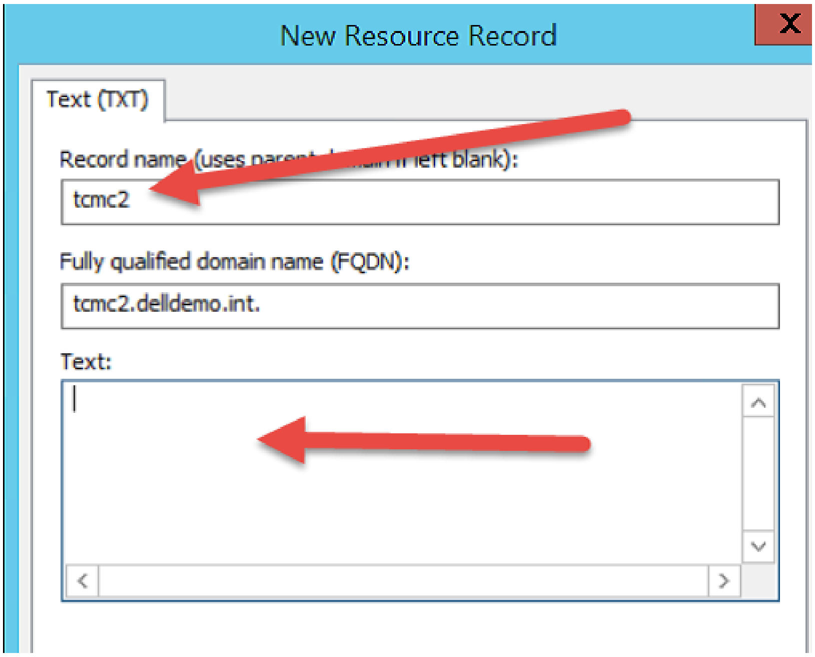


Figure 40. Create TXT record

2. Click on the domain node (delldemo.int) and select the **Other New Records** and then select Text (TXT), to create the text field which has the thumbprint of the certificate.



New Resource Record

Text (TXT)

Record name (uses parent domain if left blank):
tcmc2

Fully qualified domain name (FQDN):
tcmc2.delldemo.int.

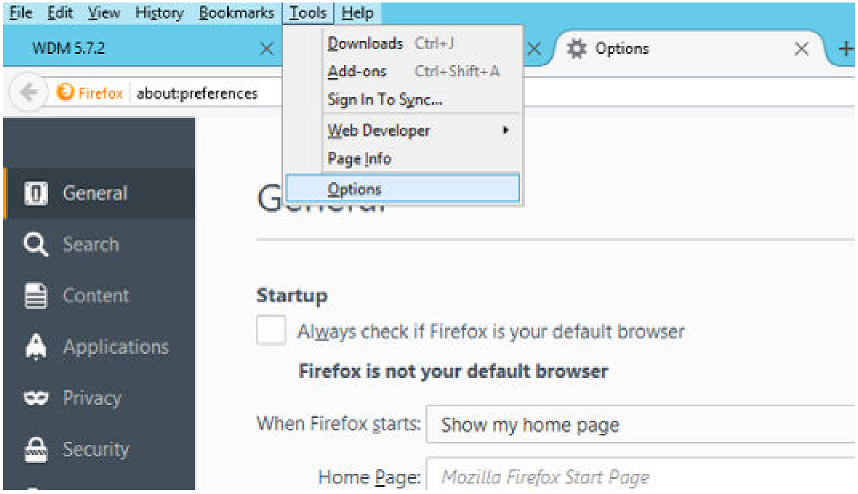
Text:

Figure 41. New Resource Record

The Sha256 thumbprint can be obtained using Firefox browser.

To obtain the thumbprint when Wyse Device Manager (WDM) is installed with Teradici 5x:

1. You must open the Firefox browser from the device where Teradici 5.x component is installed. After opening the browser, press the bring **Alt + T** key to open Tools.
2. From the drop-down list, select **Options**.



☐ Always check if Firefox is your default browser

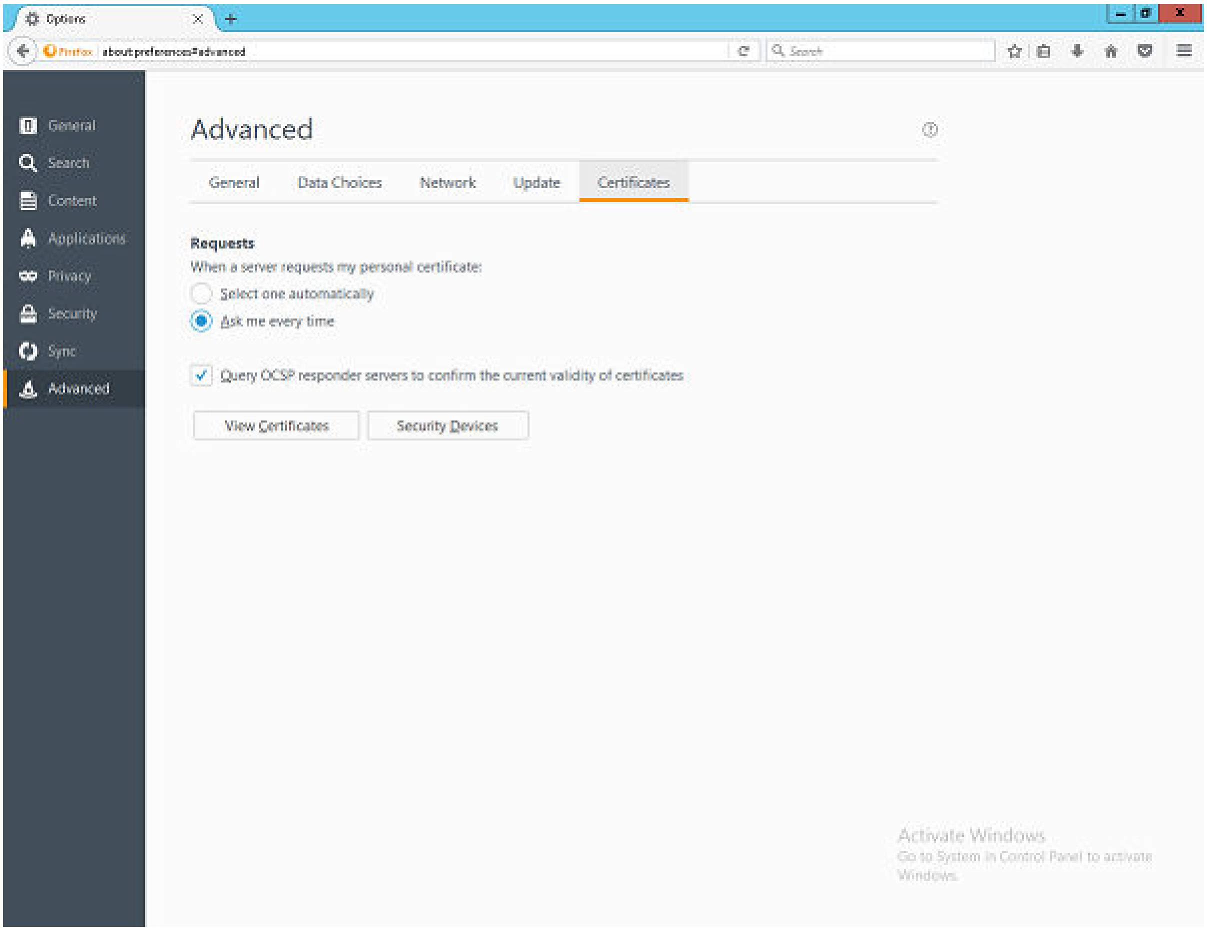
Firefox is not your default browser

When Firefox starts: Show my home page

Home Page: Mozilla Firefox Start Page

Figure 42. General Tab

3. In the left pane of the **Options** page, click **Advanced** tab and then click **Certificates** option.



Advanced

Requests

When a server requests my personal certificate:

