Dell Wyse Device Manager

Version 5.7.2 Administrator's 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. A02

Contents

1

Introduction

Dell Wyse Device Manager (WDM) software is the premier enterprise solution for managing Dell Wyse thin and zero clients simply, remotely, and securely. It enables IT professionals to easily organize, upgrade, control, and support thousands of Windows Embedded, Wyse Enhanced Linux, Wyse ThinLinux, Wyse ThinOS, Wyse ThinOs Lite, and PCoIP zero client devices (ThreadX devices) across any LAN, WAN, or wireless network.

The software uses industry standard communication protocols and a component-based architecture to efficiently manage your network devices. Dell Wyse Device Manager (WDM) includes an easy-to-use UI that enables you to easily perform all the device management functions that are required to run and maintain your WDM Environment. You can access WDM UI using any of the supported browsers from anywhere and can also perform all operations from web UI. The Web UI is user friendly and enables you to perform all the device management functions easily.

Topics:

Key Features

The key features of WDM are:

- **Device Discovery** - You can easily configure WDM to discover devices on the network by setting up different subnets or IP ranges. After you configure WDM, you can easily find and automatically add the devices to the system. Once they are added to the system, the devices are available for easy future management.
- **Device Management** - WDM allows you to view the status of your devices at any point time. WDM can be configured as to provide the information automatically about the status update of all your devices.
- **Asset Information Collection** - WDM monitors and stores all asset information about each of the devices that includes hardware asset information and software information that is installed on each device. Software information includes the operating system, and information on all applications and add-ons that have been applied to the device.
- **Remote Control of Devices and Device Shadowing** - You can shutdown, restart, or wake-up devices in the same subnet and wake-up devices across subnets from the remote console. You do not need to visit the end-user desktop. WDM also provides your help desk with a shadowing capability to diagnose issues within end-user environments from a remote location.
- **Device Organization** - WDM is a robust management tool that allows you to organize your devices according to groups that makes the most sense to your organization, regardless of the physical or network location of devices.
- **Profile Manager**- WDM enables you to deploy a predefined configuration on a specified group of devices through profile manager. These configurations are those that you create using the Dell Wyse Configuration Manager (WCM) and store them in a specified repository.
- **Software Deployment and Updates** - WDM allows you to easily deploy and update software and images on devices.
- **Capture and Deployment of Device Software** - With WDM, you can create a reference device which includes the required softwares for installation and to capture that device image. This allows you to clone the device configuration and the software installed on the device across an entire installation.
- **Device Update Scheduling** - WDM configurations allow you to schedule software deployment and updates to devices (preventing down-time). You can schedule device updates immediately, at a pre-determined time, or when a device next boots.

- **Recurring scheduler** - Allows packages to be scheduled repeatedly: daily (or specific weekdays), weekly, and monthly, upto a specific date or for a fixed number of times.
- **Device Configuration Deployment** - You can create different configurations that can be deployed to a device independent of an image.
- **Repository Creation and Administration** - WDM allows you to easily build and administer a repository of software, images, and configuration updates for distribution.
- **Device Views** - With Device Views you can easily view and modify device information, allowing you to generate useful logs and device reports.
- **Distributed Administration** - Provides you with granular control of administrator rights based on user groups or individual users. For example, you can provide Administrator A with rights to view and provide updates to Groups 1, 2, and 3, but not 4; while providing Administrator B with rights to view and provide updates to Group 4 only.
- **Administrator Specified Bandwidth Control** - Allows you to control the bandwidth to be used for server communications (for example, you can configure a server to use a lower bandwidth based on the availability; or configure dial-up connections to be at a lower speed than broadband speed by using a simple profile setup).
- **Restart Failed Updates Option** - Configure and use this option to easily restart failed updates. You can decide the number of times WDM should retry updates (either a package or an image) before it is changed to an error (the number of retries and errors can be viewed in the WDM Console).
- **Default Device Configuration (DDC) Support** - WDM allows you to easily create and manage DDCs. You can apply multiple packages to a device from a single DDC.
- **Add WDM Users** - You can add active directory users or local users in the WDM UI and provide the permissions.
- **Enhanced Report Support** - Following reports are available in WDM Web UI:
  - **Application Reports**—This enables the user to create a report for listing the devices that have specific software installed and version selected by the user
  - **Remote Session Reports**—The Remote session report provides remote session connection information on all the devices.
  - **Log Reports**—This provides important information about the events or activities went into WDM server related to WDM components.

Key features of WDM Enterprise edition

Additional WDM Enterprise Edition features include:

- **Secure Communication between a WDM Server, Repository, and a Device** - Provides secure communications between client and web server by encrypting traffic to and from the client and server and by issuing certificates. Certificates must be signed by an authority which certifies that the certificate holder is the entity it claims to be. Organizations may choose to be their own certificate authority for internal web server access.

  WDM Web UI supports **Federal Information Processing Standards (FIPS)**.
- **Merlin Imaging System** - Provides HTTP, HTTPS, and CIFS based imaging, and provides better performance when deploying large images.
- **Added Scalability with Remote Repositories** - Scale your solution by adding remote repositories to your infrastructure. This functionality allows to use the remote server locations for storing terminal firmware and software. This reduces the amount of network traffic over a wide-area network (WAN) because the bulk of the update traffic (the actual image itself) is transferred only once over the WAN to the Remote Repository. Devices can retrieve the update software from the remote server rather than centralized server. This also increases the speed of the overall update process. WDM still allows you, however, to perform all device management from a central server (for example, from your data center).
- **Distributed Architecture** - This feature allows you to place the WDM components on one or more computers on your network.
- **Default Device Configuration** - This feature allows you to configure default software and device configurations for a group of devices. This functionality ensures that the device conforms to your configurations from a software and device configuration perspective. If there is any deviation from default configurations, WDM reverts the device back to your specified configurations. This feature automates the recovery of failed devices, the re-purposing of existing devices, and the addition of new devices within an existing infrastructure.

- **Expanded Hierarchical Views** - Expand the visual device management capabilities of your WDM server by using this feature to create up to a total of 30 different organizational views of your devices.
- **Automated Grouping** - This feature is used to automatically place any new device that has been added to the system into the predefined groups that you want.
- **Support for Multiple Databases** - Multiple database supports when installing WDM for either an SQL 2008 or 2012 environment, allows you to use your existing back-end infrastructure.
- **Active Directory Integration** - Allows you to easily import WDM user groups or individual users from your existing Active Directory setup.
- **Peer Assisted Deployment** - Peer Assisted Deployment (PAD) is a mechanism that provides updates such as base images and add-ons to thin client devices that are managed through the WDM server. This mechanism works best in an environment where the devices are spread across multiple subnets.

  The PAD feature is applicable to the following platforms:
  - Windows 10 IoT Enterprise
  - SUSE Linux
  - Windows Embedded Standard 7 (WES7)
  - Windows Embedded 8 Standard (WE8S)
  - ThinLinux
- **Profile Manager** - PM enables you to deploy a predefined configuration on a specified group of devices. These configurations are those that you create using the Dell Wyse Configuration Manager (WCM) and save them in a specified repository. The configurations of the Profile manager are unique for an Operating System, and you can apply only one configuration on a single group of devices at any given time.
- **Chargeback Accounting** -

  This feature is supported on Windows, Linux, and Wyse Thin OS (ThinOS) devices. It collects and stores remote session.

Support Information

Table 1. Support information

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

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.

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.

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/.

2

Accessing WDM

To access WDM UI, do the following:

1 Open the supported browser for WDM UI. The following are the supported web browsers for accessing the WDM web UI.
   - Internet Explorer 11
   - Chrome v40 and later versions
   - Firefox v43 and later versions

2 In the browser, enter the following URL:
   https://<WDM Server Host Name/IP Address>/WebUI/app/indexf.html#

3 Press **Enter**.

4 To log into the WDM UI, do the following:
   - By default, you can use the user name that is existing in the WDM UI with the same credentials.
   - Added user can be local or domain user.
     - To log in as a domain user in web UI, you must specify domain name along with username. For example, domainName \Username.

       NOTE: User@domain is not supported.
     - For local user specify only username. For example, **Username**. The **local user** is a user created locally on the machine where the management server is installed.

   NOTE: Clear the cookies and cache before browsing the web UI.

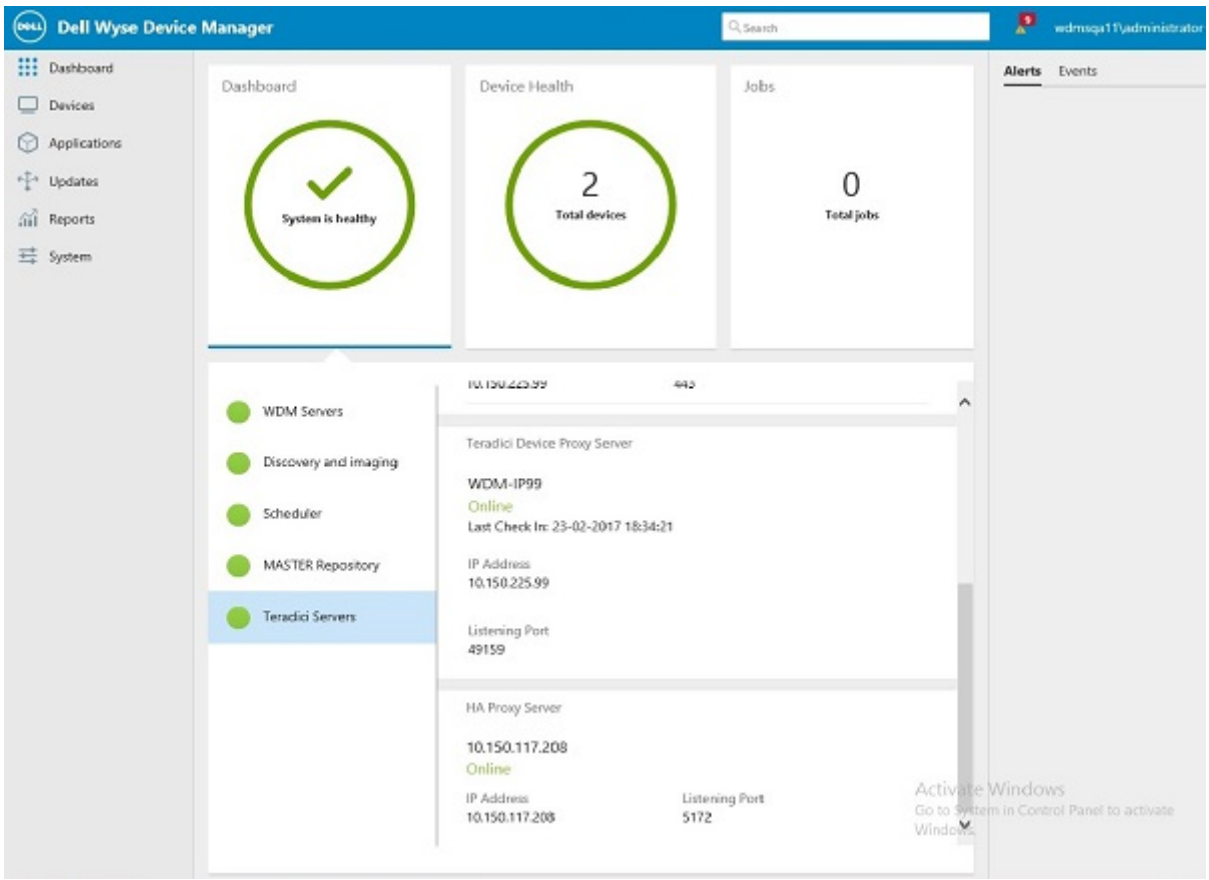
Features of WDM web UI application:

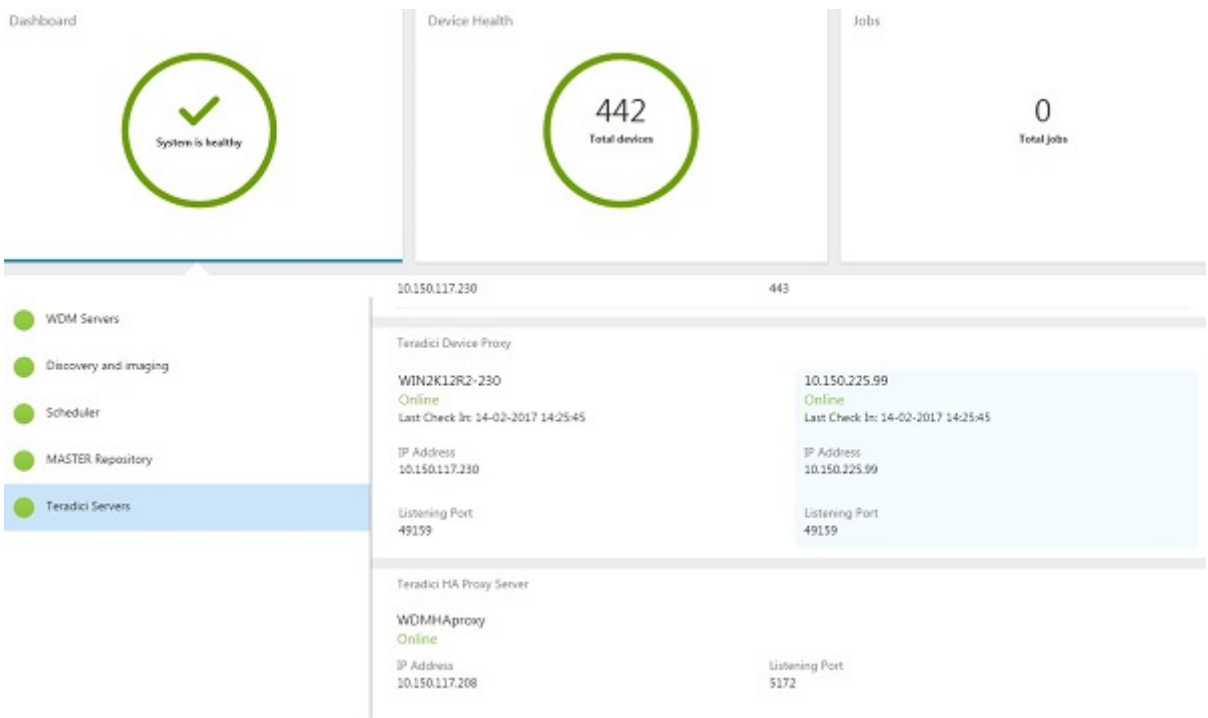
- Dashboard
- Devices
- Application
- Updates
- Reports
- System

3

Dashboard

The Dashboard page allows you to view the details of server status, device health, jobs list, alerts, events and the information about the checked-in server. You can quickly view the summary of the information for each functional area of the system. It displays the information for the following attributes:





Teradici Device Proxy Server

WDM-IP99

Online

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

IP Address

10.150.225.99

- Device Health
- Jobs

The date and time for the last checked-in server is displayed.

You can also view the system updates by clicking the following tabs on the upper right corner of the Dashboard page:

- Alerts
- Events

You must have the administrator privileges to select, deselect and delete the updates. Steps to delete alerts or events is as follows:

- Select an alert or event.
- You can select or deselect the entire list of alerts or events by clicking **Select all** or **Deselect all**.
- Click **Clear** to remove the selected alert or event.

Table 2. Dashboard

Parameter	Description

Server Status	If you click the **Server Status** tile, it displays the status of the server and provides the information about the running services.
	
	The following services are listed on the UI:
	
	• WDM Servers
	• Discovery and imaging
	• Teradici server
	  • Threadx 4x server
	  • Threadx 5x server
	  • Teradici proxy servers
	• Scheduler
	• Master Repository
	
	If any of the services are stopped due to some reason, then the status of the server is displayed as **System is down**. If the services are up and running, then the status of the server is displayed as **System is healthy**.

Device Health	If you click the **Device Health** tile, it displays the total number of device enrolled into WDM server. In the lower pane of the Device Health page, you can view the health status of each platform (horizontally listed) and list of devices connected to the WDM server, applications with Hardware version (Vertically listed). The status of the device is classified as following: • Healthy • Busy • Offline • Sleeping
Jobs	If you click the **Jobs** tile, it displays the total number of scheduled jobs. It also displays the status of the scheduled job as follows: • Waiting • Running • With errors
Alerts	This parameter allows you to view and audit system events and alerts such as, License Error.

Parameter	Description
	NOTE: For Threadx 5.x devices, it displays the following warning alerts when it reaches full capacity per Teradici Proxy server available in the WDM deployment. • At 15000 devices, it displays full capacity alert. • At 18000 devices, it displays an error alert.
Events	In the upper right of the dashboard screen, you can view the list of events or actions performed such as Device manually added, Real time commands, Distributed package and so on.

Click the **Logged in Username** drop-down list option to perform the following actions in the WDM application.

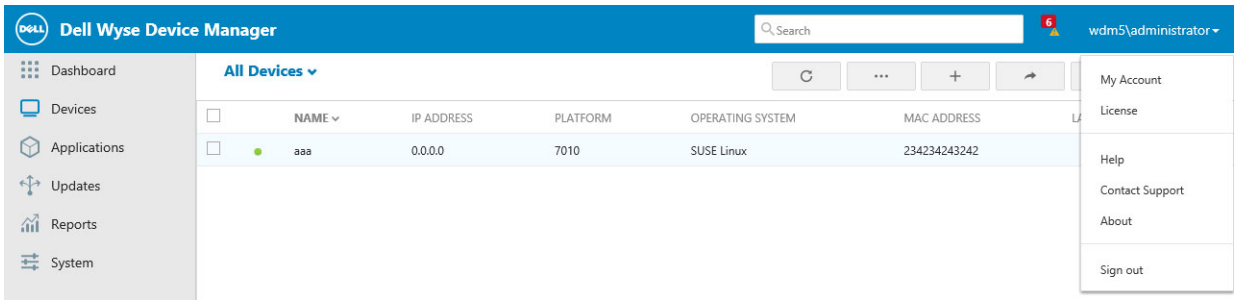


Figure 2. All Devices

- **My Account** - Click this option to view the profile of the user who is checked in.
- **License** - Click this option to view the WDM license details. For more information, see Licenses.
- **Help** - Click this option, to download the Admin guide.
- **Contact Support** - Click this option, it leads to the Dell support site, which gives you the proper contact information.
- **About** - Click this option to view the WDM version build, hotfix, description and installation details.
- **Sign out** - Click this option to log out from the WDM web UI application.

Topics:

- Licenses
- Unlicensed Devices
- WDM Utilities

Licenses

The **Licenses** page provides the details of WDM Enterprise licenses such as, the sales key, non-activated key, activation code, license, and description.

The default trial license period is for 30 days. You can extend the trial license period from 30 days to 60 days.

NOTE: The workgroup license has to be activated.

On 29th day of licensing or a day before 30 days, the trial period expires. To extend the license period, click **Extend License** on the license page. The trial period will be extended by another 30 days.

Adding workgroup license

1 Click **Add license**.

2 Enter the license in 7 characters-6 characters-6 characters-7characters format or copy-paste the license.
3 Click **Save**.

Activating workgroup license

1 Select the non-activated workgroup license.
2 Click **Activate License** on the right corner of the license page.

NOTE: Make a note of your non-activated license to use in the online WDM licensing form. You can also copy and paste the non-activated license in the online WDM licensing form.

3 Provide the WDM licensing details in the **Get Activation code** window. You need the following information to complete the form:
   - Company contact name
   - Company e-mail address
   - Company address
   - A WDM Sales Key and Non-activated Key
4 The activation code is displayed. You will also receive an e-mail with your activation code.
5 Enter or copy-paste the activation code into the **Add Activation Code** field and click **Activate Key**.
   You can verify the license details on the **Licenses** page.