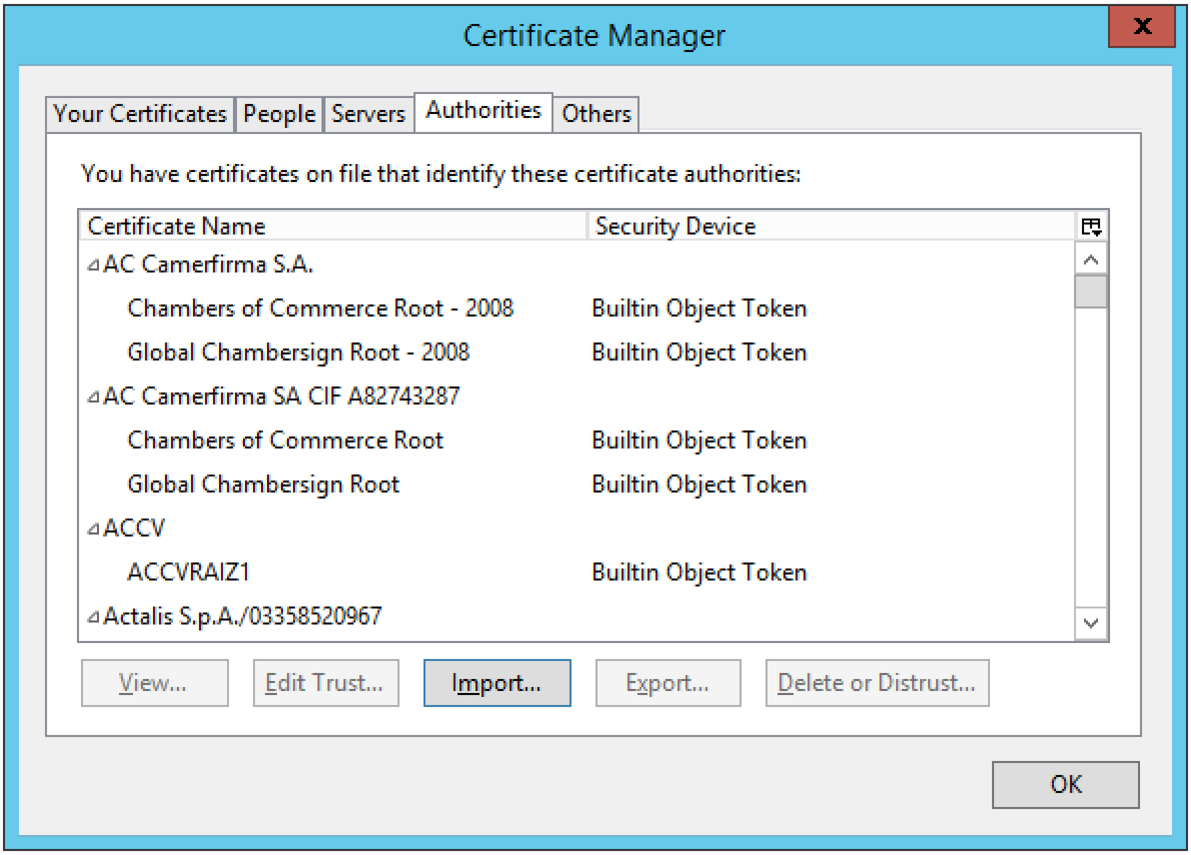
○ Select one automatically

● Ask me every time

☑ Query OCSP responder servers to confirm the current validity of certificates

Figure 43. Advanced

4. Click **View Certificates** to open the Certificate Manager window.
5. Select the **Authorities** tab on the **Certificate Manager** window and click **Import**.



You have certificates on file that identify these certificate authorities:

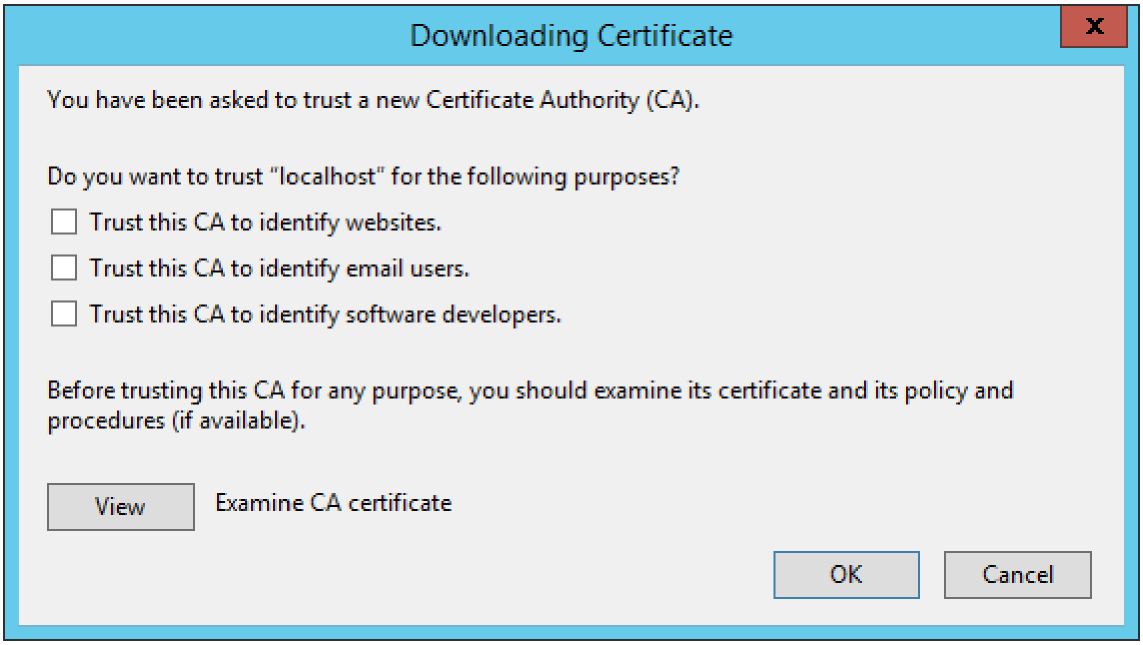
Certificate Name	Security Device
◿AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
◿AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token
◿ACCV	
ACCVRAIZ1	Builtin Object Token
◿Actalis S.p.A./03358520967	

Figure 44. Certificate Manager

6. In the file browser dialog navigate to the location where WDM is installed, For example: \Wyse\WDM\TeraDici, where the root path can be C:\Program Files (x86) based on the operating system and installation path.

   NOTE: In some cases if the Teradici components are installed in a custom manner or manually configured, the above steps must be followed on the same device, and the standard installer path may not be applicable. In such case navigate to corresponding root path where Teradici folder is available.

7. Select the file with the name **cert.pem** and then click **Open**.
8. Now click the **View** button in the **Downloading Certificate** window.



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "localhost" for the following purposes?

☐ Trust this CA to identify websites.

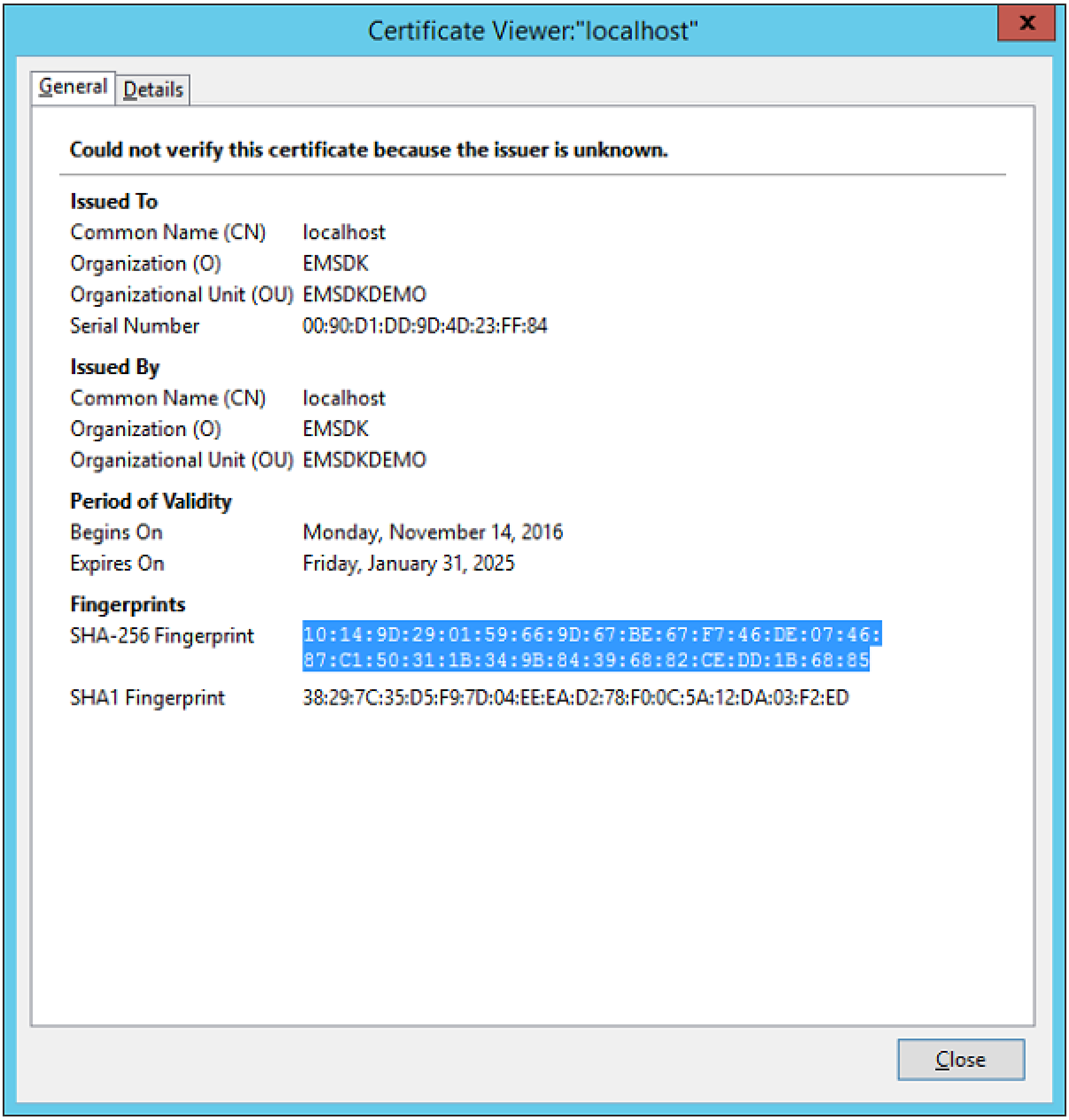
☐ Trust this CA to identify email users.

☐ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Figure 45. Downloading Certificate

9. Copy the sha256 fingerprint value. Click **Close** and cancel all the firefox windows.



Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	localhost
Organization (O)	EMSDK
Organizational Unit (OU)	EMSDKDEMO
Serial Number	00:90:D1:DD:9D:4D:23:FF:84

Issued By

Common Name (CN)	localhost
Organization (O)	EMSDK
Organizational Unit (OU)	EMSDKDEMO

Period of Validity

Begins On	Monday, November 14, 2016
Expires On	Friday, January 31, 2025

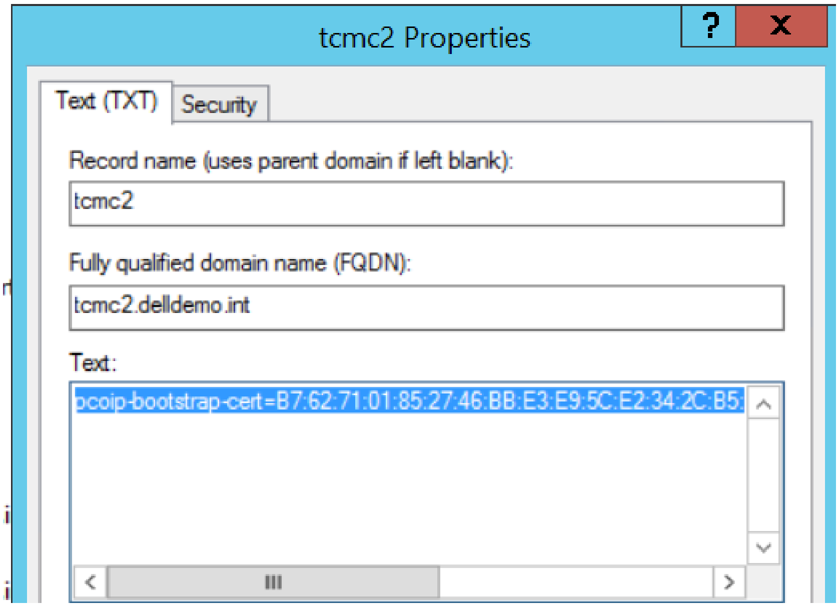
Fingerprints

SHA-256 Fingerprint	10:14:9D:29:01:59:66:9D:67:BE:67:F7:46:DE:07:46: 87:C1:50:31:1B:34:9B:84:39:68:82:CE:DD:1B:68:85
SHA1 Fingerprint	38:29:7C:35:D5:F9:7D:04:EE:EA:D2:78:F0:0C:5A:12:DA:03:F2:ED

Figure 46. Certificate Viewer

NOTE: In the Text field the text must be prefixed with pcoip-bootstrap-cert= to the sha256 fingerprint which is obtained already.

After copying the certificate fingerprint, complete the following stepson the DNS server:



tcmc2 Properties

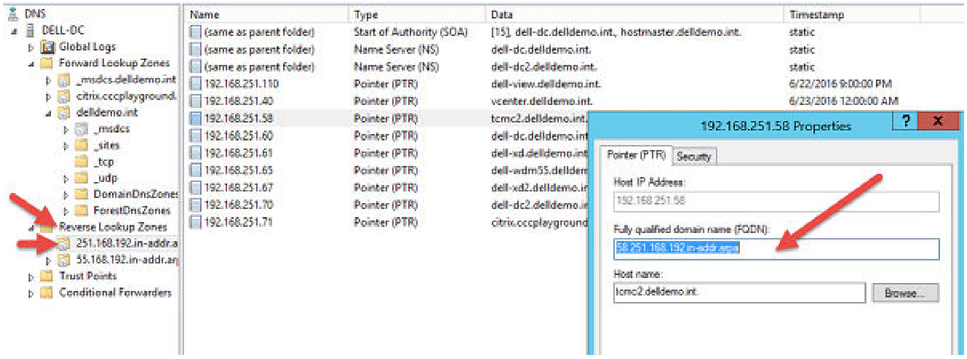
Record name (uses parent domain if left blank):
tcmc2

Fully qualified domain name (FQDN):
tcmc2.delldemo.int

Text:
pcoip-bootstrap-cert=B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C:B5:

Figure 47. tcmc2 Properties

10. The fourth and final record is a reverse PTR record for the management host.



Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[15], dell-dc.delldemo.int., hostmaster.delldemo.int.	static
(same as parent folder)	Name Server (NS)	dell-dc.delldemo.int.	static
(same as parent folder)	Name Server (NS)	dell-dc2.delldemo.int.	static
192.168.251.110	Pointer (PTR)	dell-view.delldemo.int.	6/22/2016 9:00:00 PM
192.168.251.40	Pointer (PTR)	vcenter.delldemo.int.	6/23/2016 12:00:00 AM
192.168.251.58	Pointer (PTR)	tcmc2.delldemo.int.	
192.168.251.60	Pointer (PTR)	dell-dc.delldemo.int	
192.168.251.61	Pointer (PTR)	dell-xd.delldemo.int	
192.168.251.65	Pointer (PTR)	dell-wdm55.delldem	
192.168.251.67	Pointer (PTR)	dell-xd2.delldemo.in	
192.168.251.70	Pointer (PTR)	dell-dc2.delldemo.in	
192.168.251.71	Pointer (PTR)	citrix.cccplayground	

192.168.251.58 Properties

Host IP Address:
192.168.251.58

Fully qualified domain name (FQDN):
58.251.168.192.in-addr.arpa

Host name:
tcmc2.delldemo.int.

Figure 48. PTR Record

11. The zone must match the subnet that the host is in, and the record is the IP address assigned to the Teradici Device Proxy (HAProxy).

GUID-398EA939-B93D-40D4-B8AC-5D2714138169

Installing and configuring HAProxy

HAProxy which is the load balancer for ThreadX 5x devices is configured on Ubuntu Linux version 16.04.1 with HAproxy version 1.6.