NOTE: If your WDM Server does not have an Internet connection, go to the following URL to activate your WDM Sales Key:https://www.rapportlicensing.com/clientframe/rapport.aspx

Upgrading workgroup license to enterprise license

After you have an activated or non-activated workgroup license added to your WDM installation, you can upgrade the license to an enterprise license.

NOTE: During the upgrade to enterprise license, all workgroup licenses are deleted.

1 Click **Add license**.
2 Enter or copy and paste the new enterprise license.
3 Click **Save**.
4 After the upgrade is complete, the **Licenses** page displays your new non-activated enterprise license information.
5 Activate the license by following the steps in the Activating workgroup license section.

Unlicensed Devices

When number of discovered devices exceeds the license available in WDM, then the extra discovered devices is listed in the Unlicensed device page. You can move these unlicensed devices to the licensed devices by selecting and then click the **Add to Licensed Devices** option.

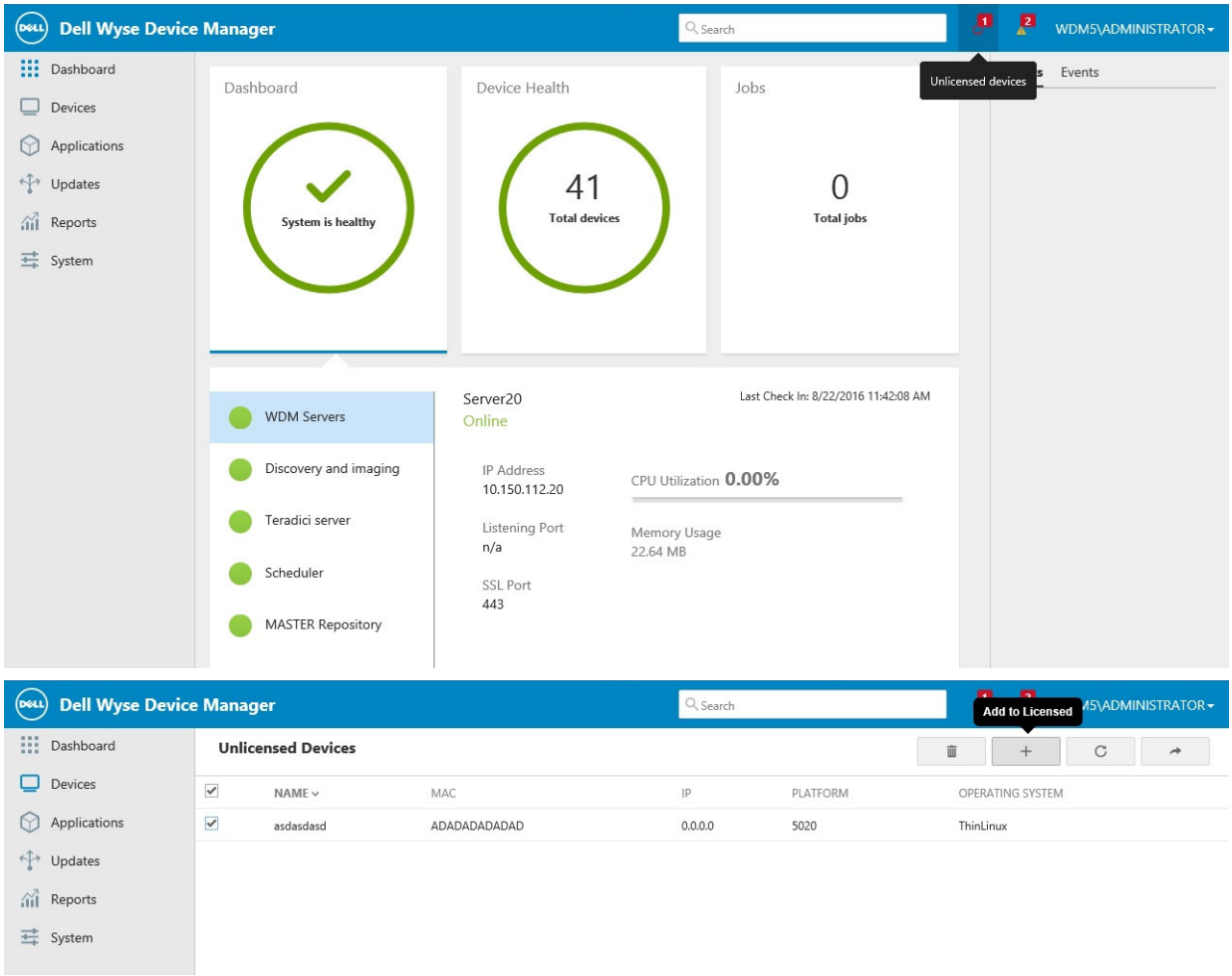


Figure 3. Unlicensed Devices

NOTE:

- To move unlicensed devices to licensed devices you must have enough number of licenses provided by the WDM administrator.
- If you do not have enough licenses and attempt to move an unlicensed device to licensed devices, the following message is displayed:`You have no license for the vendor`. If you still want to add a device to licensed page, then add the license that can accommodate more number of devices or delete the already existing devices on the license page.

WDM Utilities

WDM provides many utilities that enable to you to perform many additional functions such as high availability configuration, importing data into the database, managing accounts and DNS-DHCP lookup.

To access utility perform the following task:

1 Click the drop-down list of **Logged in Username** > **My Account** > **Download Utilities** .
2 Extract the contents from the downloaded file.
3 The following WDM utilities are displayed:
   - **HA** (High Availability Configuration Utility)
   - **Import** (Importing Data into the Database)
   - **Account** (Account Utility)
   - **DNS-DHCP** (DNS-DHCP Lookup Utility)

Importing data using import utility

In the **WDM Common Utilities** section, you can import data from **comma-delimited** and **tab-delimited** files. This utility allows you to import devices, subnets, IP ranges, repositories, or default groups for subnets from a file into the WDM database. The data must be imported from flat files. A delimited flat file contains one or more records separated by a specified delimiter or separator such as a comma or a tab.

To import data, perform the following steps:

1 From the drop-down, select the preferred category.
The **Import Category** drop-down lists the following options:
- Device
- Subnets
- IP Ranges
- Repositories
- Default Groups for Subnets

2 Navigate to the folder and select the file.
The file name appears in the **Import File Name** field.

3 Click **Import** to import the data files.

4 Click **Clear** to clear all the entries.

Format for importing device settings from flat files

The format to provide data in a flat file for device settings is as follows:

```
Client Name;MAC address;Platform;Custom field 1;Custom field 2;Custom field
3;Contact;Location;OS
```

- Client Name is the name of the device. Example: W1009341019
- MAC address of the device. For example: 0080646A1144
- Platform of the device. Example: VX0
- Custom field 1
- Custom field 2
- Custom field 3
- Contact is the contact person information for the device. Example: Administrator
- Location of the device. Example: San Jose office
- OS is the operating system code of the device. This field is applicable only to devices with the new Dell naming scheme.

The following are the operating system codes:

- Wyse Xenith — XEN
- WTOS — BL
- WTOS PCoIP — BLP
- PCoIP (ThreadX) — TDC
- SUSE Linux — SLX
- Red Hat Linux 6.x, 7.x and 8.x — RLX
- Windows XP — XP
- Windows Embedded Standard — WES
- Windows Embedded Standard 7 — WES7
- Windows Embedded Standard 7 P — WES7P
- WE8Sx Windows Embedded 8 Standard 32 — WE8Sx

- Windows Embedded 8 Standard 64 - WE8SEmbedded 8 Standard 64 — WE8S
- Windows 10 IoT Enterprise — WIE10

An example for device settings data is as follows:

```
D90Q8;A02040401050;5020;XYZ;MN;OP;WE8S;W1009341019;0080646A1144;VX0;ABCD;EFGH;IJKL;Administrator
;San Jose Office;WES
```

Format for importing subnet data from flat files

The format to provide data in a flat file for subnet is as follows:

```
Broadcast Address, Description, SW Repository, Override Default Parameters, IP Address, Subnet
Mask, Max. Web Service Simultaneous Updates, Wake On LAN Time Out(Secs.), Wake On LAN Tries,
TFTP Time Out (Secs.), TFTP Retries, Network Card Speed
```

- Broadcast address for the device. Example: 10.10.10.255
- Description is the subnet name displayed in the GUI.
- SW Repository is the name of a Software Repository. Example: Master
  You cannot add a subnet without a software repository.
- Override Default Parameters — Override Global Preferences (This is applicable for Enterprise license only)
- IP Address is the valid IP address in subnet. Example: 199.199.10.2
- Subnet Mask of the device. For example, 255.255.255.0
- Max. Web Service Simultaneous Updates is the limit for Maximum Simultaneous Updates. Example: 5
- Wake On LAN Time Out (in Seconds) is the Time Out for Wake On LAN. Example: 2
- Wake On LAN Tries is the limit for WOL retries. Example: 3
- TFTP Time Out (in Seconds). For example, 10
- TFTP Retries is the limit for TFTP retries. Example: 3
- Network Card Speed of the device. For example, 1 (for Auto), 2(for 100M-F), 3(for 100M-H)

An example for subnet data is as follows:

```
10.10.10.255,Subnet1,MASTER,False,199.199.10.2,255.255.255.0,6,2,1,1,7,2.
```

This example adds a subnet definition which discovers and manages devices on a class C subnet with IP address assignments from 199.10.0.1 to 199.10.0.254. The column header either does not exist or exists in the above proper order.

NOTE: Before working with subnets, the WDM database must contain information about at least one repository.

Format for importing IP range data from flat files

The format to provide data in a flat file for IP range is as follows:

```
StartIP, EndIP, ExclusionStartIP, ExclusionEndIP, Description
```

- StartIP — Beginning IP address for IP range
- EndIP — Ending IP address for IP range
- ExclusionStartIP —Beginning IP address for IP exclusion range
- ExclusionEndIP — Ending IP address for IP exclusion range
- Description — Enter the name of the IP range displayed on the GUI

An example for IP range data is as follows:

```
My IP Range 10.10.10.10 10.10.10.200 10.10.10.20 10.10.10.30
```

The IP range definition is added to the database to discover all devices between the ranges of 10.10.10.10 to 10.10.10.19 and 10.10.10.31 to 10.10.10.200. This IP range definition shows up in the WDM GUI as **My IP Range**.

Format for importing software repository data from flat files

The format to provide data in a flat file for software repository is as follows:

```
Name of Repository, IP Address of Repository, Transfer Type, Relative Path, Context, FTP Port Number, HTTP Port Number, FTP user name, FTP password, HTTP user name, HTTP password, IsHTTP Secure, HTTPSValidateWithCA, RemoteServerName, CIFSUsername, CIFSPassword
```

- Name of the software repository as it appears in the GUI
- Location is the IP address of the FTP server
- Transfer Type is the type of the transfer protocol that is in use. It can be FTP or HTTP or both.
- Relative Path is the path to the software repository relative to the root directory. The default value for this is /rapport.
- Context is valid for HTTP communication and is the name of virtual directory. By default HTTP context is MyWDM.
- FTP Port Number is the port number for FTP communication. Default value is 21.
- HTTP Port Number is the port number for HTTP/HTTPS communication. Default value is 80 for HTTP and 443 for HTTPS communication.
- FTP User Name is the user name for the FTP account as set up by IIS FTP or the FTP service that you use to connect to the repository.
- FTP Password is the password for the FTP account as set up by IIS FTP or the FTP service that you use to connect to the repository.
- HTTP User Name is the user name for the HTTP account as set up by IIS HTTP or the HTTP service that you use to connect to the repository.
- HTTP Password is the password for the HTTP account as set up by IIS HTTP or the HTTP service that you use to connect to the repository.
- Secure(HTTPS) — Enter -1 if **Secure** is checked(HTTPS supported) and 0 if **Secure** is unchecked (HTTP is supported not HTTPS).
- HTTPSValidateWithCA — It is -1 if **Validate Certificate with CA** is checked and 0 if unchecked.

Examples for software repository data is as follows:

- Example where the transfer type is HTTP and FTP

  ```
  RemoteHTTPFTP, 10.10.11.9,HTTP and FTP,/rapport,MyWDM,21,80,FTPUserName,FTPPassword,
  HTTPUserName,HTTPPassword ,0,0
  ```

- Example where the transfer type is HTTP

  ```
  RemoteHTTP,10.10.11.9,HTTP,/rapport,MyWDM,,80,,,HTTPUserName,HTTPPassword,0,0
  ```

- Example where the transfer type is HTTP with Secure flag Checked

  ```
  RemoteHTTP,10.10.11.9,HTTP,/rapport,MyWDM,,443,,,HTTPUserName,HTTPPassword,-1,-1 or
  RemoteHTTP,10.10.11.9,HTTP,/rapport,MyWDM,,443,,,HTTPUserName,,-1,-1
  ```

- Example where the transfer type is FTP

  ```
  RemoteFTP,10.10.11.9,FTP,/rapport,,21,,FTPUserName,FTPPassword,,,0,0
  ```

- Example where the transfer type is CIFS

  ```
  RemoteCIFS,10.150.112.3,SMB,/rapport,MyWDM,,,,,,,
  0,0,RemoteServerName,CIFSUsername,CIFSPassword
  ```

- Example where the transfer type is FTP, HTTP, and CIFS

  ```
  FTPHTTPandCIFS,10.150.112.3,HTTP and FTP and SMB,/Rapport,MyWDM,
  21,80,FTPusername,FTPpassword,Httpusername,Httppassword,
  0,0,RemoteServerName,CIFSusername,CIFSpassword
  ```

- Example where the transfer type is FTP, HTTPS, and CIFS

  ```
  FTPHTTPSandCIFS,10.150.112.7,HTTP and FTP and SMB,/Rapport,MYWDM,
  21,443,FTPUsername,FTPPassword,HttpUsername,HttpPassword,-1,0,RemoteServerName,CIFSUserName,CI
  FSPassword
  ```

The software repository definition is added to the database to define a repository on a server at 10.10.11.9. The default path for the root directory of the FTP service is **/rapport**. This repository is accessed with the username of the user. The FTP is used as the transfer protocol and is displayed in WDM as remote.

Format for importing default groups for subnets from flat files

The format to provide data in a flat file for default groups for subnets is as follows:

```
Broadcast Address, Default group, Default group value
```

- Broadcast Address of the device. For example, 10.10.10.255
- Default Group. For example, State
- Default Group Value. For example, California

```
Example 1: 10.150.115.255;States;California

Example 2: 10.150.115.255;Department;Sales

Example 3: 10.150.116.255;States;California
```

NOTE: The WDM database must contain the subnet, groups and group values.

A check box labeled **Update Existing Default Groups for Subnets** appears at the bottom of the page when **Default Groups for Subnets** is selected.

If the box is unchecked, the import for any group name value fails if the subnet already contains the assigned default group.

If the box is checked, the group value is updated with the import file group name value.

High Availability Configuration Utility

The High Availability Configuration Utility is used when you are setting up a High Availability environment and are clustering the database. This utility helps WDM to connect to the cluster in order to function within the cluster and ensure that there is zero downtime. This utility is available after you install WDM.

1 Enter the following details:
   - **Database Name** – This is displayed by default and cannot be edited.
   - **Database Server** – Specify the hostname of the database cluster.
   - **Database Port**— Specify the port number.
   - **Database User Name** – Specify the database user.
   - **Database Password** – Specify the password of the database user.

2 Click **Provision**.
   The connection details are displayed on the right side of the utility.

   NOTE: You should re- enter the licence as provisioning alters the license. Do not execute HA utility in non HA environment.

Account Utility

The Account utility enables you to view the details of the WDM database and also create new credentials to access the database.

1 The account utility displays the following information:
   - **Server Port —** The IP address of the WDM database server and the database server port number.

- **Database Name —** The name of the WDM database.
- **User Name—** The user name to access the WDM database. This is the user name you have specified while installing WDM.

2 To change the credentials to access the database:

   a Enter the new **User Name** under **New credentials for WDM database**.

   b Enter the **Password** to access the database.

   c Re-enter the password in the **Confirm Password** field.

   d If you want to use your domain user name and password, select **Connect as domain user**.

3 Click **Update** if you have entered new credentials, or click **Clear** to close the window if you have not entered any new credentials.

DNS-DHCP Lookup Utility

It allows you to find out the method that has been configured in the network to discover WDM by the client.

You can check results of DNS and DHCP lookup for the WDM server.

4

Devices

In the Devices page you can view all the devices which are discovered automatically or manually. You can also view the details of the device information and perform the tasks such as adding the new device manually, real time commands and so on.

Table 3. Devices

Parameter	Description
Name	Displays the name of the device.
IP address	Displays the IP address of the devices.
Platform	Displays the platform of the devices.
Operating system	Displays the operating system running on the devices.
MAC address	Displays the MAC address of the devices.
Last check in	Displays the time stamp when device reports to WDM server.

NOTE: For all the devices, the health status is displayed next to its name. If you pause the pointer over the health status icon, the health status of that particular device is displayed.

The detailed summary of the devices are displayed under **All Devices** tab on the upper left of the page.

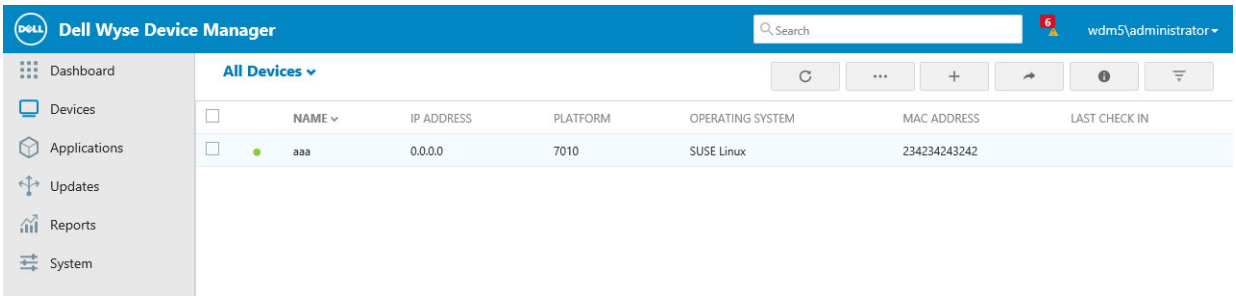


Figure 4. All Devices

To perform real time commands on the discovered devices complete the following task:

General real time command options:

1 The real time commands are available on the top of the screen.

a To refresh the page, click **Refresh**.

b Click **More** to rename the device and enter the updated name in the **Rename Device** field.

c Click **Add or find Device** to add a device manually or find more devices to WDM by manual discovery.

Figure 5. Find Devices

To discover a device, perform the following tasks:

1 Click the **Find Devices** option. You can discover a device using **Local Network**, **IP Range** and **Subnet**.

2 Click the **IP Range** option to discover a device using IP range and enter a range of the IP address in the provided field.

3 Click the **Subnets** option to discover a device using subnets. You can search for a subnet in the **Global Search** bar.