Follow the steps to install and configure HAproxy on Ubuntu Linux machine:

Reference link: https://haproxy.debian.net/#?distribution=Ubuntu&release=precise&version=1.6

1. Log in to Ubuntu machine by providing the user credentials used during the installation of Ubuntu operating system.
2. Open the terminal and execute the following commands to install HAProxy:

   - sudo apt-get install software-properties-common
   - sudo add-apt-repository ppa:vbernat/haproxy-1.6
   - sudo apt-get update
   - sudo apt-get install haproxy

3. Execute the following commands to configure HAProxy:

   - Back up original configuration before editing, with the command sudo cp /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy.cfg.original
   - Now edit the configuration file with the command sudo nano /etc/haproxy/haproxy.cfg
   - In the configuration file edit the following sections as per the requirement:
     - Global section: Maxconn <maximum number of connections>
     - Frontend tcp-in: bind <HAProxy server IP>:5172
     - Back end servers: server <server alias name> <Teradici Device Proxy server IP>:5172
     - maxconn <maximum number of connections per Teradici Device Proxy server>

     NOTE: For achieving high availability, administrator may add additional back end servers beyond the total number of clients capacity to have seamless fail over.
   - After editing the configuration, save it with command Ctrl + O
   - The sample HAProxy configuration is provided as follows:

```
global
log /dev/log local0
log /dev/log local1 notice
chroot /var/lib/haproxy
daemon
#maxconn is maximum allowed connections
maxconn 50000
defaults
log global
mode tcp
timeout connect 5000ms
timeout client 50000ms
timeout server 50000ms
errorfile 400 /etc/haproxy/errors/400.http
errorfile 403 /etc/haproxy/errors/403.http
errorfile 408 /etc/haproxy/errors/408.http
errorfile 500 /etc/haproxy/errors/500.http
errorfile 502 /etc/haproxy/errors/502.http
errorfile 503 /etc/haproxy/errors/503.http
errorfile 504 /etc/haproxy/errors/504.http
frontend tcp-in
#replace IP with IP of your Linux proxy machine
```

```
bind 10.150.99.102:5172

default_backend servers

backend servers

#Add your multiple back end windows machine IP with 5172 as port

# maxconn represents number of connection- replace 10 with limit #(below 20000)

# server1 server2 are just names and not keywords

server server1 10.150.99.107:5172 maxconn 10

server server2 10.150.99.107:5172 maxconn 10
```

4. Now validate the HAProxy configuration file with the command sudo haproxy –f /etc/haproxy/haproxy.cfg –c.

   If configuration is valid the following message will be shown:

   Configuration file is valid
5. Now restart HAProxy service by using the following command:

   Sudo service haproxy restart
6. **Command to stop the HAProxy service**

   Sudo service haproxy stop
7. **Command to verify the version of HAProxy**

   Sudo haproxy –f
8. **Command to uninstall HAProxy**

   Sudo apt-get remove haproxy

   or

   Sudo apt-get purge –auto-remove haproxy

GUID-8B851175-579E-4F23-8E25-81F5E2CC4869

Installing Teradici Device Proxy Servers

Teradici Device Proxy servers can be installed on the servers which run the following operating systems:

- Windows 2012
- Windows 2012 R2
- Windows 2008 R2 x64bit

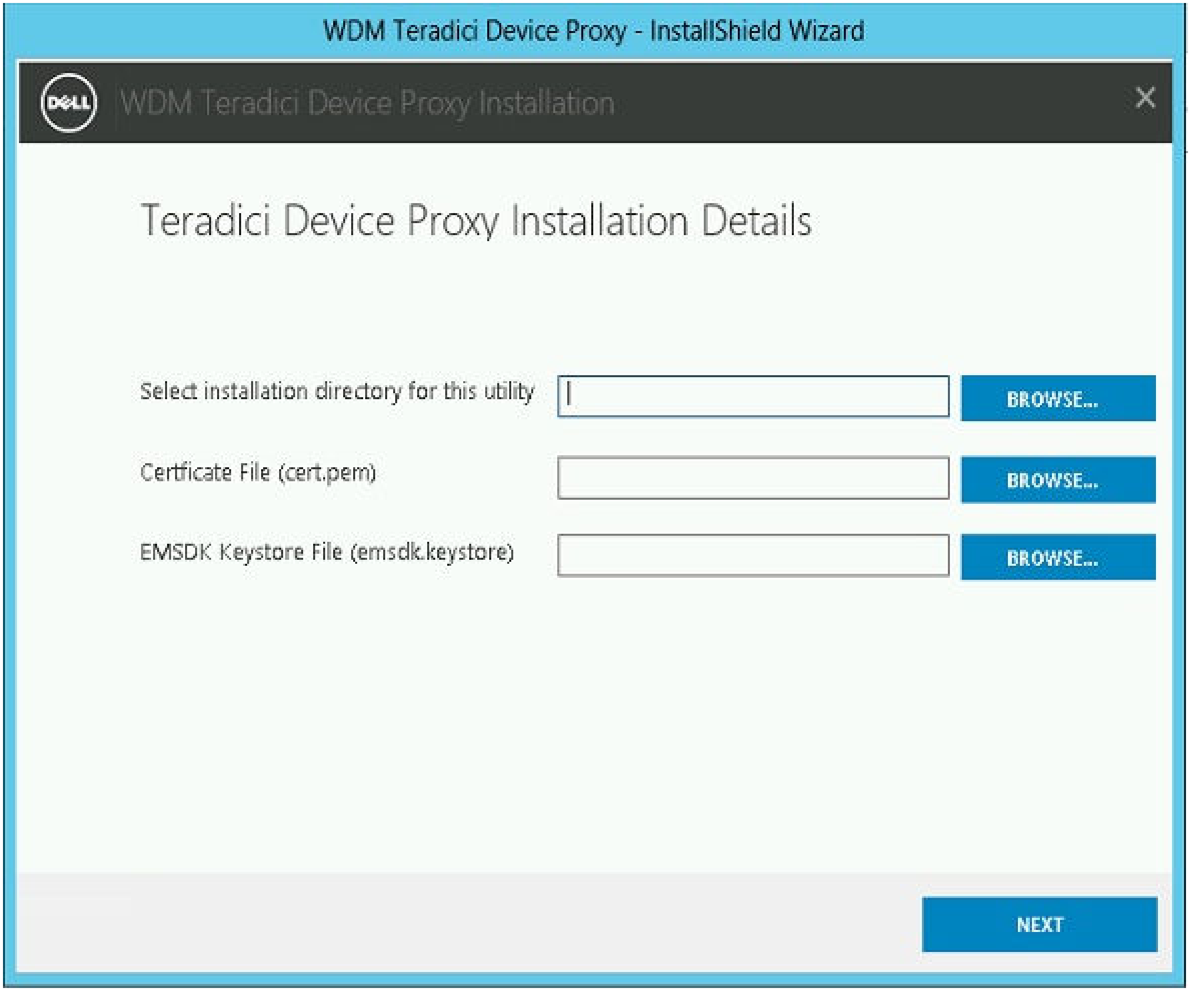
Follow the steps provided to install Teradici Device Proxy service:

1. Log in to the system as administrator.
2. Copy the **WDM installer** folder to the target machine.
3. Go to **TeradiciDeviceProxy** folder.
4. Double click the WDMTeradiciDeviceProxy.exe file to install the same.
5. Provide the following inputs:

   a. Select the path where you want to install Teradici Device Proxy and its dependent components.

   b. Select Cert.pem file from the folder **<WDM installed location>\Teradici** on the machine where **ThreadX 5X** component is selected while installing WDM.

c. Select **emsdk.keystore** file from the folder **<WDM installed location>\Teradici\EMSDK\config** on the machine where **ThreadX 5X** component is selected while installing WDM.



WDM Teradici Device Proxy - InstallShield Wizard

WDM Teradici Device Proxy Installation

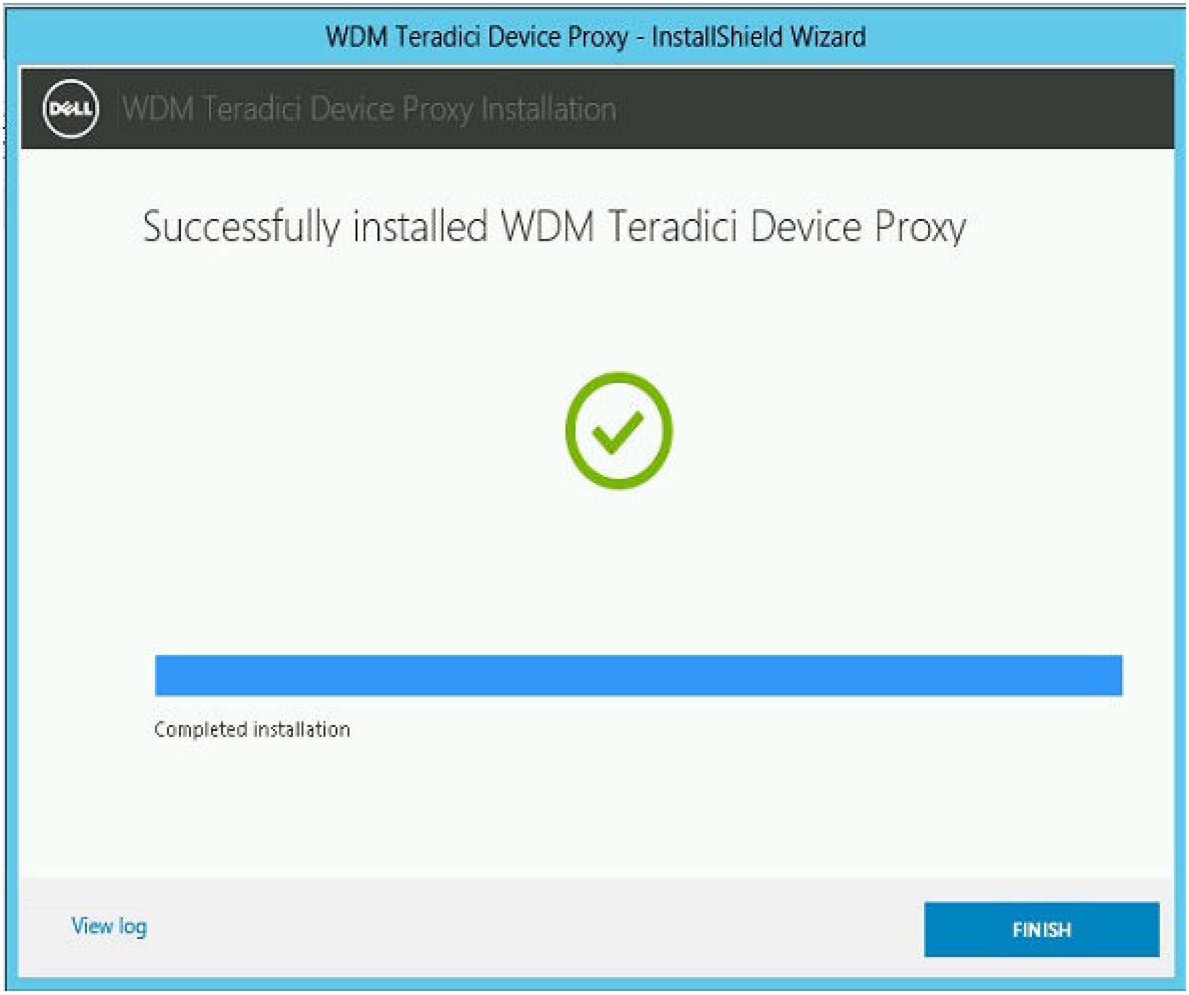
Teradici Device Proxy Installation Details