4 Click the **Local Network** option to discover devices from the local network.

5 Click **Discover**.

To add a device manually, do the following:

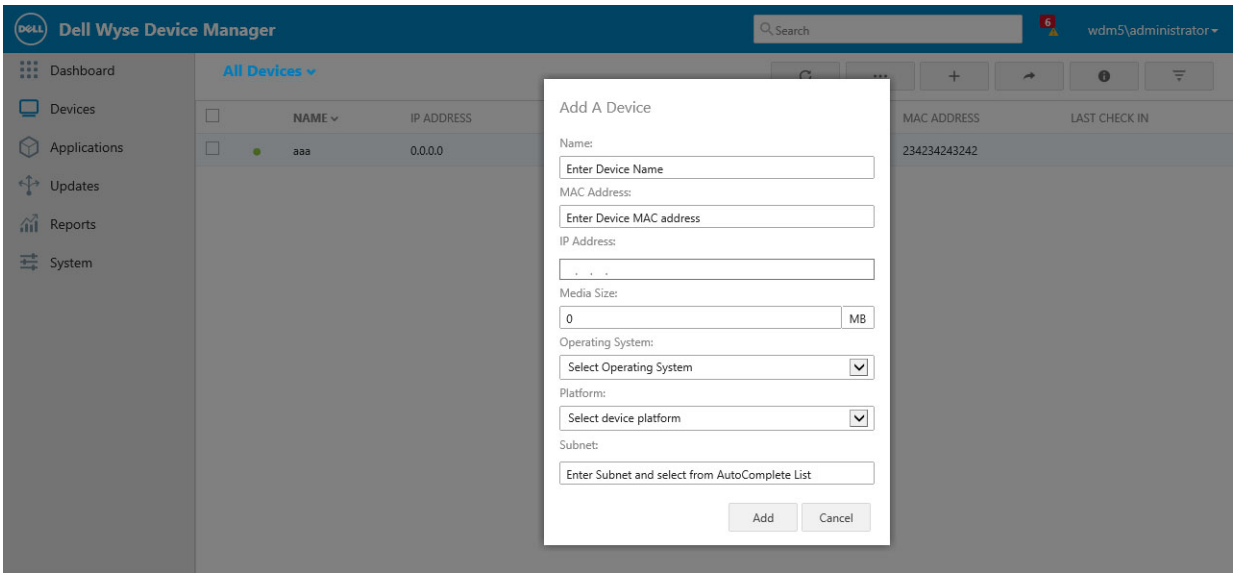


Figure 6. Add a Device

1 Click the **Add A Devices** option.

2 Enter the device name in the **Name** field.

3 Enter the device MAC address in the **MAC address** field.

4 Enter the IP address of the device in the **IP Address** field.

5 Enter the media size (specified in MB) of the device in the **Media Size** field.

6 From the drop-down lists, select your preferred **Operating System** and the device **Platform**.

7 Enter **subnet** and select subnet IP from the Autocomplete list.

8 Click **Add**.

d Click **Export** to export the device list in **.csv** or **.txt** (tab delimited) format.

e Click **View Details** to view complete overview, Status, Network, Hardware and Logs of the selected device.

- **Overview** — Provides a complete overview of the **System**, **Location**, **Capabilities**, **Network**, and **Drives** of the selected device.
- **Status**— Provide details of Apps that are installed and running on the system. Installed Update also provides details about the Processor running and system performance. The details of the Remote session are displayed for the selected devices.
- **Network**— Provides the **NIC card** details and the **Network Details** of the selected device.
- **Hardware**— Provides the details of the following attributes:
  - **Disks**: Displays the number of partitions available on the device and its memory size.
  - **Drives**: Displays the number of drives and its memory size.
  - **Systems**: Displays the hardware related details.
- **Logs**— Provides the details of the **Audit Trails** and **Deployed Packages** of the selected device.

f Click **Add/Modify Filter** to filter devices page depending on Name, IP Address, Operating System, Platform, Last Check-in and MAC Address. Use the following guidelines:

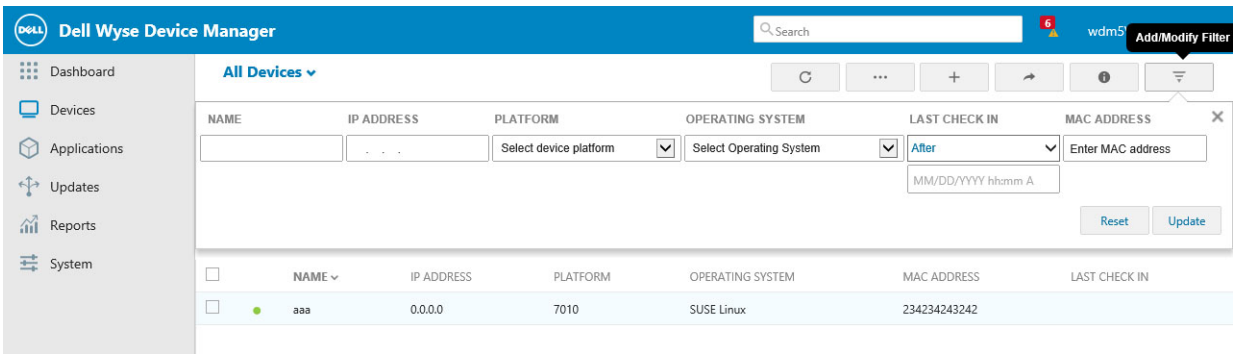


Figure 7. Add/Modify Filter

1 To filter devices page depending on the device name, enter Device name in the **Name** field, and then click **Update**.

NOTE: Use Partial Name of the device, if you are searching a device by part of the names.

2 To filter devices page depending on the IP address, enter the IP address of the device in the **IP Address** field, and then click **Update**.

3 From the drop-down lists, select your preferred **Operating System** and the device **Platform** to filter the devices page depending on the operating system and platform.

4 From the **Last Check-in** drop-down list, select either After or Between based on your preference and specify the date and time in MM/DD/YYYY hh:mm format during which the device was checked-in.

5 Enter the **MAC address** of the device, and click **Update** to filter the devices page depending on the MAC address of the device.

6 Click **Reset** to reset the entered value.

7 Click **Update** to add a filter to the devices page

8 Pause the mouse pointer on the filtered attribute, and then click the **x** icon displayed next to the filter to remove the applied filter.

Select the preferred device to perform the following real time commands:

a To push a package to specific device, click **Update**.

b To restart the selected device, click **Reboot Device**.

c To shutdown or stop the selected device, click **Shutdown**.

d To send a message for the selected device, click **Send Message**. The **Send Message** screen is displayed.

1 Select the radio button of the preferred message type from the displayed message type options. The following are the message types:

- Information
- Warning
- Critical

2 Enter the title of your message in the **Message Title** field.

3 Enter the content of the your message in the **Message Body** field.

4 Click **Send** button to send your message.

e Click **More** to perform more tasks. You can perform the following tasks:

Table 4. More

Parameter	Description
Rename Device	Enter the updated name in the **Rename Device** field.
Update Device Information	Enter the device details to update the device information. To update the device information enter the following details: • Device Location • Contact • Add Custom Tags Click **Update** option to update the device information.
Execute Commands	To run the commands, enter the command or the path in the **Execute Commands** field and click **Execute** option to run the entered command.
Wake on LAN	To wake up the devices that are shutdown on the same subnet where WDM is installed, click **Wake on LAN**.
Relay Wake on LAN	To wake up the devices across the subnet, click **Relay Wake on LAN**.
Get Image	Enter the name of the Image and the related description in the respective fields. Click the **Compress image** button to enable the image compression. **NOTE: Compressing the image increases the processing time.**
View Logs	Use this option to view the device logs. To create your own log, click the **Create Log** button, specify the name for the log, and then click **Create**.
Include to PAD Repository	To include a device that is excluded from PAD Repository, click **Include**.
Exclude from PAD Repository	To exclude the device from PAD repository, click **Exclude**.
Delete	To delete a device from WDM database, click **Force-delete**. To delete the device by removing the server details from agent, click on **Delete**.
Remote Shadow	Use this option to enable remote shadowing of your device. This allows you to view and control a device remotely (shadowing a device).

To manage the group types perform the following task:

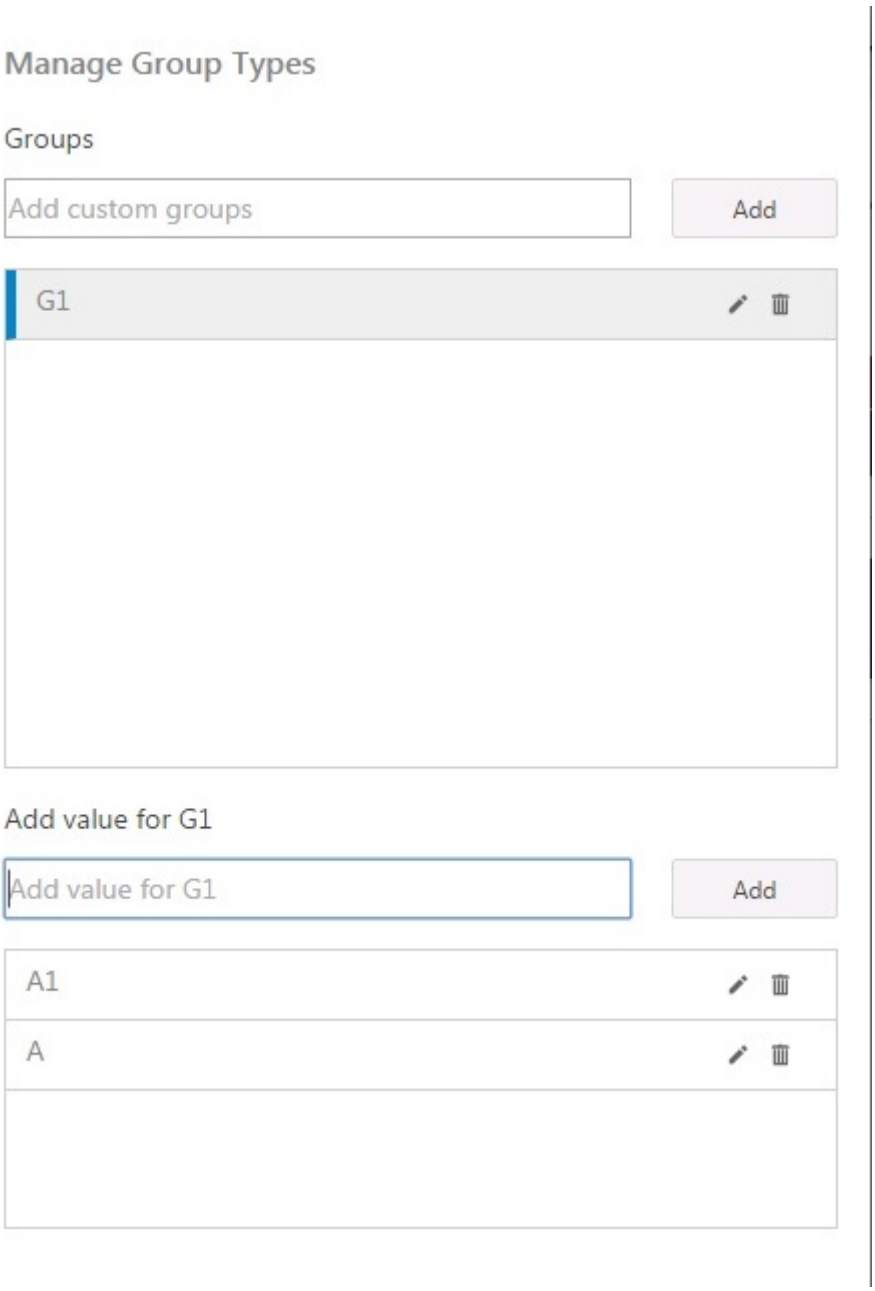


Figure 8. Manage Group Types

1 Click the **All Devices** option and select **Manage Group Types** option. A **Manage Group Types** page is displayed.
2 Enter the name of the custom groups in the **Groups** field.
3 Click the **Add** option to add the selected custom groups.
4 Select the added group from the list and add value for the particular group.
5 Click the **Add** option to add value for the selected groups.
6 Click the **Save** option to save your changes.

To create a new view perform the following task:

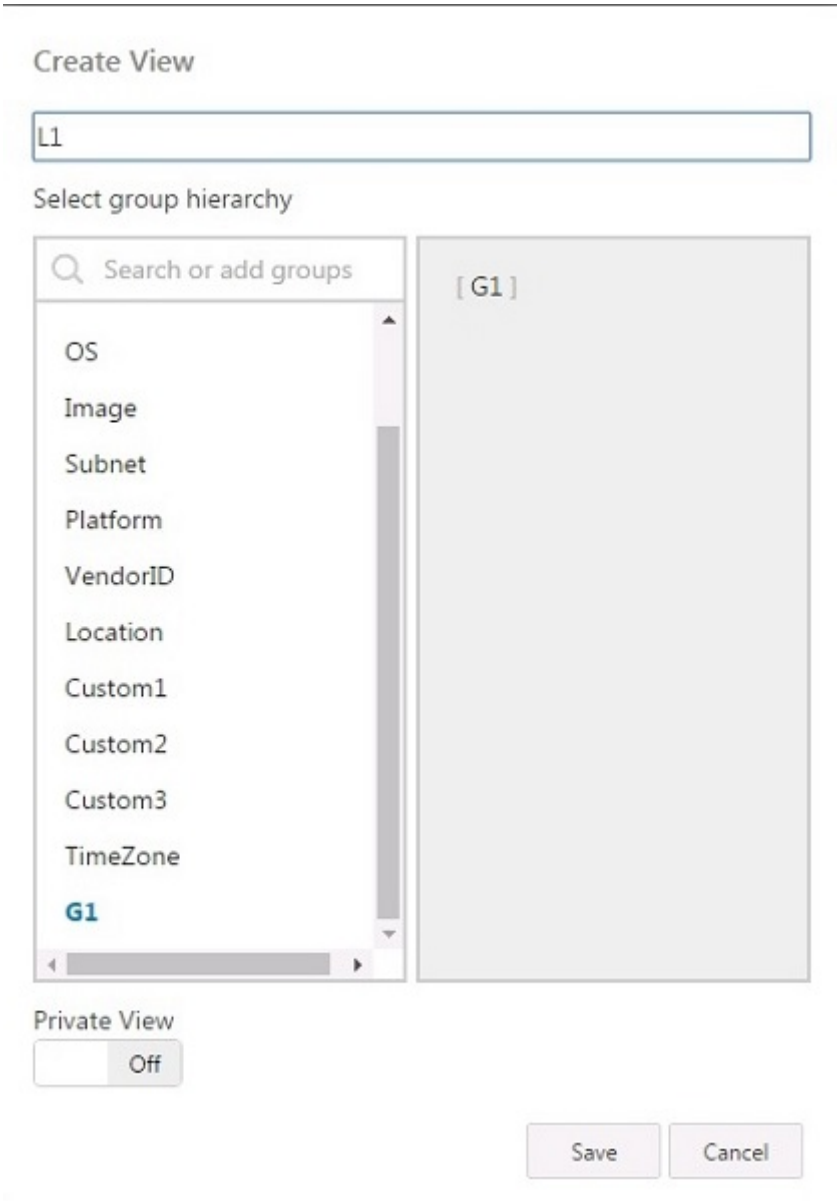


Figure 9. Create View

1 Click the **All Devices** option and select **Create View** option. A **Create View** page is displayed.

2 Enter the name of the view in the **New view** field.

3 Select the groups displayed on the left side of the screen in order of preferred hierarchy.

NOTE: To add a custom group, click the + Add custom group option. Enter the name of the group and select the check mark to add the custom group in the list of group hierarchy. You can view the order of selected groups of hierarchy.

4 Click the **ON/OFF** button to enable or disable the **Private View** option.

5 Click the **Save** option to save your changes.

To assign a device to a custom group, do the following:

1 Click **All devices** and select the custom view created.

2 Click **Unassigned** .

3 Select a device, and then click **Assign Group**.

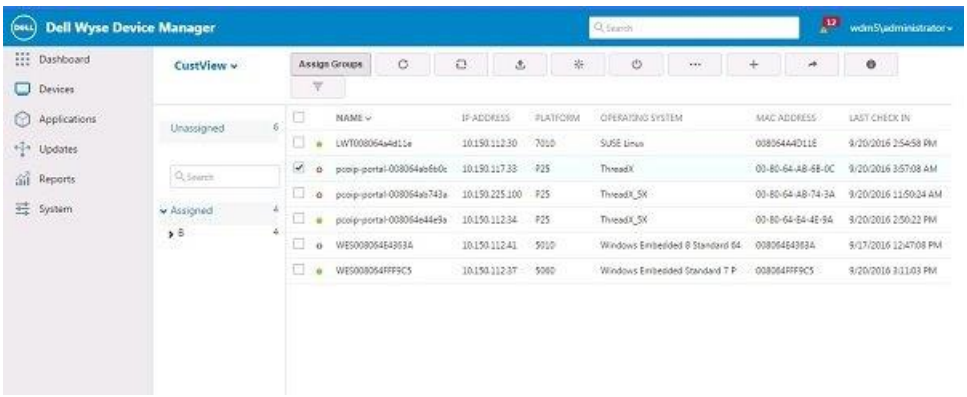


Figure 10. Assign Group

4 Select the group value to which you want to assign the device.

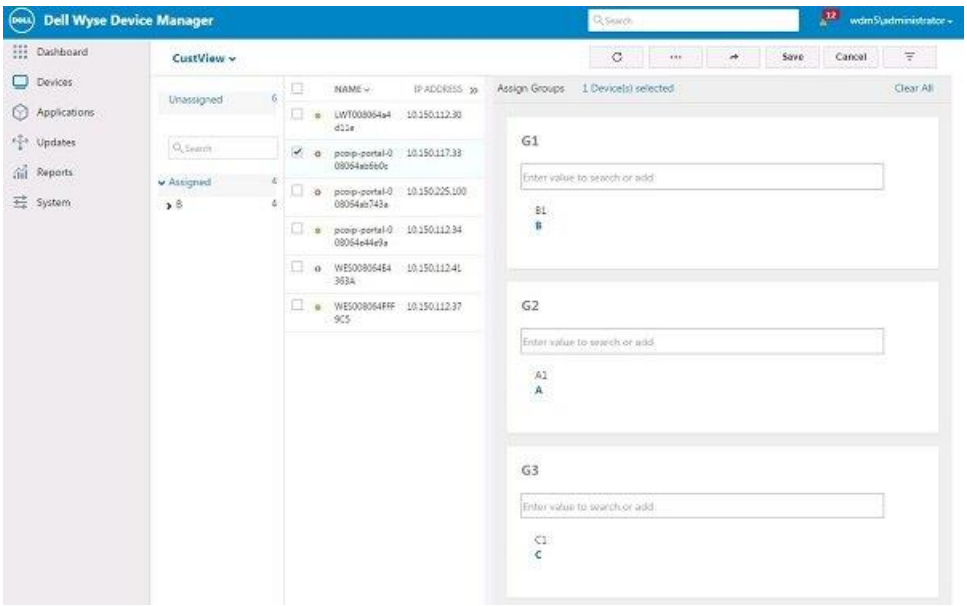


Figure 11. Assign Group

5 Click **Save**.

5

Applications

The Applications page allows you to perform the following tasks:

- Register packages to the WDM Master Repository.
- Deploying a package to the devices.
- Manually registering the package images and/or configurations packages that you register or create or get from the devices in your network (to distribute it to other devices).
- Upgrading the pre-registered WDM Agent and Boot Agent Packages.
- Organize the packages into functional categories and distribute packages to selected devices (immediately or on a scheduled basis).

By default, WDM provides a few standard packages that can be deployed to the devices. These packages are divided into five categories:

1 Agent Upgrade
2 Device Configuration
3 Images
4 Other Packages
5 PCoIP Device Configuration

- **Agent Update**—The Agent update page is used to view the list of available agent packages. The description for individual Agent package is displayed along with the details of operating system on which these packages can be registered.