Select installation directory for this utility

Certficate File (cert.pem)

EMSDK Keystore File (emsdk.keystore)

6. Provide the required inputs and click **Next**.



WDM Teradici Device Proxy - InstallShield Wizard

WDM Teradici Device Proxy Installation

Successfully installed WDM Teradici Device Proxy

Completed installation

7. Click **Finish**.
8. The install log will be created at <EMSDK Installed location>\Teradici\Detail_TeradiciDeviceProxy.log.
9. Click the **Start menu** → **Administrative tools** → **Services**.
10. Verify ThreadX 5x Manager Windows Service is installed and running.

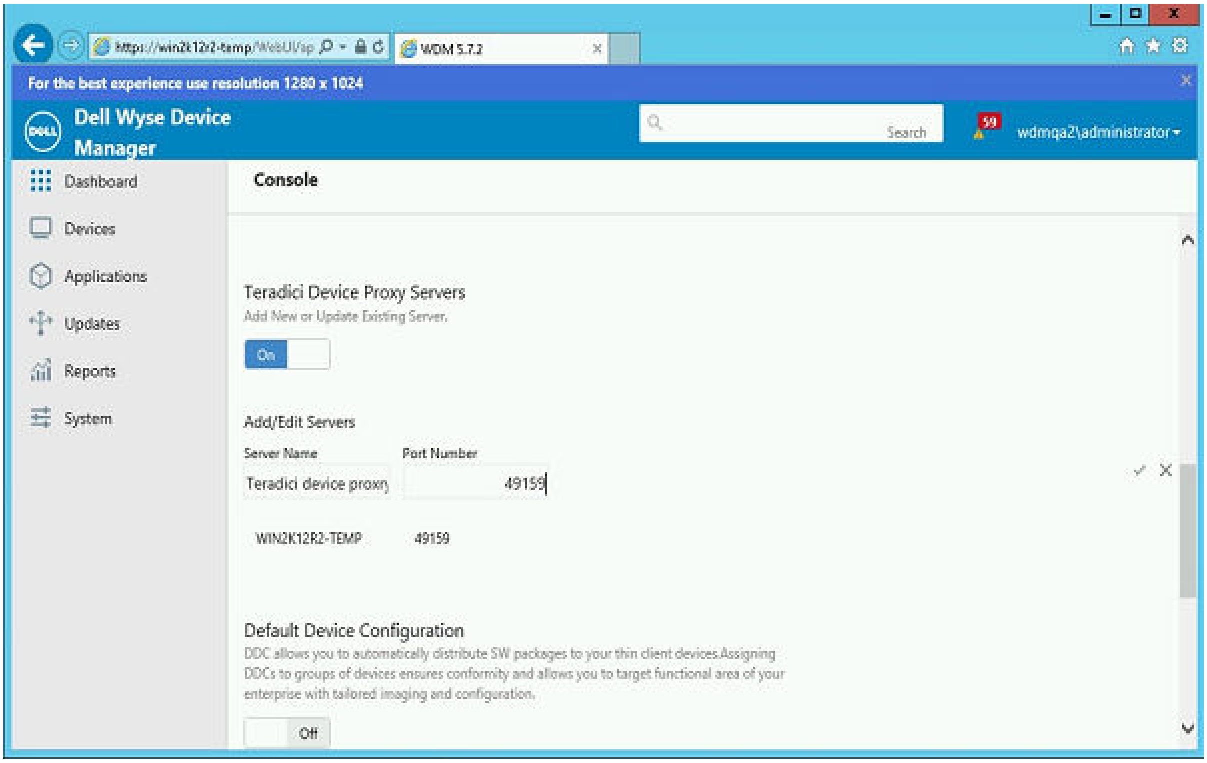
GUID-1F1F0F08-1799-4424-8681-339D80B2E193

Adding Teradici Device Proxy Servers to WDM

Follow the steps provided to add Teradici Device Proxy Servers to WDM:

1. Open WDM Web UI and log in as administrator.
2. Go to **System** → **console** and enable **Teradici Device Proxy servers** option.
3. Click **Add Server**.
4. Add the Teradici Device Proxy server name in the **server name** field and give port number of the Teradici Device Proxy service in the **port number** field. The default value is 49159.

   NOTE: If the default port number is changed, it must be updated in WDM. Please refer the *WDM 5.7.2 Admin guide.*



For the best experience use resolution 1280 x 1024

Console

Teradici Device Proxy Servers

Add New or Update Existing Server.

On

Add/Edit Servers

Server Name	Port Number
Teradici device proxy	49159
WIN2K12R2-TEMP	49159

Default Device Configuration

DDC allows you to automatically distribute SW packages to your thin client devices.Assigning DDCs to groups of devices ensures conformity and allows you to target functional area of your enterprise with tailored imaging and configuration.

Off

5. Click on the **Check Mark** on the right hand side of the text boxes to save the values.

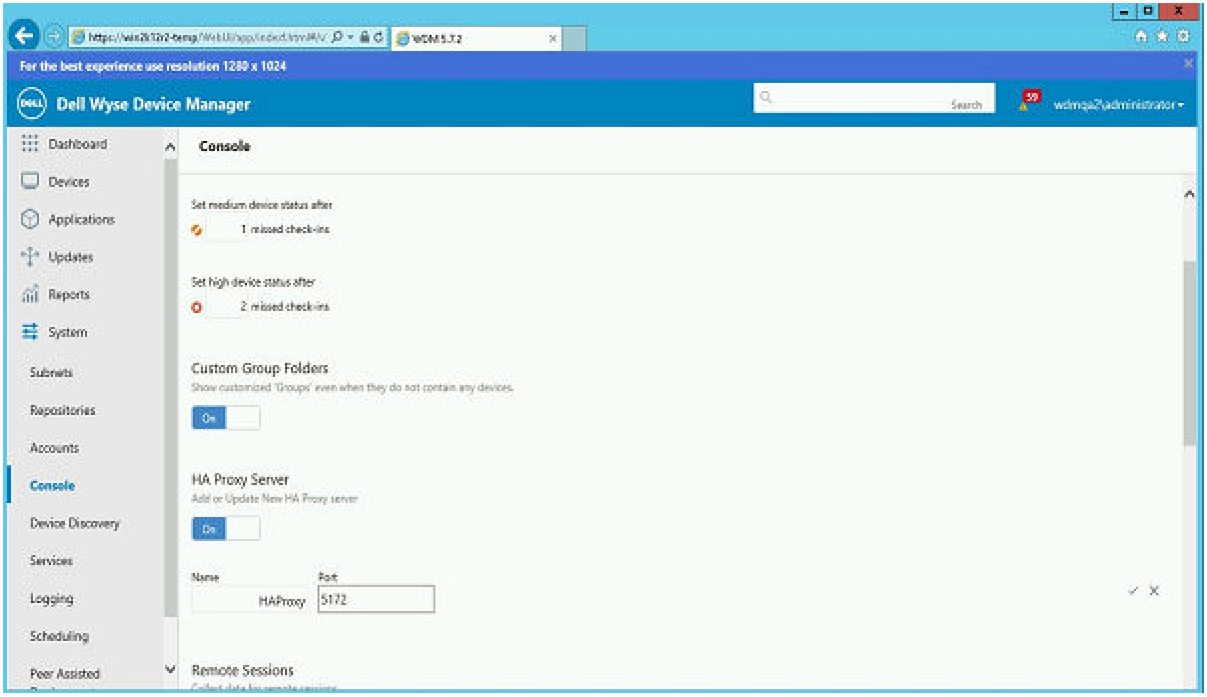
GUID-F9A5DD5F-8612-41D2-85BA-B7BDA44E9DF4

Adding HAProxy to WDM

Follow the steps provided to add HAProxy to WDM:

1. Log in to WDM Web UI as administrator.
2. Go to console page and enable **HAProxy Server** option.
3. Click **Add Server**.
4. Add the HAProxy Server name in the server name field and give port number as 5172.