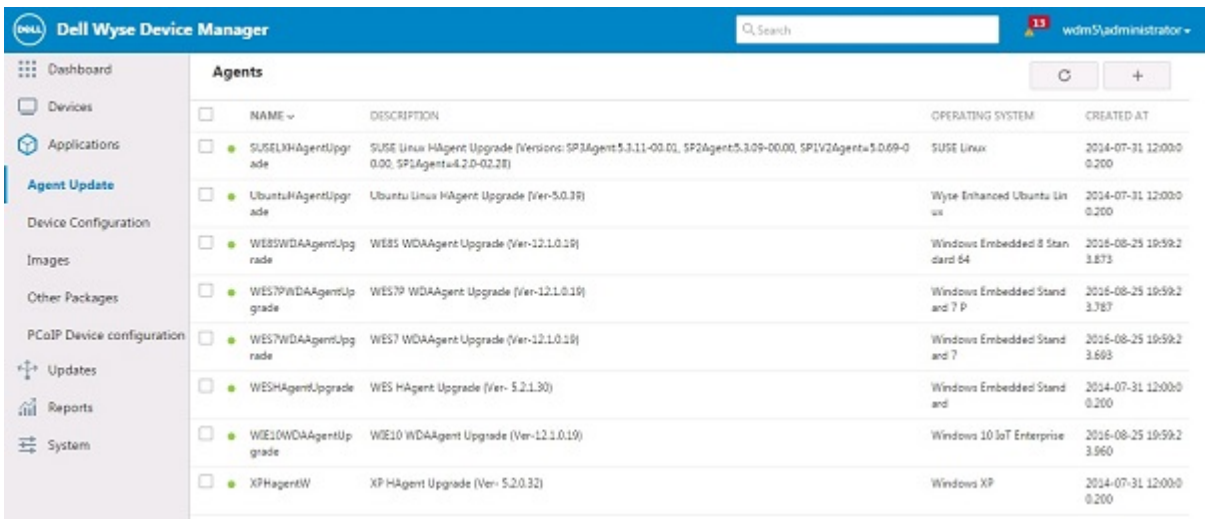


Figure 12. Agents

- **SUSELXHAgentUpgrade**— This package can be scheduled only to the devices running SUSE Linux OS , This package can be used to update the existing HAgent to the HAgent version incorporated in WDM.
- **UbuntuHAgent Upgrade**— This package can be scheduled only to the devices running the Wyse Enhanced Ubuntu Linux OS,. This package can be used to update the existing HAgent to the HAgent version incorporated in WDM.
- **WE8SWDAAgentUpgrade**— This package can be scheduled only to the devices running the Windows Embedded 8 Standard 64 bit OS. This package can be used to update the existing HAgent and WDA to the WDA version incorporated in WDM.
- **WES7WDAAgentUpgrade**— This package can be scheduled only to the devices running WES7 OS. This package can be used to update the existing HAgent and WDA to the WDA version incorporated in WDM.

- **WES7PWDAAgentUpgrade** - This package can be scheduled only to the devices running WES7P OS. This package can be used to update the existing HAgent and WDA to the WDA version incorporated in WDM.
- **WESHAgentUpgrade**— This package can be scheduled only to the devices running WES OS. This package can be used to update the existing HAgent to the HAgent version incorporated in WDM.
- **WIE10WDAAgentUpgrade**— This package can be scheduled only to the devices running WIE10 OS. This package can be used to update the existing HAgent and WDA to the WDA version incorporated in WDM.
- **XPHAgentW**— This package can be scheduled only to the devices running XPe OS. This package can be used to update the existing HAgent to the HAgent version incorporated in WDM.

Table 5. Agents update

Parameter	Description
Name	Displays the name of the packages.
Description	Displays the description of the packages.
Operating System	Displays the operating system of the registered packages.
Created At	Displays the Date and Time of the package creation.

- **Device Configuration**— The Device Configuration page is used to create, and register new application configuration packages.

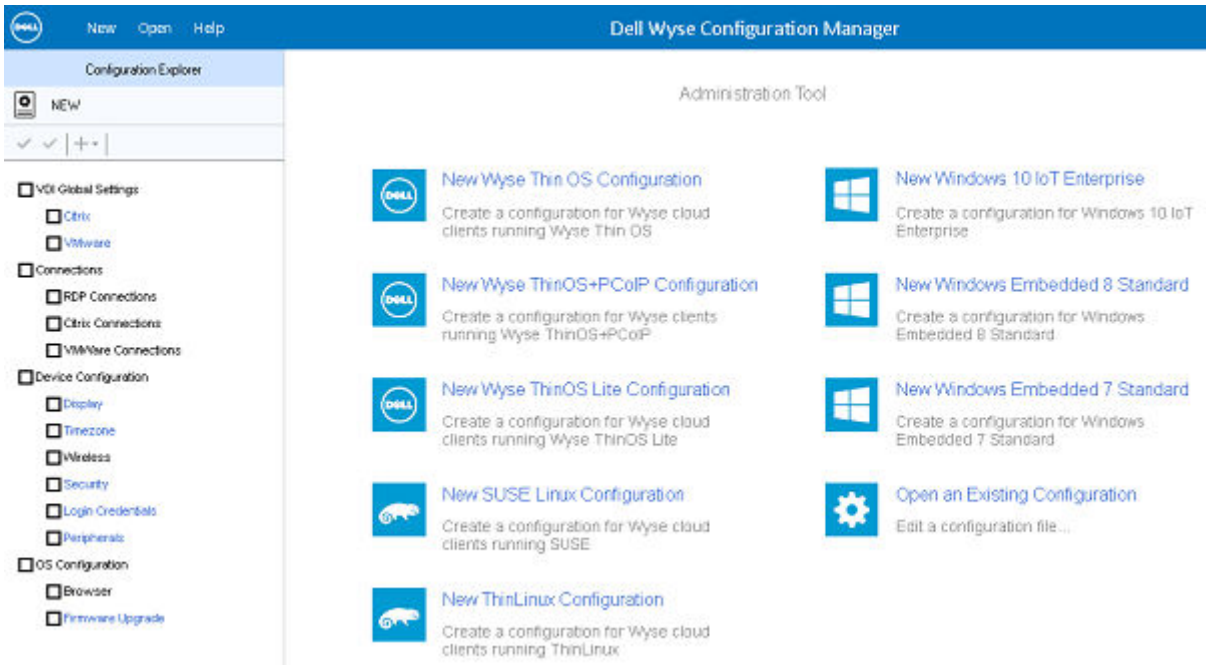


Figure 13. Device Configuration

a To start the WCM application, click the **create package** option or the **+** icon.

b Click **Download** to download WCM Utility.

c Create the device configurations using the WCM Application GUI by selecting and updating the required configurations and save them. The configuration packages are saved in the WDM repository and are listed on the right-hand pane of the WDM console when you select the **Device Configuration** node.

For more information on creating WCM Configurations, see the *Dell Wyse Configuration Manager Administrator's Guide* .

- **Images**— The Images page is used to view the list of the registered image packages. The description for individual image package is displayed along with the details of operating system, image type, and size of the packages. The registered image packages and pulled image packages are listed in the Images page. By default, the boot agent upgrade package for WES and XPe are listed in the Image page.

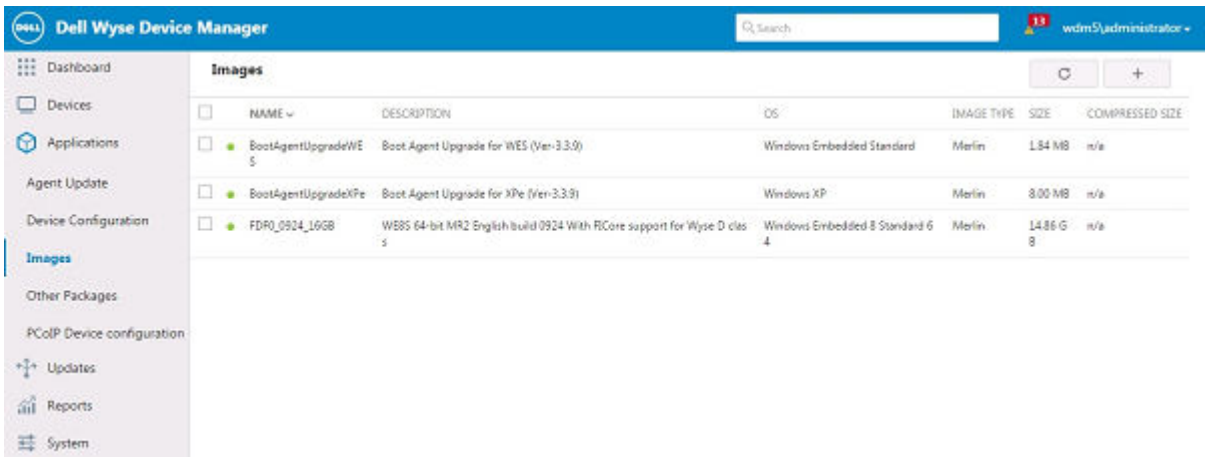


Figure 14. Images

- **BootAgentUpgradeWES** - This package can be scheduled only to the devices that are having Boot Agent embedded with the image. When scheduled to a device, it upgrades or downgrades the Boot Agent of the device.
- **BootAgentUpgradeXPe** -This package can be scheduled only to the devices that are having Boot Agent embedded with the image. When scheduled to a device, it upgrades or downgrades the Boot Agent of the device.

Table 6. Images

Parameter	Description
Name	Displays the name of the packages.
Description	Displays the version of the packages.
Operating System	Displays the operating system of the registered package.
Image Type	Displays the image type of the packages.
Size	Displays the size of the images.
Compressed Size	Displays the compressed image size.

- **Other Packages**— The other packages page is used to view the list of the AgentUpgrade packages and other packages. The description for individual AgentUpgrade package and other packages is displayed along with the operating system on which these packages are registered. Other Package Category has default Boot Agent upgrade packages for all the Operating system. It also contains the default Reboot, shutdown Wake On LAN and ResetOSsetting packages.

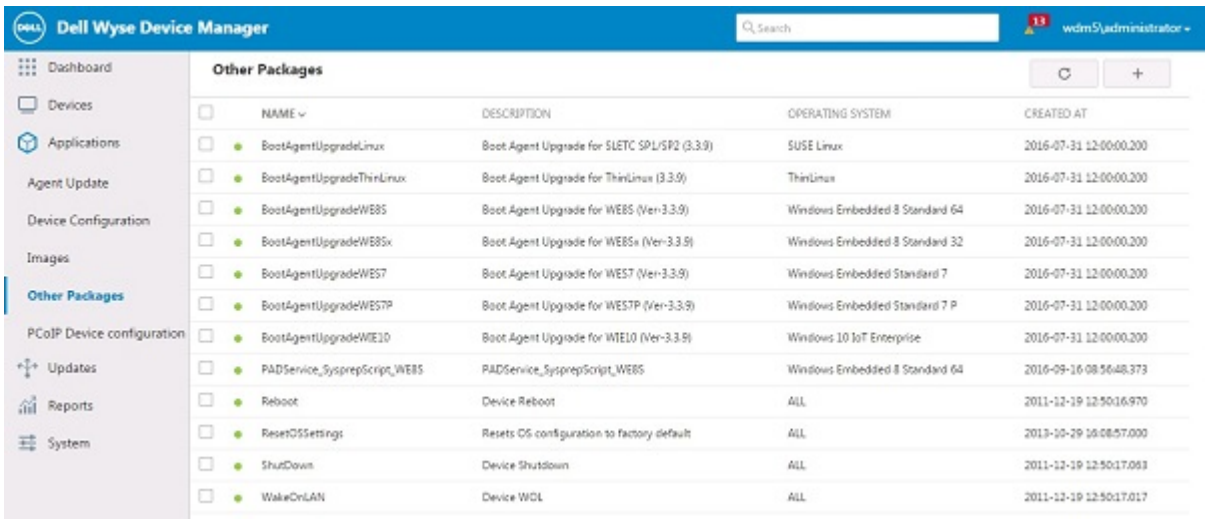


Figure 15. Other Packages

- **BootAgentUpgradeLinux**- To upgrade the boot agent for a device running the SUSE Linux Enterprise OS.
- **BootAgentUpgradeThinLinux**— To upgrade the boot agent for a device running the ThinLinux OS.
- **BootAgentUpgradeWE8S**- To upgrade the boot agent for a device running Windows Embedded 8 Standard 64 bit OS.
- **BootAgentUpgradeWE8Sx**- To upgrade the boot agent for a device running Windows Embedded 8 Standard 32 bit OS.
- **BootAgentUpgradeWES7**- To upgrade the boot agent for a device running Windows Embedded Standard 7 OS.
- **BootAgentUpgradeWES7P**- To upgrade the boot agent for a device running Windows Embedded Standard 7P OS.
- **BootAgentUpgradeWIE10**- To upgrade the boot agent for a device running Windows 10 IoT Enterpise OS.
- **Reboot** - When scheduled to a device, the device gets rebooted.
- **ResetOSSettings**- To reset the OS configuration of the device to factory default.
- **Shutdown** - When scheduled to a device, the device shuts down.
- **WakeOnLAN** - When scheduled to a device, it sends the WOL command to the device.

Table 7. Other Packages

Parameter	Description
Name	Displays the name of the packages.
Description	Displays the description of the packages.
Operating System	Displays the operating system of the registered packages.
Created At	Displays the Date and Time of the package creation.

- **PCoIP Device Configuration**— The PCoIP device configuration page is used to view the list of the PCoIP Devices packages. The description for individual PCoIP device package is displayed along with the operating system. The registered PCoIP configuration package is displayed under PCoIP Device Configuration.

  The default available packages are applicable only for ThreadX 4.x firmware.

  - ThreadX: The packages belongs to ThreadX 4.x firmware.
  - ThreadX_5x: The packages belongs to ThreadX 5.x firmware.

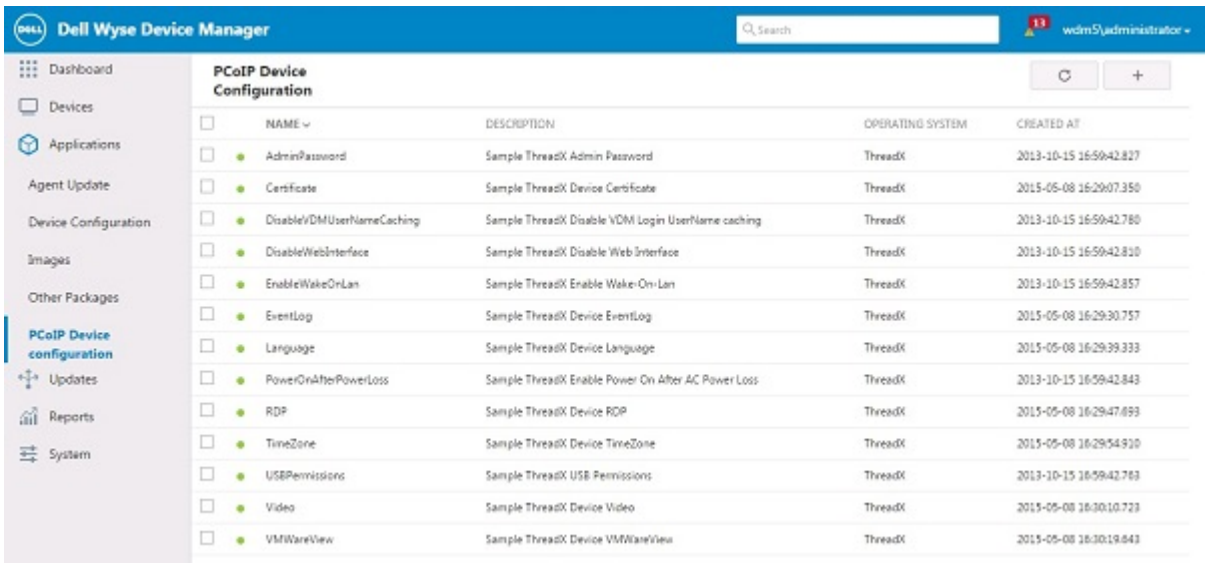


Figure 16. PCoIP Device Configuration

- **AdminPassword** — Sample package to change the administrator password for ThreadX devices.
- **Certification** — Sample package to change the device certificate for ThreadX devices.
- **Disable VDMUserNameCaching** — Sample package to disable the caching of the VDM Login user name for ThreadX devices.
- **DisableWebInterface** — Sample package to disable the web interface for ThreadX devices .
- **Enable WakeOnLan** — Sample package to enable WakeOnLAN feature for ThreadX devices.
- **EventLog** — Sample package for ThreadX devices event logging.
- **Language** — Sample package to change the language configuration for ThreadX devices.
- **PowerOnAfterPowerLoss** — Sample package to enable power on after power loss on ThreadX devices
- **RDP** — Sample package to change the RDP configuration for ThreadX devices.
- **TimeZone** — Sample package to change the timezone configuration for ThreadX devices.
- **USBPermissions** — Sample package to configure USB Permissions for ThreadX devices
- **Video** - Sample package to change the video configuration for ThreadX devices.
- **VMWareView** - Sample package to change the VMWare view configuration for ThreadX devices.

Table 8. PCoIP Device Configuration

Parameter	Description
Name	Displays the name of the packages.
Description	Displays the version of the packages.
Operating System	Displays the operating system of the registered packages.
Created At	Displays the Date and Time of the package creation.

General options for configuring the packages/images

1 Select any of the listed packages/images.

The options to perform the tasks are available on the upper-right corner of the screen.

a Click the **Update** option to update the selected package/image.

1 Select your preferred package from the application list.
2 Click the update option displayed on the top of the screen.
3 From the **Select View** drop-down list, select your preferred view.

NOTE: The package distribution is the mass deployment process under Application tab. You can not select individual device to deploy a package. The selected package is deployed to the entire selected view.

4 Schedule the package distribution based on your preference. You can distribute a package in following ways:
- If you select the **One time distribution** option, enter the details of package distribution. Select the distribute option as **Now** if you prefer to distribute the package or you can select the distribute option as **A specific date and time** and enter your preferred date and time of package distribution. Click the **On/Off** option to enable or disable the **Retry failed updates** option.
- If you select **Recurring distribution** option, enter the following package distribution details:
  1 Enter the name for the recurring scheduler.
  2 From the **Recur** drop-down list, select the day for package distribution.
  3 Enter the start and end date of the package distribution.
  4 Enter the time duration of the package distribution.

5 Click the **Save** option displayed on the top of the screen to save your changes.

b Click the **Disable Distribution** option to disable the package for distribution.

c Click the **Package Script** option to view or export the selected packages' script.

For more information, see Export the Package Script of a registered package and Edit the Package Script of a registered package

d Click the **Refresh** option to refresh the page.

e The **Register Package** option is used to register a package.

1 Click **Register Package** option to download package register utility. The WDM Package Registration Utility dialog box is displayed.
2 Enter the WDM server address and credentials in the WDM Server, Username and Password fields.
3 Click the **On/Off** option to enable or disable the **Save credentials (encrypted)** option.
4 Two types of package can be registered using Package Registration utility dialog box:
- **Register RSP**: Allows you to select a .rsp package, and upload it to the WDM server. For more information, see Registering a Package from a Script File (.RSP)
- **Register EXE**: Allows you to choose a .exe, .msi, .msu, or .bat file, and upload it to the WDM server. For more information, see Register a Package to install a File. (exe, msi, msu, or bat files only)

5 Click **Upload**.

f **(This option is applicable only for Images)** Click the **Deploy via peers** to deploy a package to a device. To deploy a package to a device, complete the following task:

1 From the drop-down list, select your preferred platform.
2 Enter the start date, end date and timings in hh:mm:ss format to schedule a deployment.
3 Enter the subnet IP to select from the available subnets.

NOTE: At least one subnet needs to be selected for creating PAD schedule.

4 Click **Deploy**.

Topics:

Editing the Package Script of a Registered Package

To view the property of a software package:

1 Click the **Package Script** option.

The Package Script window is displayed.

2 Click the **Edit** option to edit the script.

3 Click **Save**.

NOTE: You cannot modify the script for default packages. This is valid only for custom packages.

Exporting the Package Script of a registered Package

To export the package script of a registered software package:

1 Click the **Package Script** option. The Package Script window is displayed.

2 Select **Export** option to export the package script.

3 Browse through the path where you want to save the script and click on **OK** button to save.

4 The confirmation window is displayed. Click **OK** to save the script at specified location.

Registering a Package from a Script File (.RSP)

To register a .rsp software package:

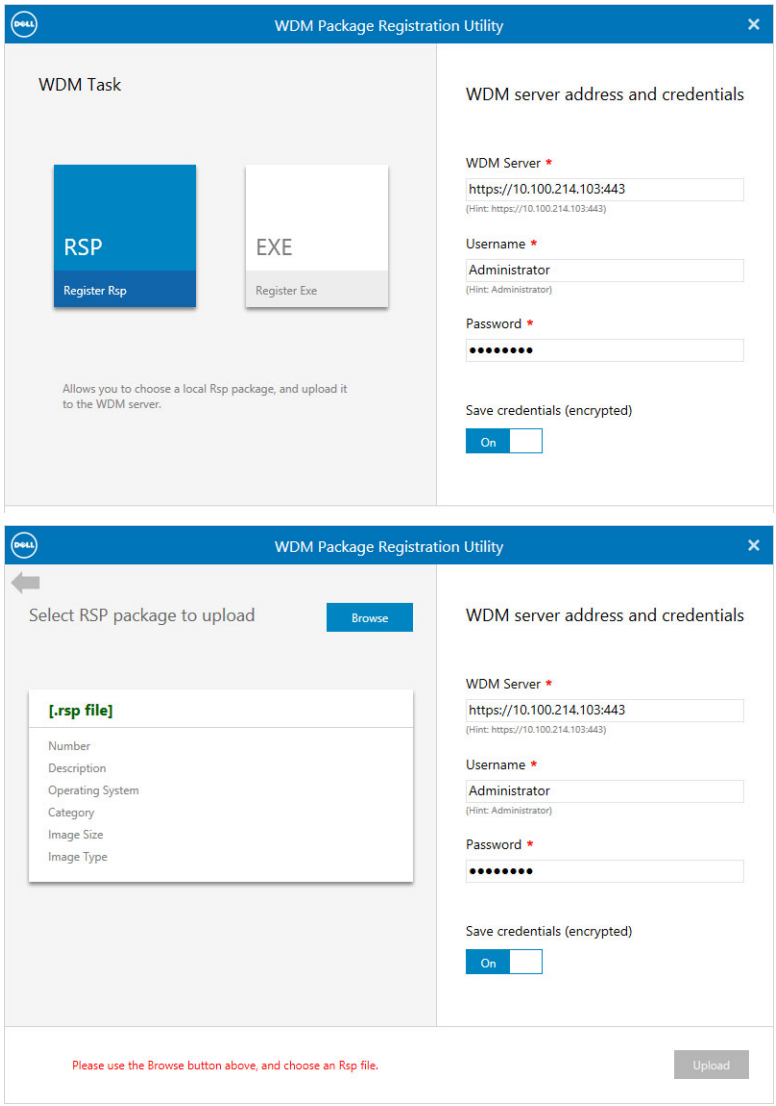


Figure 17. Register Rsp

1 Download and open the Package Registration Utility dialog box.
2 Click the **RSP** tile displayed on the WDM Package Registration Utility dialog box.
3 Browse the .rsp file or package to upload.
4 The following details of the RSP package is displayed.
   - Name
   - Description
   - Operating System
   - Category
   - Image Size
   - Image Type
5 Click **Upload**.

Register a Package (exe, msi, msu, and bat files only)

To register a package, do the following:

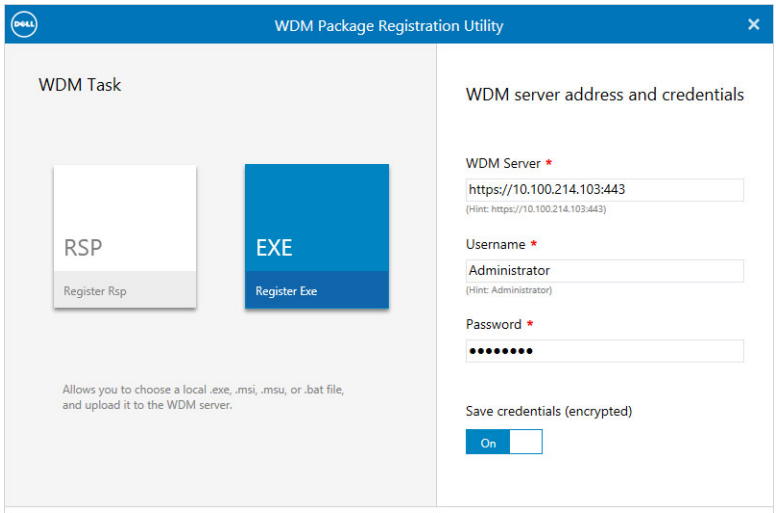


Figure 18. WDM Package Registration Utility

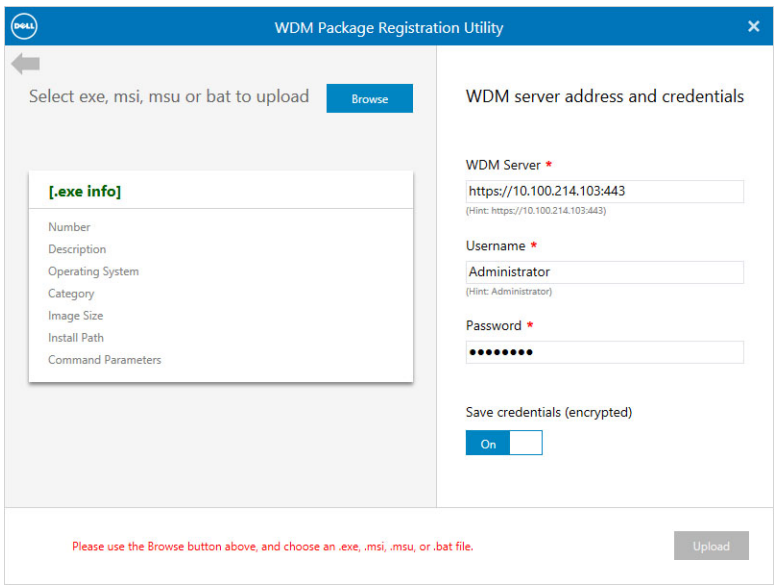


Figure 19. WDM Package Registration Utility

1 Download and open the Package Registration Utility dialog box.

2 Click the **EXE** tile displayed on the WDM Package Registration Utility dialog box.

3 Browse the exe, msi, msu, or bat files only or package to upload.

The following details of the selected package is displayed.

- Name
- Description
- Operating System
- Category
- Image Size
- Install Path

- Command Parameters

4 From the Operating System drop-down list, select the operating system.

5 Enter a valid thin client path to install the package in the provided field.

6 Enter the command parameters in the provided field.

7 Click **Upload**.

PCoIP Device Configuration

Use the **PCoIP device configuration** page to create and deploy new PCoIP device configuration packages.

To create a new PCoIP device configuration package, do the following:

1 Click the **Register PCoIP Package** option to download the PCoIP device configuration utility.
The screen displays the following menu options:

- On the upper-right corner of the page, click either of the following ThreadX versions for which you want to create a PCoIP device configuration package:
  - Version 4.X
  - Version 5.X
- Enter the Package name and the description details in the **Package Name** and **Description** field.
- **System**

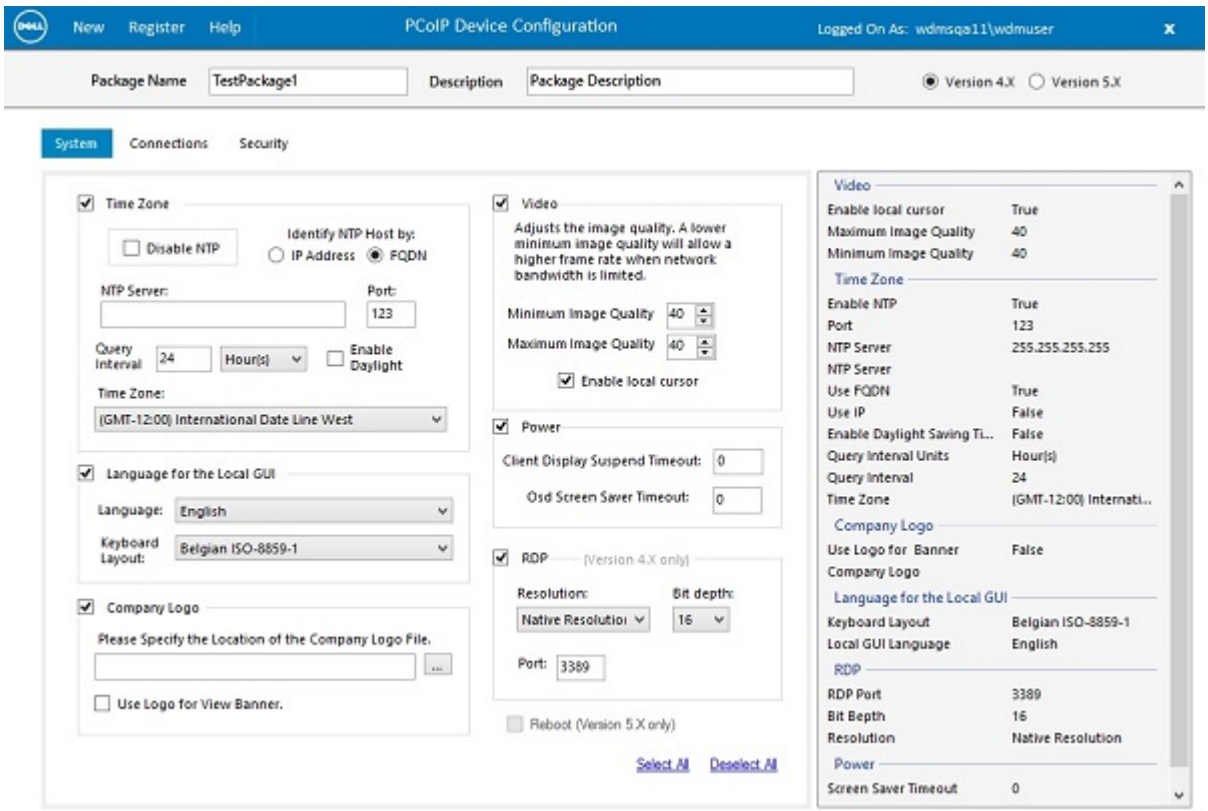


Figure 20. System Version 4.X

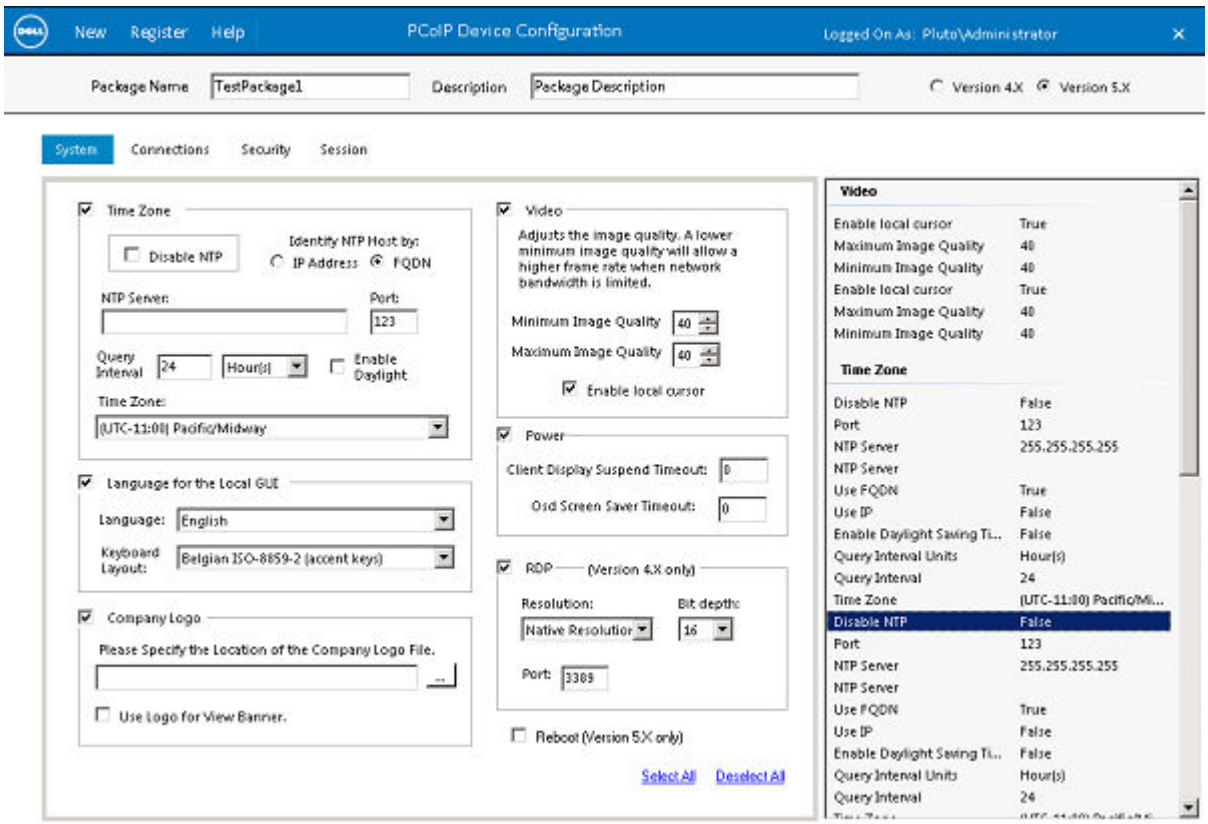


Figure 21. System Version 5.X

Table 9.

Time Zone Configuration	Provide the following details: • Select the mode through which you want to identify the Network Time Protocol (NTP) Host. • Enter the IP address or the host name of the NTP server. • Enter the Port number, the Query Interval in minutes and select **Enable Daylight Saving Time**, if it is applicable to the time zone you are selecting. • Select the time zone from the drop-down list.
Language for the Local GUI	Provide the local language and keyboard details for the localized GUI.
Company Logo	Select the option to add the Company logo. Browse and navigate to the specific location to select the .BMP file. The company logo must be a 24 bmp bitmap which should not exceed 256 pixels by 64 pixels.
Video	Provide the minimum and maximum image quality details. Select the check box to enable or disable local cursor feature.
Power	Select the option to set the Client Display Suspend Timeout and Osd Screen Saver Timeout. The units of the time should be in seconds.

	To Enable the setting, the Timeout range is 10 to 14400 seconds and to disable enter 0.
RDP This option is applicable only to ThreadX v4.X	Provide the RDP connection details.
Reboot This option is applicable only to ThreadX v5.X.	Select this check box along with the **Company Logo** check box. This results in rebooting of the ThreadX device after deploying the package that contains the Company Logo.

- **Connections**

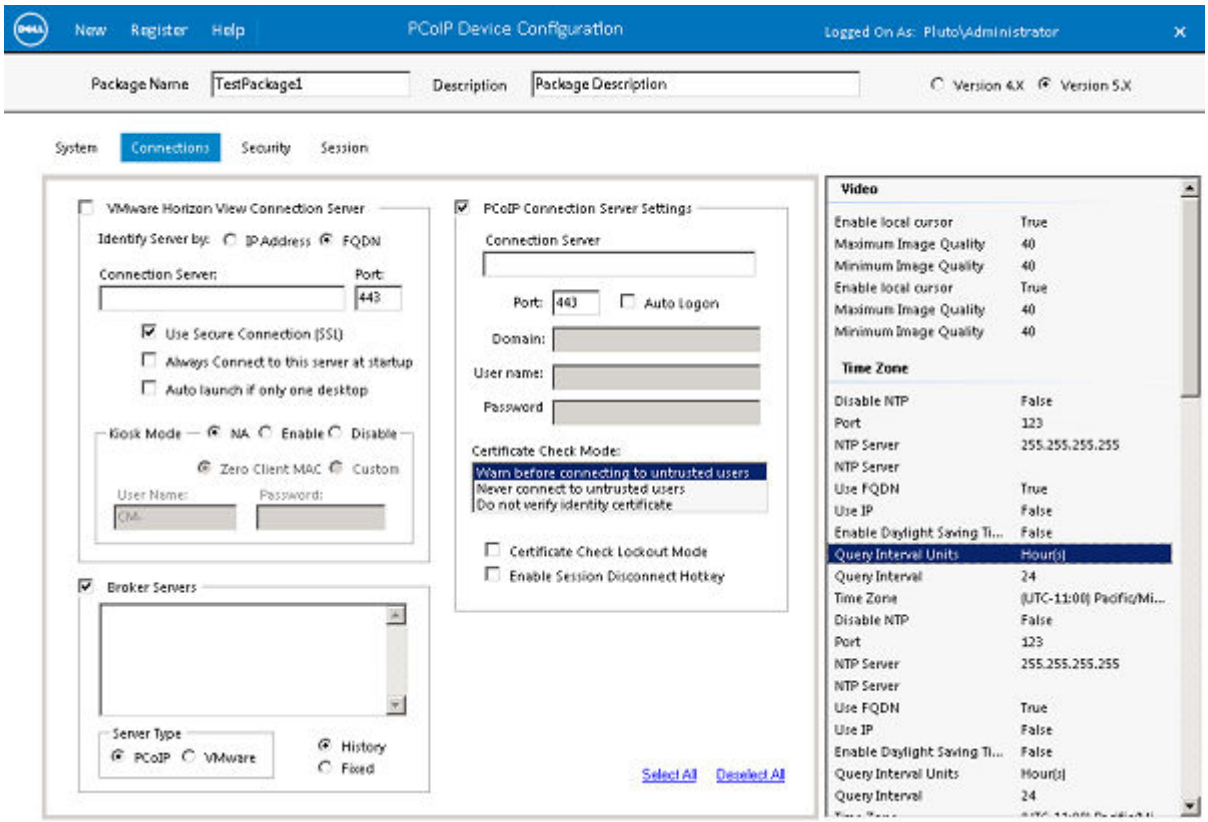


Figure 22. Connections

Table 10.

VMware Horizon View	Provide the following details for the VMware Horizon view connection server: • Select the mode through which you want to identify the connection server. • Enter the IP address or the host name of the connection server. • Enter the connection port number and select the connection options as per your requirement. • Click **Kiosk Mode** if the device is to function as a Kiosk type terminal.
PCoIP Connection Server Settings	Select the option to provide the details on the following: • Connection server

	• Port number • Domain • User Name • Password • Certificate Check Mode Based on your requirement, select the following check boxes: • Certificate Check Lockout Mode • Enable Session Disconnect Hotkey
PCoIP or VMware	You can select the server type as PCoIP or VMware. A maximum of 25 servers can be added for both PCoIP as well as VMWare.