5. Click **Add Server** again.



Console

Set medium device status after

1 missed check-ins

Set high device status after

2 missed check-ins

Custom Group Folders

Show customized 'Groups' even when they do not contain any devices.

On

HA Proxy Server

Add or Update New HA Proxy server

On

Name: HAProxy

Port: 5172

Remote Sessions

6. Click on the check mark on the right hand side of the text boxes to save the values.

GUID-82113E1B-2964-4809-B588-F8BF3EC699F5

Restarting Threadx API

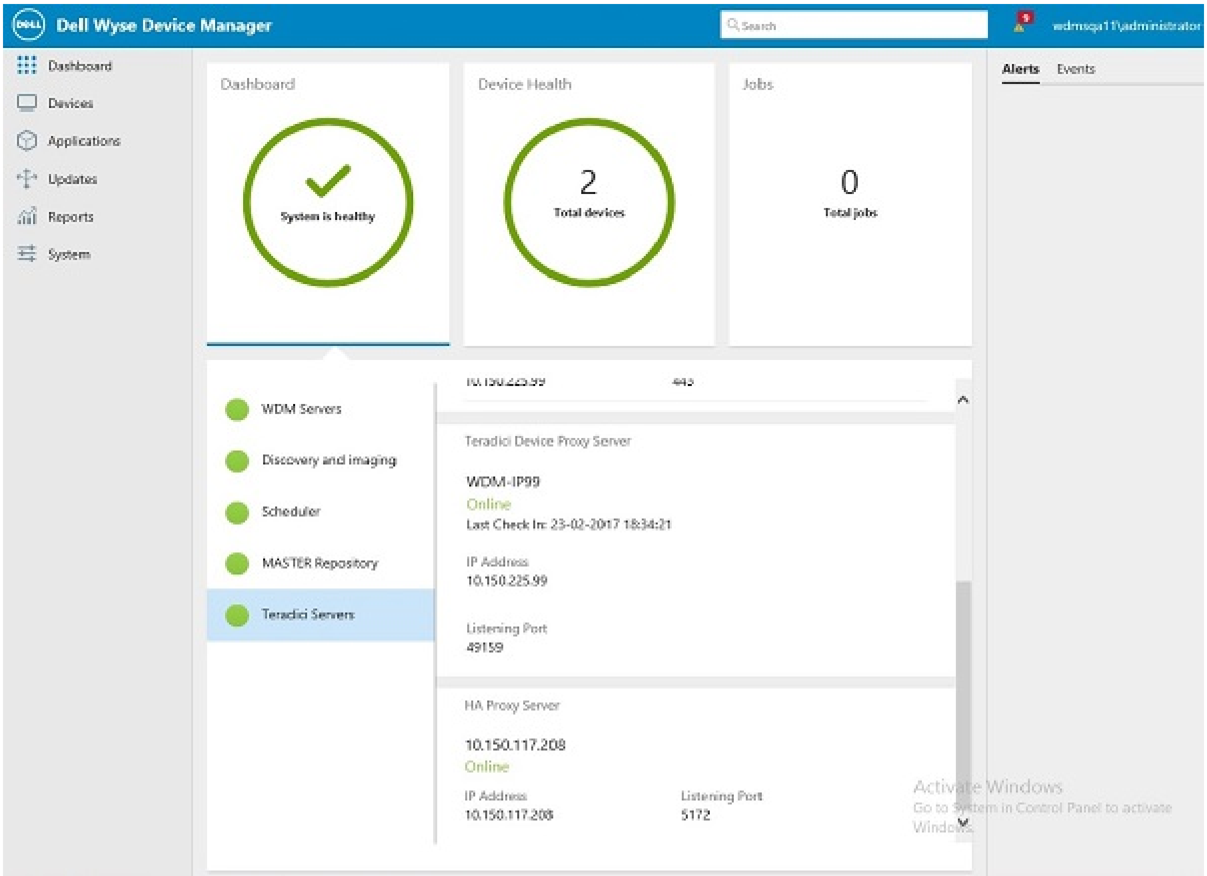
Follow the steps provided to restart Threadx API:

1. Log in to the server where WDM ThreadX 5x component is installed.
2. Click the **Start menu** → **Administrative tools** → **Internet information service (IIS) manager.**.
3. Expand the root node (host name of the server) and select **Application pools** → **ASP .Net v4.0**.
4. Right click **ASP .Net v4.0** and select **Stop**.
5. Again right click **ASP .Net v4.0** and select **Start**.
6. Open WDM web UI and login as administrator.
7. Verify the status using the dashboard.

GUID-7A522D24-B585-4A3F-9599-6CEF32764EFD

Verify status from Dash board

1. Click on dash board and Select Teradici Servers.
2. Verify that Thread5x, Teradici HAproxy and Teradici Device proxy server status are Online.



10.150.225.99 443

Teradici Device Proxy Server

WDM-IP99
Online
Last Check In: 23-02-2017 18:34:21

IP Address
10.150.225.99

Listening Port
49159

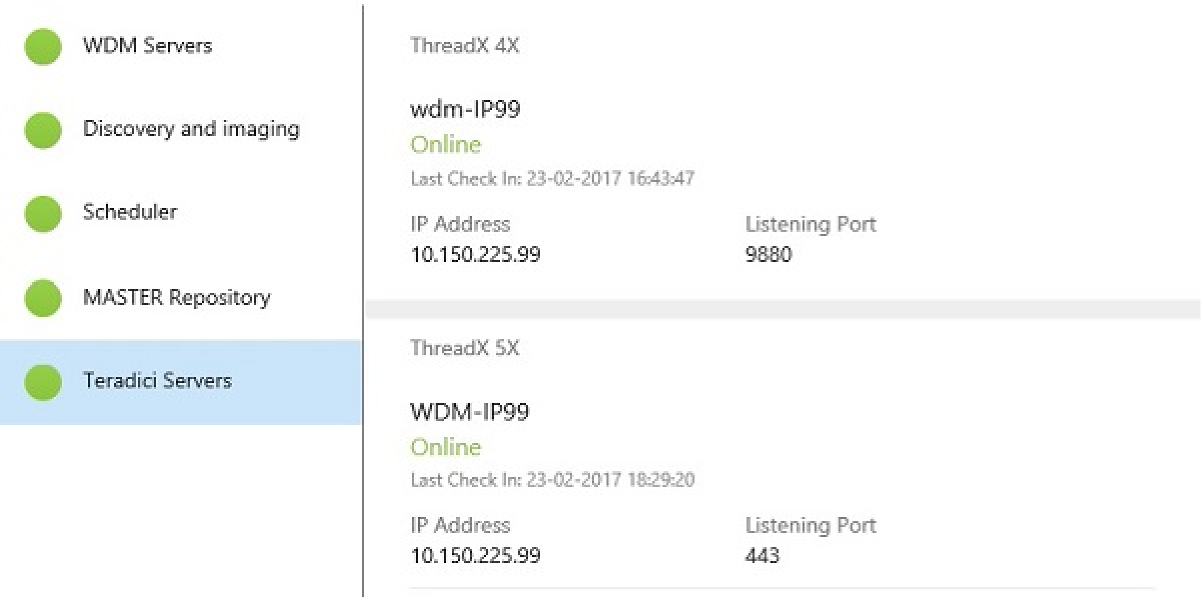
HA Proxy Server

10.150.117.208
Online

IP Address
10.150.117.208

Listening Port
5172

Figure 49. Status on Dashboard



ThreadX 4X

wdm-IP99
Online
Last Check In: 23-02-2017 16:43:47

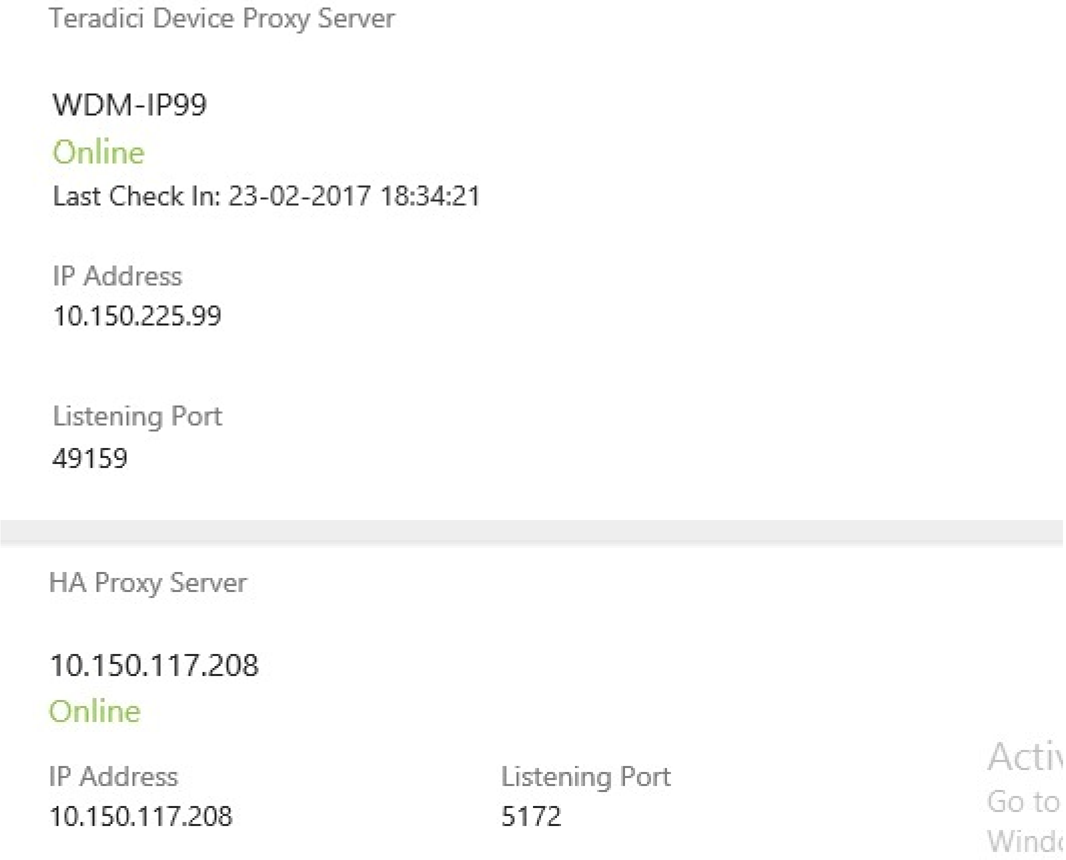
IP Address	Listening Port
10.150.225.99	9880

ThreadX 5X

WDM-IP99
Online
Last Check In: 23-02-2017 18:29:20

IP Address	Listening Port
10.150.225.99	443

Figure 50. Status on Dashboard



Teradici Device Proxy Server

WDM-IP99

Online

Last Check In: 23-02-2017 18:34:21

IP Address

10.150.225.99

Listening Port

49159

HA Proxy Server

10.150.117.208

Online

IP Address	Listening Port
10.150.117.208	5172

Figure 51. Status on Dashboard

GUID-E660BA4F-137A-4D32-82B1-6159CC886736

7

Manual installation of WDM database using scripts

This section contains database scripts supported by Wyse Device Manager (WDM) and related functionality details.

CONCEPT-13-9B7B8096

Requirements

Existing WDM database support

WDM installation supports SQL Server 2008. The database contains all the SQL server objects such as tables, views, stored procedures, and so on. The WDM installer stores the database to the respective folder (default is: C:\Program Files (x86)\Wyse \WDM\Database) and attaches the same to server machine where WDM needs to be install.

Then the installer updates the server details, user details, Software Repository configuration details, and so on to the server machine.

CONCEPT-14-9B7BAFBB

Proposed way of installing WDM database

Provided scripts are used to install WDM database version 5.7.

Prerequisites—Before executing the scripts, the database path folder must be created and firewall must be disabled in the database server.

NOTE: The following scripts must be executed in the same order as they are mentioned. If not, you have to delete the database and repeat the entire process again.

GUID-2FDC0585-3B1E-47CF-B454-1120E3000336

Script files

The following database script files will be used to install database of WDM 5.7:

- CreateDatabase.sql
- Schema&User.sql
- Tables.sql
- Userdefinedtables.sql
- Views.sql
- Stored_Procedures.sql
- Default_Table_Data.sql
- CustomizeScript.sql

CreateDatabase.sql

To create the database manually, execute the following script:

NOTE: The database scripts are mentioned here for customization purpose.

```
CREATE DATABASE [RapportDB]

ON PRIMARY

(NAME = N'Rapport_dat', FILENAME = N'C:\Program Files (x86)\Wyse\WDM\Database\Rapport4.MDF,
SIZE = 42496KB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%)

LOG ON

(NAME = N'Rapport_log', FILENAME = N'C:\Program Files (x86)\Wyse\WDM\Database
\Rapport4.LDF', SIZE = 768KB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%)

GO
```

1. The script file contains RapportDB Database creating scripts.
2. User or Administrator can change the file path. Default file path is C:\Program Files (x86)\Wyse\WDM\Database.

   NOTE: Check the above mentioned folder to verify the step. This folder should contain Rapport4.mdf and Rapport4.ldf.

Schema&User.sql

To create a user account execute the script. You can add and assign permission to any user account.

1. The script file contains the details about creating schema and User role.
2. The default values are rapport schema and rapport user. If you want to change the WDM access user, you can change from here.

Tables.sql

This script file contains script for all table objects and constraints.

NOTE: Custom changes are not included in this file.

Userdefinedtables.sql

This script file contains script for all the User Defined Table objects.

NOTE: Custom changes are not included in this file.

Views.sql

This script file contains script for all View objects.

NOTE: Custom changes are not included in this file.

Stored_Procedures.sql

This script file contains script for all Stored Procedure objects.

NOTE: Custom changes are not included in this file.

Default_Table_Data.sql

This script file contains script for all Default Table Data values such as, OS, Platform, Management Type, Default Groups, Default Software Packages, Default Parm details, and so on.

NOTE: Custom changes are not included in this file.

CustomizeScript.sql

This script file contains script for Customize Data values.

Provide the database server name while executing the following script. An error is displayed, if you do not enter the server name.

NOTE:

---- Customize Script

```
Use RapportDB
Go
SET IDENTITY_INSERT [dbo].[License] ON
INSERT [dbo].[License]
([LicenseID], [Sales], [UnActivated], [Code], [License], [Utilize], [NumberOfClients],
[VendorID])
VALUES
(1, N'7V931PHY08K01LZHYXWKKP6GQ1', N'BR69T51SSP500PFW9W4R0Z0TL5', NULL, NULL, NULL, NULL,
NULL)
SET IDENTITY_INSERT [dbo].[License] OFF
GO
SET IDENTITY_INSERT [dbo].[sysHash] ON
INSERT [dbo].[sysHash] ([ID], [Hash]) VALUES (2,
0x4458473935334D315130345252545246434753383434424858 36)
SET IDENTITY_INSERT [dbo].[sysHash] OFF
Go
Begin
Declare @DBServerName varchar(200) = ''
Set @DBServerName = ''
If (@DBServerName is null or @DBServerName = '')
Begin
RAISERROR(N'Database Server Name Should not be Empty...', 16, 1)
End
Else
Begin
SET IDENTITY_INSERT [dbo].[Install] ON
INSERT [dbo].[Install]
([InstallID], [Module], [ServerName], [UserName], [Installed], [Status], [Information],
[RegKey], [RegName], [RegValue], [LatestHFID], [SiteID], [SiteName])
VALUES
(0, N'Rapport4DB', @DBServerName, N'administrator', GetDate(), N'MASTER', NULL, NULL, NULL,
NULL, N'00HF05070001516', 0, NULL)
SET IDENTITY_INSERT [dbo].[Install] OFF
End
End
Go
```

GUID-6DEAFAE5-586B-4B12-AC67-5FE033ABD362

Upgrading WDM using database scripts

To upgrade from WDM 5.7 to WDM 5.7.2, do the following:

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 go to WDMv5.7.2_GA\SQL path.
3. Execute the scripts in the following order:
   - `CommonTables.txt`
   - `CommonStoredProcs.txt`
   - `Tables.txt`
   - `StoredProcs.txt`

GUID-FAFC4809-DB30-4FB7-99AF-1AE3A80F51BC

8

Troubleshooting

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

GUID-A74DFC00-88C0-457A-9B67-2BD38395A266

.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 Sever 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.