- **Security**

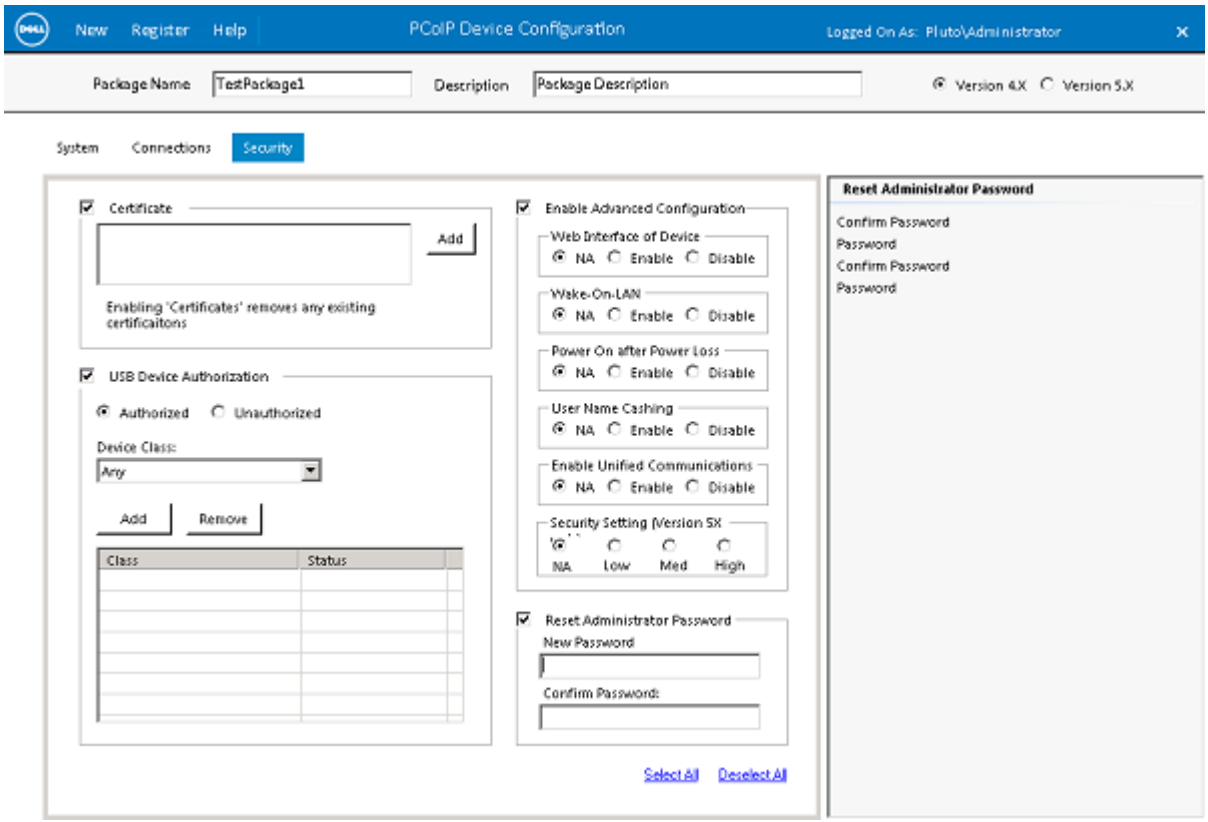


Figure 23. Security

Table 11.

Certificate	Select the option to enter the content of the certificate.
USB Device Authorization	Provide the USB permission details (Authorized and Unauthorized) for the device.
Enable Advanced Configuration	Select the options if you want to enable the web interface of device, Wake-on-LAN, Power on after Power Loss, User Name Caching and Enabling Unified communications.

Reset Administrator Password	If you want to reset the password of the device administrator, then select the option and provide the new password.

- **Session** (Version 5.X)

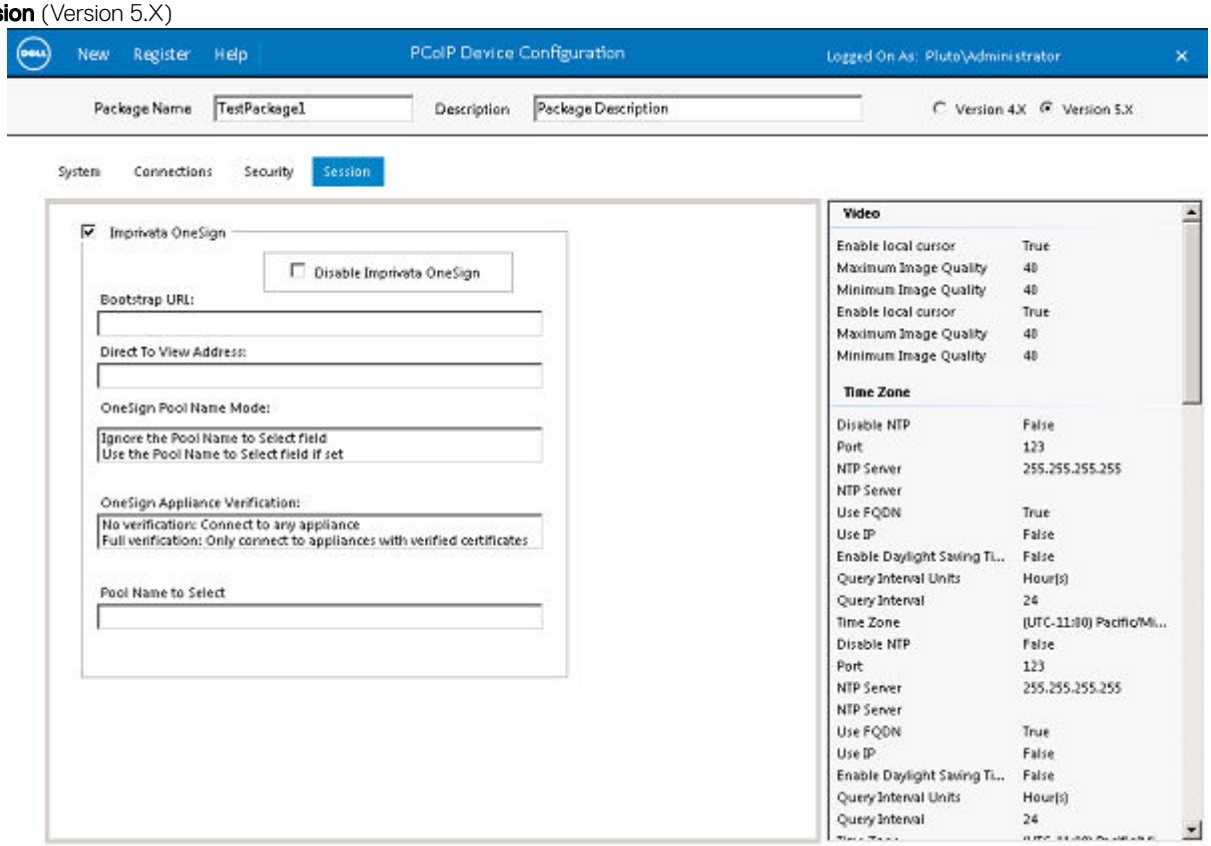


Figure 24. Session

Table 12.

Imprivata OneSign	Select this option to enable Imprivata OneSign.
Disable Imprivata OneSign	Select this option to disable Imprivata OneSign.
Bootstrap URL	Enter the Bootstrap URL in the provided field.
OneSign Pool Name Mode	Select the preferred option. The options are: · Ignore the Pool Name to Select field · Use the Pool Name to Select field if set
OneSign Applicable Verification	Select the preferred option. The options are: · No verification: Connect to any appliance · Full verification: Only connect to appliance with verified certificates.
Pool Name to Select	Enter the Pool name in the provided field.

2 Click the **Register** tab to save the current configuration and finish the process.

3 Click the **New** tab to create new PCoIP device configuration package.

NOTE: For information about upgrading the ThreadX devices from version 4.X to version 5.X, see Upgrading the ThreadX 4.X devices to ThreadX 5.X from WDM.

6

Updates

The Update page provides you the summary of Scheduled Jobs, Recurring Updates, Repository sync Jobs, Peer assisted delivery details. You can also create Profile and DDC.

Topics:

Jobs

This parameter helps you to view the schedule agent updates, images, configurations, or other packages from devices or application pages. You can view the details of the scheduled jobs as following:

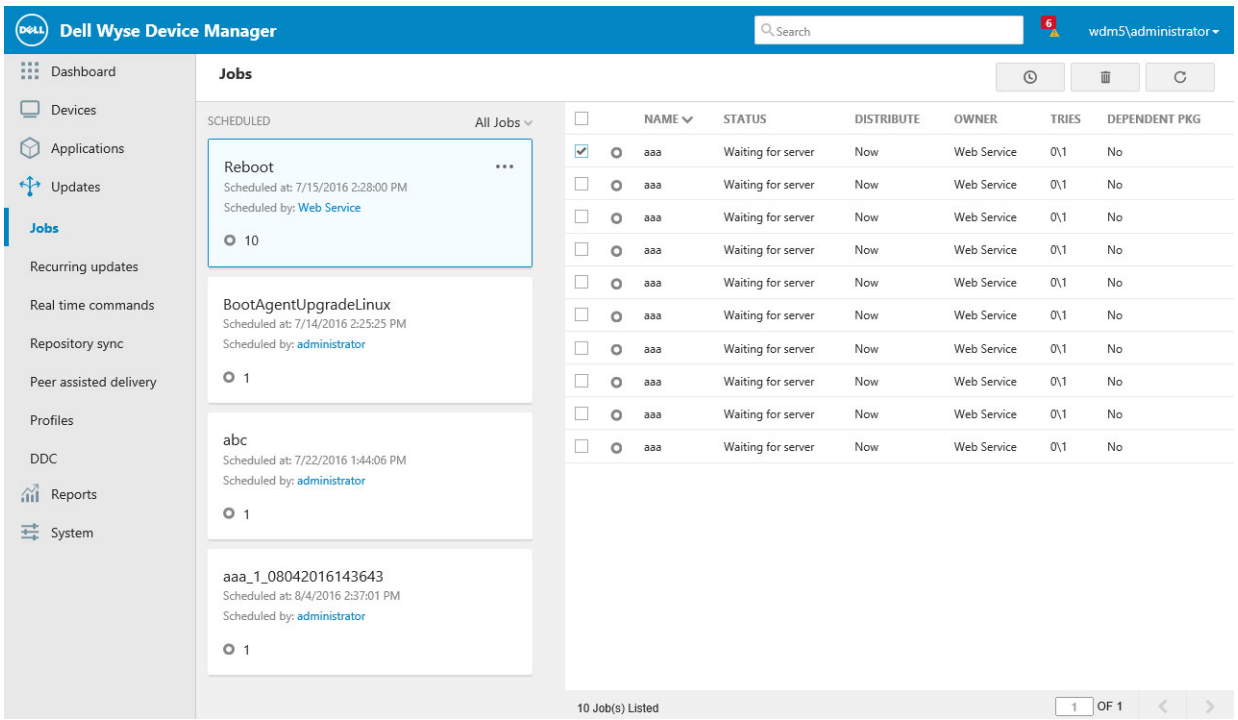


Figure 25. Jobs

- All jobs — If you select All Jobs, the Scheduled Jobs of all the Users are listed.
- My jobs — If you select My Jobs, only the Scheduled Jobs of the logged in user are listed.

1 To reschedule the job, Select the distribute option as **Now** if you prefer to distribute the package or you can select the distribute option as **A specific date and time** and enter your preferred date and time of package distribution. Click the **On/Off** option to enable or disable the **Retry failed updates** option.

2 Click **Reschedule**.

3 Click **Delete** to delete the job.

Recurring Updates

This parameter helps you to view the schedule agent updates, images, configurations or other packages as recurring updates from devices or application pages.

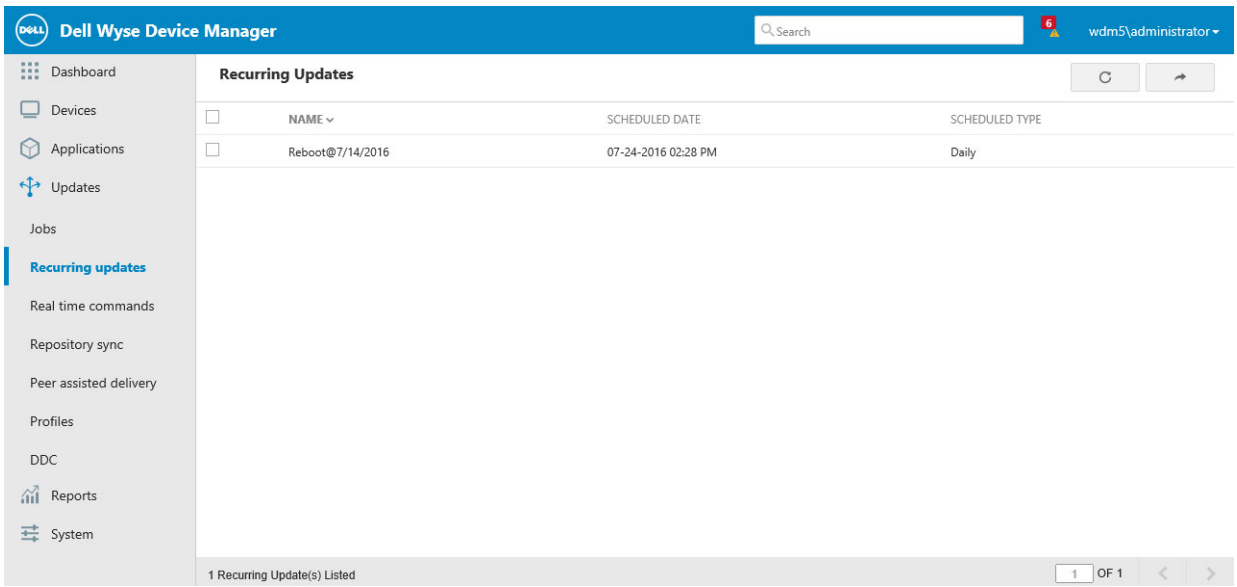


Figure 26. Recurring Updates

1 Click **Refresh** option to refresh the page.

2 Click **Reschedule** option to reschedule the package distribution.

a Enter the following package distribution details:

1 Name of Recurring update.

2 From the **Recur** drop-down list, select the day for package distribution.

3 Enter the start and end date of the package distribution.

4 Enter the time duration of the package distribution.

5 Click **Reschedule**.

3 Click **Delete** option to remove the jobs.

4 Click **Export** option to export the device in .csv or .txt (tab delimited) format.

Real Time Commands

In this category, you can view the details of the Real time commands scheduled to the devices. You can also perform the following operations.

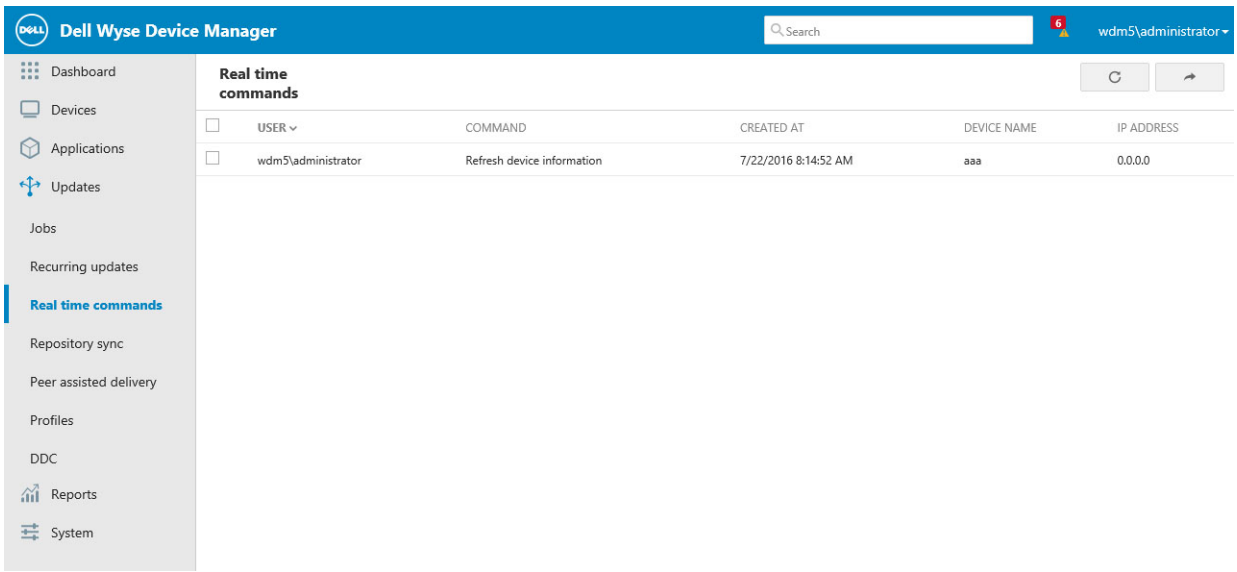


Figure 27. Real Time Commands

1 Click **Refresh** option to refresh the page.

2 Click **Delete** option to remove the command.

3 Click **Export** option to export the device in .csv or .txt (tab delimited) format.

Repository Sync

In this category, you can view the Remote Sync jobs that are scheduled to the Remote Repository created.

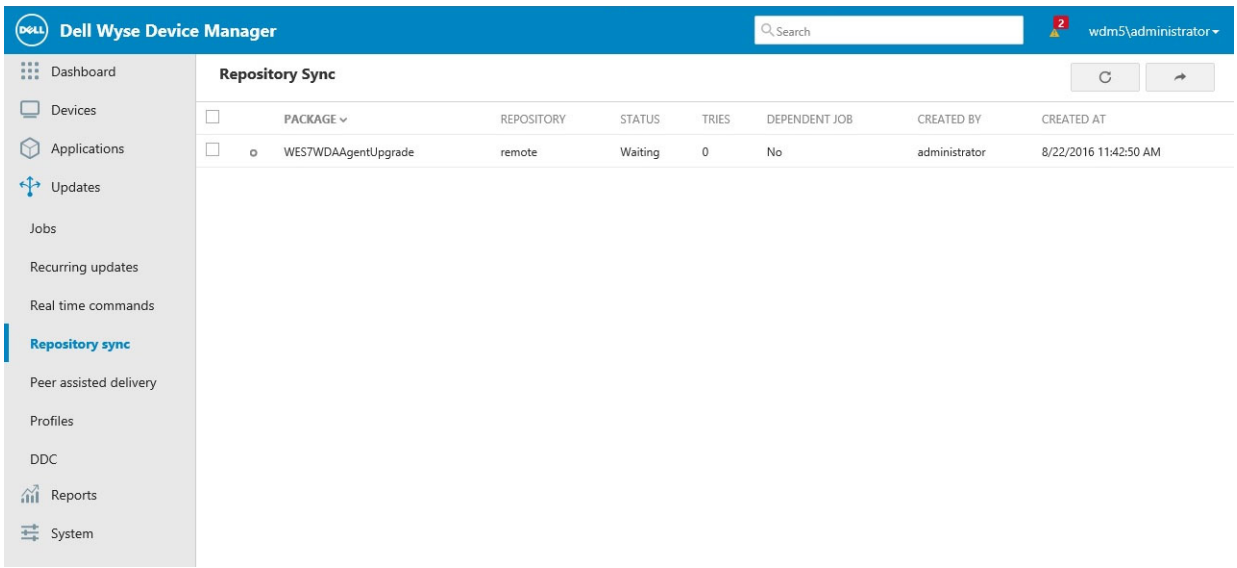


Figure 28. Repository Sync

Peer Assisted Delivery

In this category, you can view the details of the Peer Assisted deployment schedule for Subnet. For more information about PAD, see Peer Assisted Deployment and Configuring PAD.