GUID-BD2A305A-5A9C-4088-877B-14623A926C63

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.

GUID-30C90F4C-5F33-4B37-BB2C-E723F08C8254

Error While Installing WDM Database in a Distributed Setup

Issue: When you are installing the WDM Database on a separate system that has the supported version of SQL Server installed on it, then the following error may be displayed when you launch the **Setup.exe** : *Setup was unable to initialize the required libraries.*

Resolution: Make sure that the **Microsoft Visual C++ Redistributable 2008**, **version 9.0.21022** is installed. You need to navigate to **Start** → **Control Panel** → **Programs** to view if the redistributable is installed. If it is not installed, then you must manually install it by running the **vcredist_x86.exe** available under the **Prereq** folder of the WDM Installer.

GUID-BB4AF8CB-E6FC-4F7C-9FEF-0E6C599DF265

Database Installation Failure After Manual Uninstallation of SQL Server Express 2014

Issue: The WDM database installation fails after you manually uninstall the existing SQL Server Express 2014, and use the **Install New Database** option in the installer.

Resolution: To resolve this issue:

1. Uninstall SQL Server Express 2014 R2 from Add\Remove Programs.
2. Launch the **Services** window from **Control Panel** → **Administrative Tools**.
3. Delete the **MSSQL$RapportDb** Service

   .
4. Delete **MSSQL12.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.

GUID-442F1C0A-2584-42E0-9E3A-DA828C76E11B

After Upgrading from WDM 5.5.1 to WDM 5.7 Software Repository is not Secure

Issue : If WEB UI is selected during Upgrade, then Management server will be configured to Https, But WDM Software repository will not be configured by the installer.

Resolution : Manually Set the Software repository to HTTPs in the WDM GUI. To set manually, go to **Configuration Manager Software Repository**.

GUID-1BBD711E-DD78-465F-9574-76C25BA1B02F

Troubleshooting Post Deployment

Issue : HTTP Error 404.0 – Not Found. the Web.config of the HApi shall be added with a url routing module if it’s missing:

Resolution : Add the Web.config of the HApi with a URL routing module as follows:

```
<system.webserver>
<modules>
<remove name= "urlroutingmodule-4.0"/>
<add name= "urlroutingmodule-4.0" type="system.web.Routing.urlroutingmodule"
precondition="" />
</modules>
```

GUID-82ED96F4-1A02-4318-B24E-98A25C4550B7

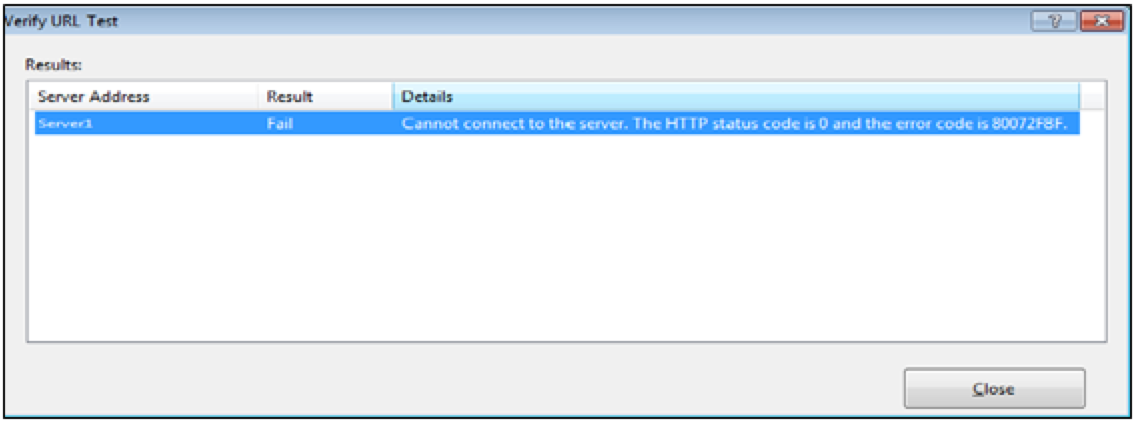
Troubleshooting Load Balancing Issues

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

GUID-FDC5106D-3FA2-464D-896C-0747F1D2C48C

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.



Server Address	Result	Details
Server1	Fail	Cannot connect to the server. The HTTP status code is 0 and the error code is 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.

GUID-183E8E99-7976-4DBD-B585-1FE11BC36817

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>
```

GUID-DBA7BB21-ECFF-4200-B5CB-CCA2712F3616

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

GUID-7DA71B0C-E311-4BC8-8AD5-FE9FC8A5C2EC

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**.

..

GUID-70C13F27-BF3A-41B8-A956-F5D24B610962

Indefinite Preceding during Installation

Issue: Installation proceeds indefinitely while installing Microsoft Visual C++ Redistributables or Microsoft SQL Express 2008. The OS Supported are Windows 2012 Standard and Windows 2012 R2.

Resolution: Open the Task Manager, and check whether the '**Windows Modules Installer Worker**' process is running on your thin client or not. If this process is running, you must end the process for installation to resume. Restart the thin-client after the installation is complete.

GUID-E4D7093E-6813-4B3E-B4EC-EB543019BDFA

Load Balancer Issue

Issue: Proxy Server does not respond if the IP V6 Address is enabled.

Resolution: Disable the IP V6 Address of the Load Balancer Setup.

GUID-F5B8454B-BF9E-4D67-9F5C-4C3D75015F89

Upgrading WDM on Windows 2008 SP2 32 bit

Issue: To upgrade WDM 5.7 on Windows 2008 SP2 32 bit, enable the Windows Update service.

Resolution: To upgrade WDM 5.7 on Windows 2008 SP2 32 bit, enable the Windows Update service to install the Hotfix KB980368. After the installation of Hotfix KB980368, disable the Windows Update Service to install the WDM 5.7.

GUID-21AF881B-53EE-4686-A4C8-6B54396C2567

WDM Upgrade Installation Fails

Problem: WDM Upgrade installation fails while connecting to software repository.

Resolution: One of the reason for this issue is, the Computername for the setup has more than 16 characters. This brings out a mismatch in Computername and NetBIOS name (truncated to 15 chars) for the setup. To confirm this issue, check if the above mentioned system variables are different. If yes, install WDM on a setup which has hostname to a max of 15 characters, and then re-run upgrade installer.

GUID-2A1382E1-EB00-4364-A06D-1DE6E5E46501

Configuration Error After Upgrading from WDM 5.7 to WDM 5.7.2

Issue: After you install WDM successfully and reboot the system, the following services are configured to run under dedicated account, but do not start due to a logon failure. Such as,

- ThreadX Manager
- Recurring Schedule
- HServerInit
- WDM DHCP Proxy

Reason: Installer failed to provide 'Log On As A Service' right to the user account.

Resolution: Manually configure the user account to have 'Log On As A Service' permission.

GUID-86152FE1-EECE-474F-9F9B-38545B3DF7CD

Cloud Environment Setup Issue

Issue: An error message is displayed intermittently when you run the `setup.exe` file during WDM installation in the cloud environment.

Resolution

- **Scenario 1– Only the error message is displayed**

  Close the dialog box displaying the error message, and then run the `setup.exe` file again.
- **Scenario 2– An error message is displayed along with the Welcome Screen running in background**

  Close the dialog box displaying the error message and the Welcome screen, and then run the `setup.exe` file again.

GUID-0335A4B8-4510-4269-A20F-D92EA95BEBD0

Error in Installation of WDM in Upgrade Setup

Issue: During the installation of WDM, if you use different database user other than the default user, then you will not be able to proceed with the installation of WDM in Upgrade setup. **Unable to proceed with the installation, aborting installation** error message is displayed.

Solution:

- Open WDM GUI.
- Right click **Configuration Manager** and select **Utilities** → **Database Credential Manager**.

- A warning message is displayed. Click **OK**.
- Enter the user name and password of the user used when you installed WDM. Click **Ok** to continue.
- Now close the WDM GUI and proceed with the installation.
- After installation, run the **Database Credential Manager** available in the Install path (`C:\Program Files(X86)\Wyse\WDM\Utilities\Database`) again.
- Provide your username and password used when you installed WDM, and then reboot the server.