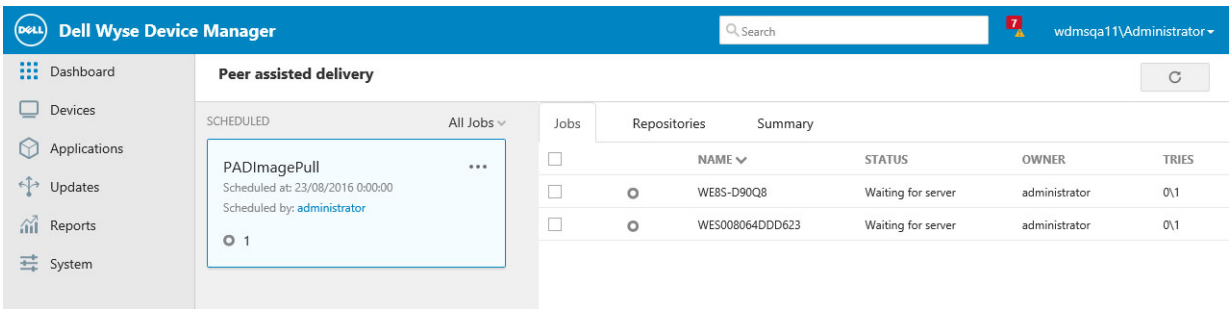


Figure 29. Peer Assisted Delivery

Profiles

The **Profiles** page enables you to deploy a predefined configuration on a specified group of devices. You can create the configurations by using the Dell Wyse Configuration Manager (WCM) and save them in a specified repository. A repository is a system where the configurations are saved. Thin client devices connect to these repositories through HTTP , FTP, or CIFS and download the configurations. For more information, see the *Dell Wyse Configuration Manager Administrator's Guide* available on the Dell Wyse support site. Profiles are unique for an operating system and you can apply only one configuration on a single group of devices at any given time.

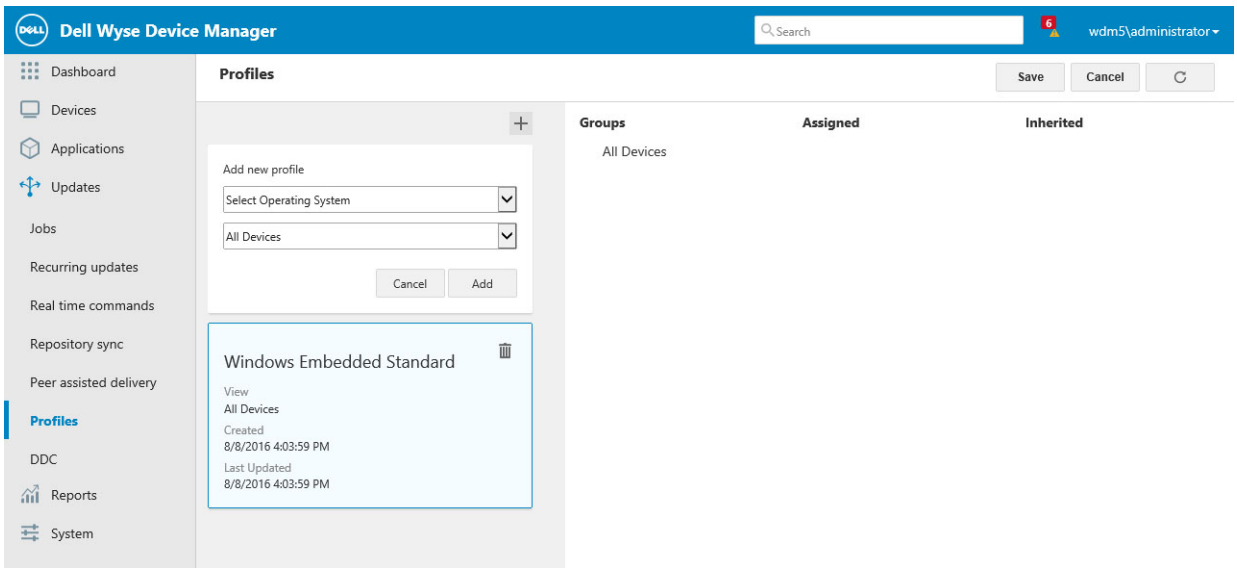


Figure 30. Profiles

This parameter helps to add new profile and provides the details such as, **Groups**, **Assigned**, and **Inherited**.

To add a new profile complete the following task:

1 From the **Select Operating System** drop-down list, select your preferred operating system.
2 From the drop-down list, select the preferred view to be deployed for a particular profile.
3 Click **Add** to include the new profile to the groups.

For information about PM supported devices, configuration package deployment and deleting a profile configuration package, see Identifying PM Supported Devices, Deploying a Configuration Package Using Profile Manager, Creating a Device Configuration Package, Enabling Profile Manager in System and Deleting a PM Configuration Package.

Identifying Profile Manager Supported Devices

1 In the **Device** page, select a device.

2 Click the view details option and check the capabilities section.
3 In the capabilities section, look for WCM support.
4 The device is profile manager capable if it is in the following condition:
   - Green color: The device is profile manager capable.
   - Red color: The device is not profile manager capable.
5 To make the device profile manager capable, deploy the latest WDA agent available in WDM.

NOTE: For HAgent supported devices, register the WCM client package and push to the devices having HAgent.

When these devices check-in to the WDM server, the Hserver service recognizes these devices based on the value they send in the WCMSUPP tag.

Deploying a Configuration Package Using Profile Manager

To create a configuration package using profile manager follow these steps:

1 On the WDM web UI, click **Updates** > **Profiles**.
   The **Profiles** page is displayed.
2 From the **Select Operating System** drop-down list, select your preferred operating system.
   The drop-down box displays only those operating systems for which you have not created configuration packages. You can create only one profile per operating system. The leaf configuration takes precedence over parent but WTOS is an exception.
3 From the drop-down list, select the preferred View on which the particular profile needs to be deployed.
4 Click **Add** to include the new profile to the groups.
5 Select a WCM configuration from the **Assigned** drop-down list.
   This list displays all the configuration packages that you have created for the selected operating system using the WCM application.
6 Click **Save**.

Whenever there is any change in configuration from the existing configuration on the client, PM applies the updated configuration whenever the client checks in. The **Update Now** window is displayed on the client, and when you click **OK** PM applies the updated configuration.

NOTE: Please note the differences between the XML configurations and the JSON configurations.

Table 13. Differences between XML and JSON configurations

XML Configurations	JSON Configurations
They can be created only from MMC UI.	They can be created from Web UI and MMC UI.
They can be created only for Windows OSs.	They can be created for Windows, WTOS and Linux OSs.
They can be deployed only for devices with HAgents.	They can be deployed to devices with WDA.
They are not displayed under assigned drop-down list on Web UI.	

Deleting a PM Configuration Package

To delete a configuration package:

1 On the WDM Web UI, click **Updates** > **Profiles**.
   The existing profiles are listed on the page.
2 Select any profile, and click the **Delete** icon.
   You will be prompted to proceed with the delete operation or cancel it.
3 Click **Delete** to delete the configuration package.

NOTE: You can only create one profile for a particular operating system at any given point. If you want to create another profile for the same operating system, you must delete the existing package and create a fresh one.

Default Device Configuration (DDC)

WDM allows you to easily create and manage DDCs. You can apply Images or multiple Software packages or both to the devices using DDC. DDC ensures that all the device in the Group where DDC is assigned will have same Images or Configurations assigned.

This parameter helps to add new Default Device Configuration (DDC) and provide the details such as, **Groups**, **Image**, **Packages**, and **Execute DDC**

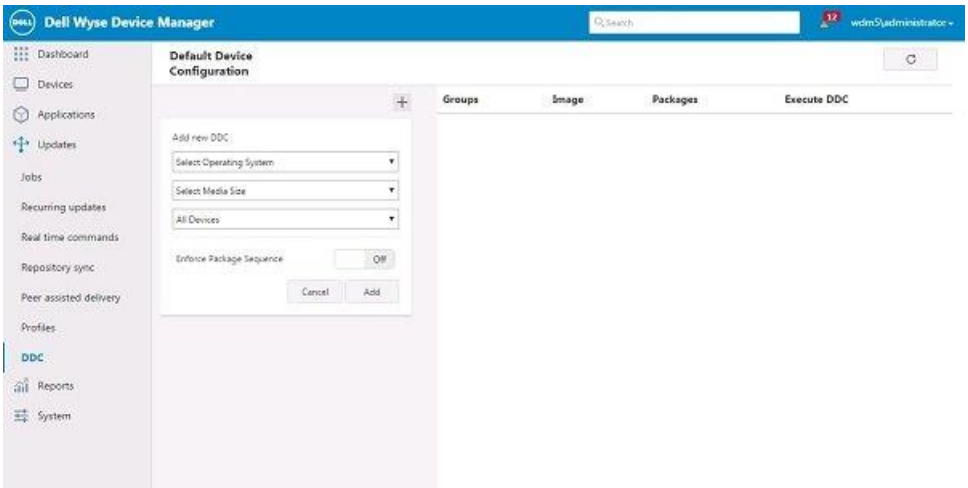


Figure 31. DDC

To add a new DDC, complete the following task:

1 From the **Select Operating System** drop-down list, select your preferred operating system.

2 From the **Select Media Size** drop-down list, select your preferred media size.

3 From the drop-down list, select the preferred view to be deployed for a particular profile.

4 Click the **On/Off** option to enable or disable the **Enforce Sequence** option. Depending on whether or not you want the packages that are a part of the DDC to be the only packages allowed for the devices (that is no other packages can be sent to the devices), select or clear Enforce Sequence.

> **NOTE: Selecting Enforce Sequence may interfere with any packages that are sent or scheduled to a device outside the DDC process.**

5 Click **Add** to include the new DDC to the groups.

6 Select an Image from the Image drop-down list.

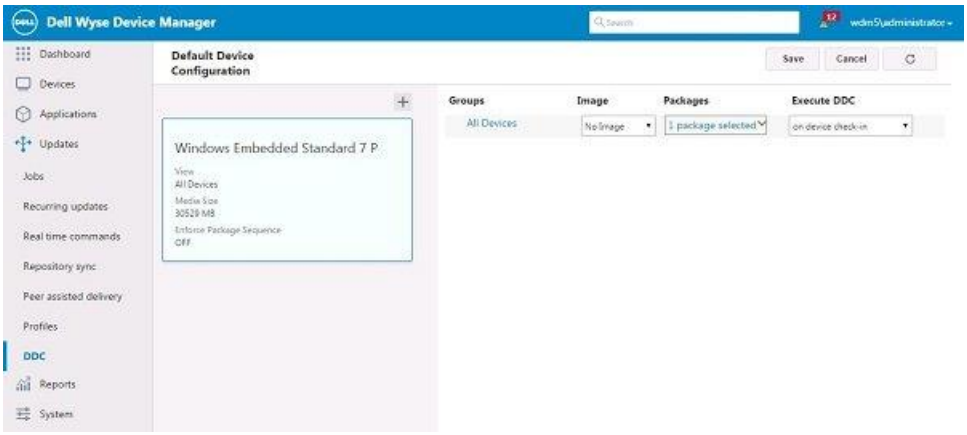


Figure 32.

7 Select a software package from the packages drop-down list.

8 Specify Execute DDC either Device Checks in or Every Day at Specific Time.

9 Click **Save**.

8

Reports

In the Web UI you can generate the log reports on the daily basis, Weekly basis, or monthly basis. The report generated can be viewed, edited, and saved.

Topics:

Creating a Log Report

Log Reports provide important information about the events or activities went into WDM server related to WDM components. It allows you to easily see what you want, when you want it. After you create a report, WDM automatically saves the report in the Reports tab, so you can use it again whenever you want. There is no need to create the same report once you have created it. Every time you view the report you get the latest information to the criteria you set up in the report.

NOTE: Reports are not static. If information changes (for example, new devices are discovered or new logged information is generated) a report will display the new information (assuming it fits in the criteria of the report).

Use the following guidelines to create, view, and save a log report:

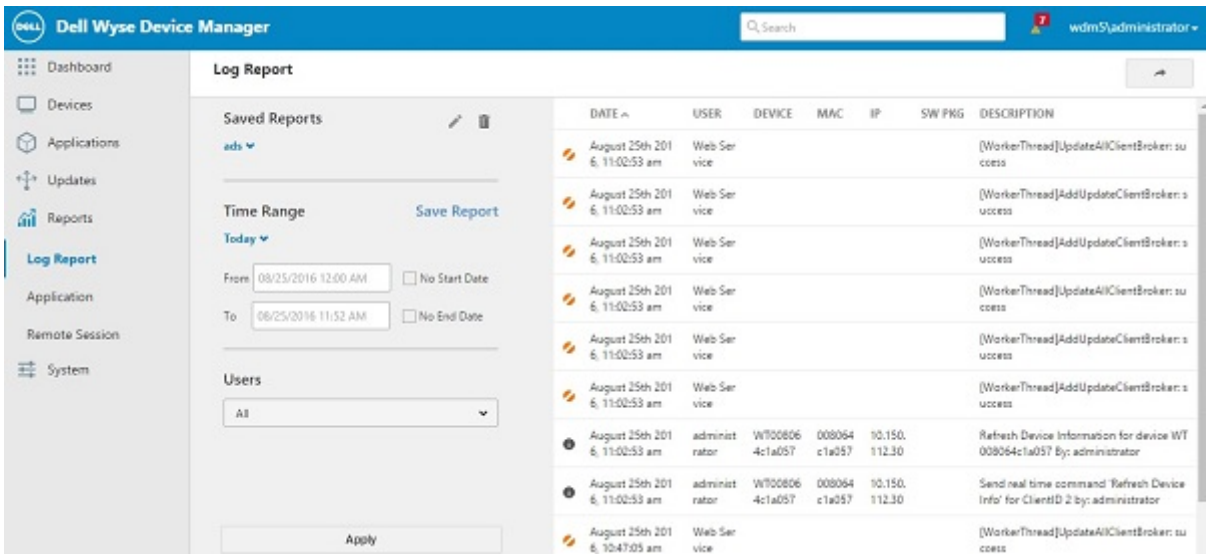


Figure 33. Log Report

1. Click **Reports** > **Log Report**.
2. Select the desired ranges and select the number of users whose activity your log report will include. If you wish to restrict the report to the activities of a specific user, select the user below and if you wish to show the activities of all the user, select **All** in the drop-down list.
3. Click **Apply**.

   When your log report is compiled, it is displayed on the right pane of the page.
4. To save the report, click the **Save Report** link in the **Time Range** area.

5 In the **Save Report** dialog box, enter the report name, and click **Save**.

The saved report is listed in the **Saved Reports** drop-down list.

NOTE: To save a log report as a .txt file or .csv file, click the Export icon on the upper-right corner of the page and select either .csv or .txt (tab delimited) based on your preference. To use the report in the future, select the report from the Saved Reports. The saved reports can be edited or deleted as per your requirement.

Creating an Application Report

This enables the user to create a report for listing the devices that have specific software installed and version selected by the user.

1 Click **Reports** > **Application**.

The **Application Report** page is displayed.

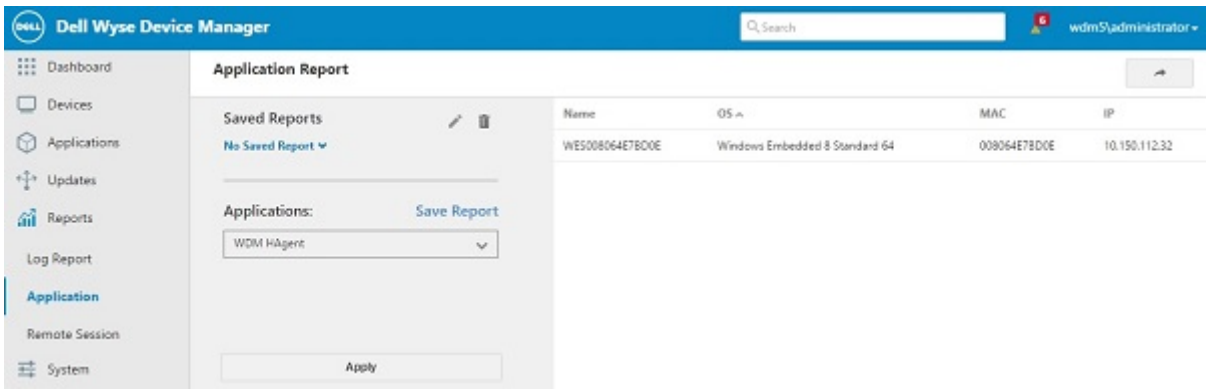


Figure 34. Application Report

2 From the **Applications** drop-down list, select your preferred application for which you want to view the report, and then click **Apply**.

When your application report is compiled, it is displayed on the right pane of the page.

3 To save the report, click the **Save Report** link in the **Applications** area.

4 In the **Save Report** dialog box, enter the report name, and click **Save**.

The saved report is listed in the **Saved Reports** drop-down list.

NOTE: To save an application report as a .txt file or .csv file, click the Export icon on the upper-right corner of the page and select either .csv or .txt (tab delimited) based on your preference. To use the report in the future, select the report from the Saved Reports. The saved reports can be edited or deleted as per your requirement.

Creating a Remote Session Report

Remote session Reports provide connection information on all devices in WDM based on the filter criteria defined during report generation. It allows you to see what user, for how long connected to what type of broker connection. After you create a report, it is displayed on the right pane of the page. You can export this report and use it later.

Use the following guidelines to create, view, and save a Remote Session report:

1 Click **Reports** > **Remote Session**.

The **Remote Session Report** page is displayed.

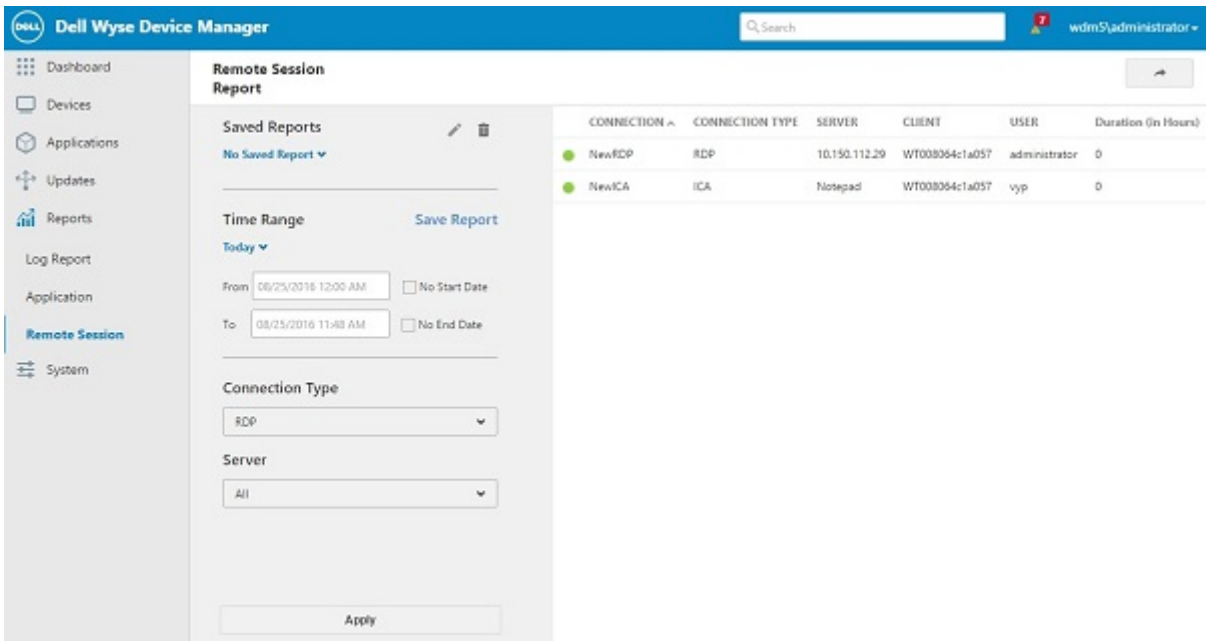


Figure 35. Remote Session

2 From the **Time Range** drop-down list, select the desired time range or duration for which you want to generate the report. Reports can be generated for the present day, previous day, last 7 days, last 30 days or All time. To specify your own time range, click **Custom** and specify the start date and end date.

3 You can generate the report based on the following search criteria:

- From the **Connection Type** drop-down list, select your desired connection type.
- From the **Server** drop-down list, select your desired server name or IP.

4 Click **Apply**.

When your application report is compiled, it is displayed on the right pane of the page.

5 To save the report, click the **Save Report** link in the **Time Range** area.

6 In the **Save Report** dialog box, enter the report name, and click **Save**.

The saved report is listed in the **Saved Reports** drop-down list.

NOTE: To save an Remote session report as a .txt file or .csv file, click the Export icon on the upper-right corner of the page and select either .csv or .txt (tab delimited) based on your preference. To use the report in the future, select the report from the Saved Reports. The saved reports can be edited or deleted as per your requirement.

9

System

The **System** page in the web UI enables you to configure the following options:

- **Subnets**: The Subnets page helps you to view the system broadcast IP, active IP, subnet mask and description. Subnets are auto-created when the device gets checked-in to WDM Server. You can also configure subnet manually. To manually configure the subnet, see Setting Subnets Manually.
- **Repositories**: The Repository page contains the details of the Master repository and remote Repository. To create remote repository, see Registering Remote Repositories.
- **Accounts**: The Accounts page helps you to view the details of the users. You can also perform the following tasks:
  - Adding Users and Groups from Active Directory.
  - Adding Users from Local Computer Accounts.
  - Editing User Permissions.
  - Deleting Users .
- **Console**: The **Console** page helps you to view the following details:
  - Device Health Status
  - Custom Group folders
  - Remote Sessions
  - Default Device Configuration (DDC)
  - Profile Manager
  - Management Server alias name

  For more information, see Console.
- **Device Discovery**: The Device Discovery page helps you to view the agent discovery behavior after the first check-in to management server and the DHCP discovery details. For more information see Configure Device Discovery .
- **Services**: The Services page helps you to view the TFTP Server and the Wake on Lan details. For more information, see About Services.
- **Logging**: This parameter helps you to configure the the logging levels for different WDM components. Higher logging level causes more data to be stored in the database. This could result in server slow down. For more information, see Configure Logging Levels.
- **Scheduling**: The Scheduling page helps you to view the details such as maximum simultaneous updates, timezone of schedule updates, maximum retry attempts for rescheduling failed updates and auto sync remote software repositories. For more information see Scheduling.
- **Peer Assisted Deployment**: The Peer Assisted Deployment page helps you to do the following:
  - Prerequisites for PAD.
  - Configuring PAD.
- **Wyse ThinOS**: This parameter helps you to view the WTOS INI root path and the check in path. For more information see Wyse ThinOS.

Topics:

- Adding Users and Groups from Active Directory
- Editing User Permissions
- Deleting Users
- Console
- Configure Device Discovery
- About Services
- Configure Logging Levels
- Scheduling
- Peer Assisted Deployment
- Wyse ThinOS

Setting Subnets Manually

With WDM, you can add and configure subnets manually.

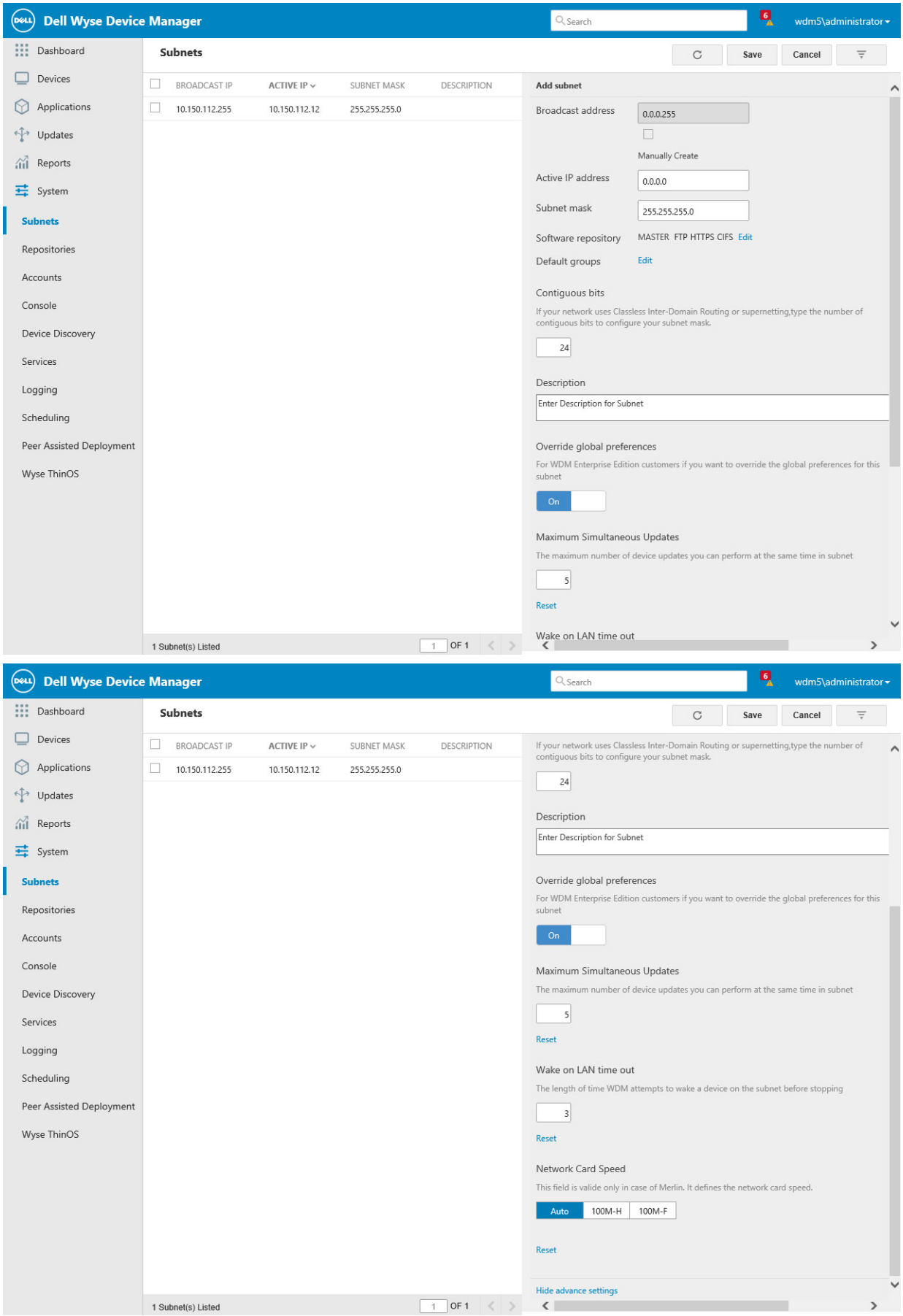


Figure 36. Add Subnet

To add and configure a subnet:

1 In the WDM Console, expand **System** and click the **Subnet** option.

2 Click **Add subnet** option.

3 Complete one of the following task:

- If you want to provide a broadcast address for the subnet manually, select **Manually create** and enter the **Broadcast Address**.
- If you do not want to provide a broadcast address for the subnet manually, enter the **IP Address** (Type a valid IP address from the subnet), **Subnet Mask** (Type the subnet mask for the subnet), and **Contiguous Bits** (if your network uses Classless Inter-Domain Routing or supernetting, type the number of contiguous bits to configure your subnet mask).

4 Enter a **Description** to identify the subnet in the WDM Database.

5 Complete one of the following task:

- If you do not want to override the global preferences for this subnet, click **OK**.
- **(WDM Enterprise Edition only)** If you want to override the global preferences for this subnet, select **Override Global Preferences**, complete the subnet preferences using the following guidelines and click **OK**:
  - **Maximum Simultaneous Updates** - The maximum number of device updates you can perform at the same time in the subnet.
  - **Wake On LAN Time Out (Secs.)** - The length of time WDM attempts to wake a device on the subnet before stopping.
  - **Network Card Speed** - This field is valid only in case of Merlin. It defines the network card speed. The possible values are Auto, 100M-F, 100M-H.

The information about the subnet and its preferences are now stored in the WDM Database and WDM can discover the devices on the subnet.

NOTE: Subnet should match with the contiguous bits provided.

Registering Remote Repositories

WDM Enterprise Edition allows you to install multiple repositories on your network. Remote Repositories help save network bandwidth because they store and distribute software updates locally to devices that reside in the same subnet as each repository.

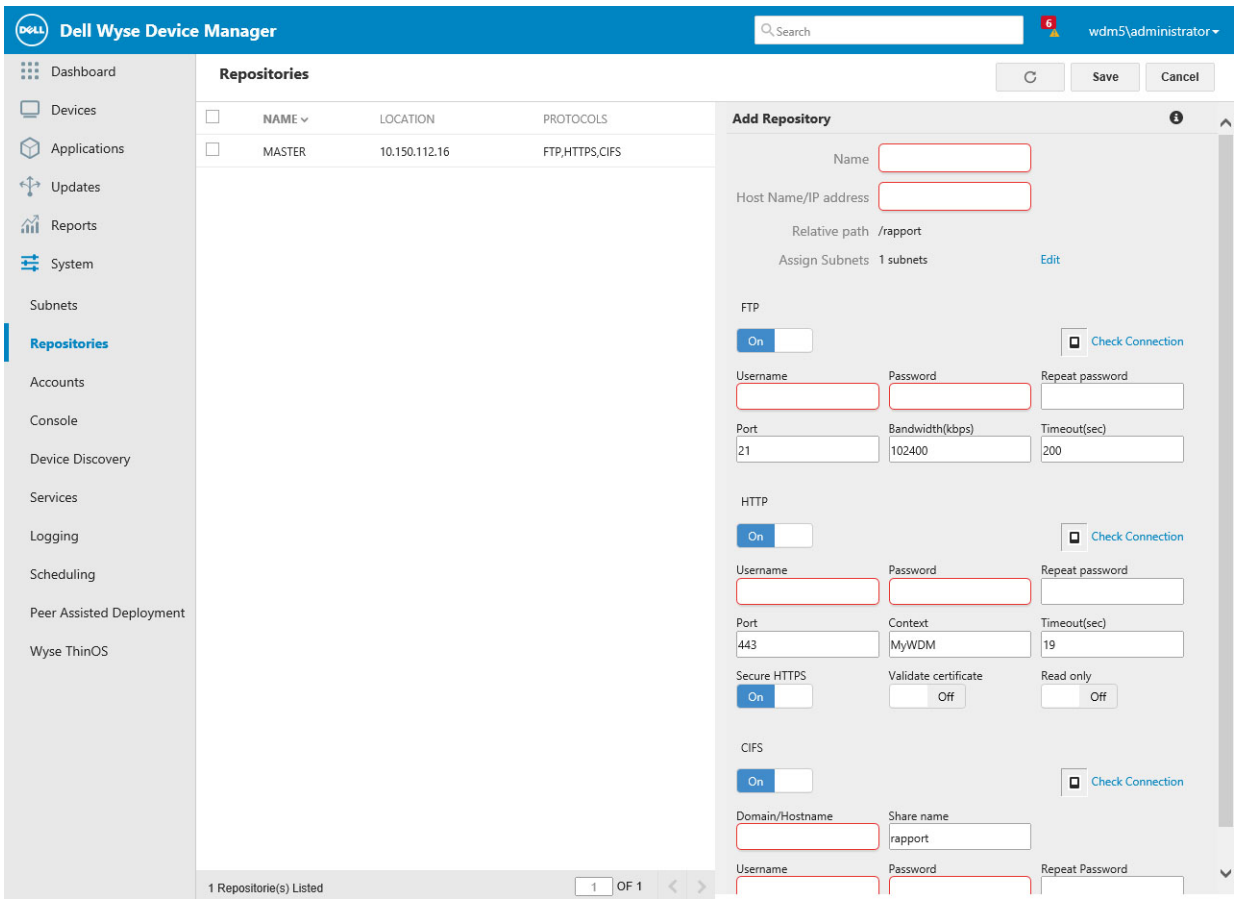


Figure 37. Registering Remote Repositories

You must configure the following points before you register remote repositories:

- WDM always names the first Repository *Master*. Any additional Remote Repositories that you install can be named anything other than Master.
- If you do not install multiple Remote Repositories, then WDM uses the Master Repository for all subnets.
- If you deployed WDM components separately, then it is recommended that you install the Master Repository on a machine on the same subnet as where you installed the other WDM components.

Before you register, make sure that you have successfully installed the following:

- WDM Enterprise Edition on your network.
- Any Remote Repositories, so that you can connect to them.

To register a Remote Repository:

1 In the WDM Console, expand **System**.

2 Click the **Repositories** option. To configure a new repository click the **Add Repository** option and complete the configurations using the following guidelines:

- **Repository Information area:**
  - **Name** - Provide the name to identify the Software Repository.
  - **Host Name/ IP address** - Provide the **Host Name** or **IP address** of the server where you want to configure the repository.
  - **Relative Path** - Provides the root path of WDM software repository.
  - **Assign Subnets** - Allows you to assign a subnet to a repository.
- **FTP area:**

- **Username** - Username for FTP repository access.
- **Password** - Password for FTP repository access.
- **Repeat Password**- Re-enter the password for FTP repository access to confirm the password.
- **Bandwidth** - How much bandwidth in Kbps to utilize for data transfer to and from the Software Repository.
- **Timeout (sec)** - Time in seconds that the connection for each session should remain open.

- **HTTP area:**
  - **Username** - Username for HTTP repository access
  - **Password** - Password for HTTP repository access.
  - **Repeat Password** - Re-enter the password for HTTP repository access to confirm the password.
  - **Port Number** - Displays the port number for HTTP communication. The default port number for HTTP is 80, and for HTTPS is 443.
  - **Context** - Displays the virtual directory path for HTTP communication.
  - **Timeout (sec)** - Time in seconds that the connection for each session should remain open.
  - **Secure HTTPS** - If checked, the HTTP communication for the repository is secure.
  - **Validate Certificat** - If checked, the Certificate validation for HTTPS communication is enabled.
  - **Read Only** - If checked, the the repository will be read only.
- **CIFS area:**
  - **Domain/Host Name** - Give the domain or host name of the repository server.
  - **Share Name** - Give the name of the shared folder from where package needs to be deployed.
  - **Username** - Give the user name that has access to the shared folder.
  - **Password** - Password for CIFS user that has access to the shared folder.
  - **Repeat Password** - Confirm the password for CIFS user that has access to the shared folder.

3 Click **Save**.

NOTE: WDM tests the connection to the Remote Repository that you added to ensure that it is properly set up . You can test the connection to a Remote Repository at any time by clicking the Check Connection.

The new Remote Repository is now successfully set up and registered in the WDM Database. You can now assign the Remote Repository to a subnet.

NOTE: WDM stores every package that you register in its Master Repository. You can synchronize Remote Repositories whenever you perform an update for a device on a subnet that has access to a local repository.

Adding Users from Local Computer Accounts

You can add WDM users from local computer accounts.

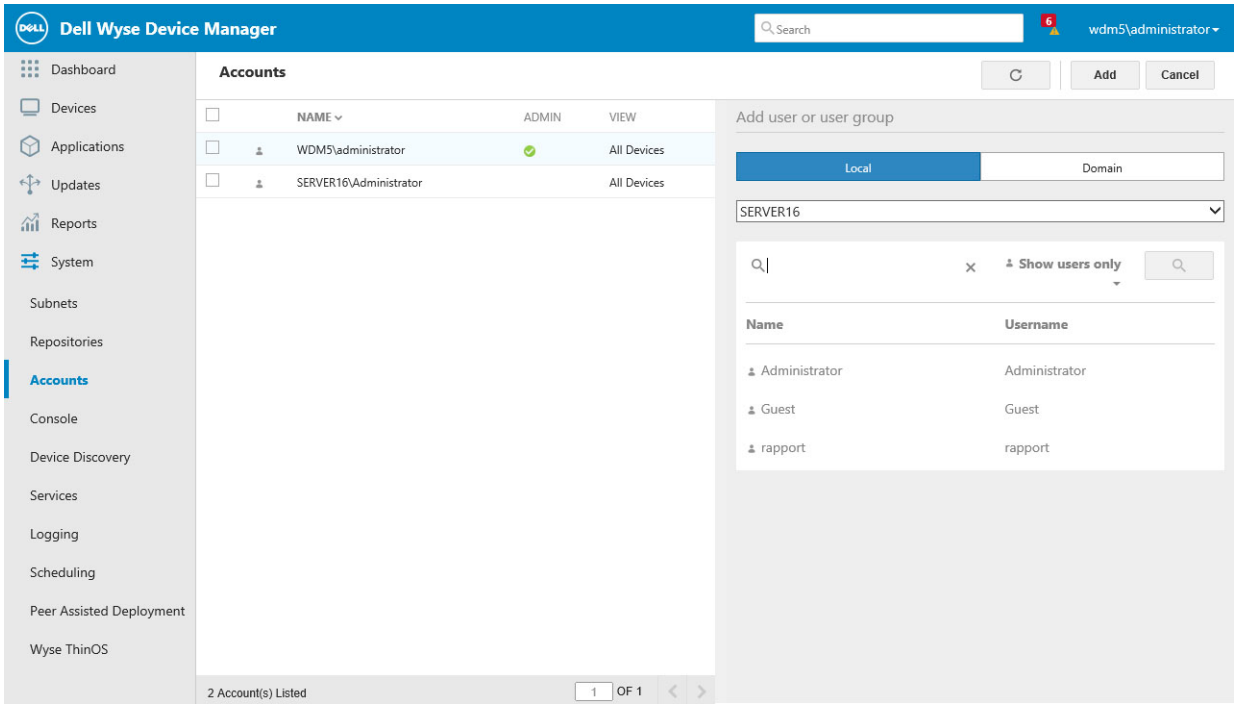


Figure 38. Accounts

NOTE: Before you can add a WDM user, the user must already exist in the list of users for the Windows Domain where you installed WDM.

To add a user from a local computer account:

1 In the WDM Console, expand **System**.
2 Select the name of the user you want to add as a WDM user and click **Add**.
3 Click **OK** to add the new user to the list of WDM users.

NOTE: New users do not have permissions until you edit the user permissions.

Adding Users and Groups from Active Directory

As an administrator you can add WDM users and groups from Active Directory.

NOTE: Before you can add a WDM group, the group must already exist in the Active Directory.

To add a user or group from Active Directory:

1 In the WDM Console, expand **System**.
2 Select the **Domain Controller** option if you want to select the users from the domain.
3 Enter an IP Address/name or select a Domain Controller from the list. The server on which you installed WDM must be a part of the Domain.
4 Select the search criteria option you want.

NOTE: If you select Show user only, be sure to enter the exact name of the user in the text box that becomes active.

5 Click **Search** to view the users and groups that match your criteria.
6 Click **Add** to integrate the users and groups with WDM.

Editing User Permissions

As an administrator you can edit the permissions of WDM users.

NOTE: If It is an upgrade setup from the previous version of WDM, you must reassign the permissions for all existing users before using WDM 5.7.2.

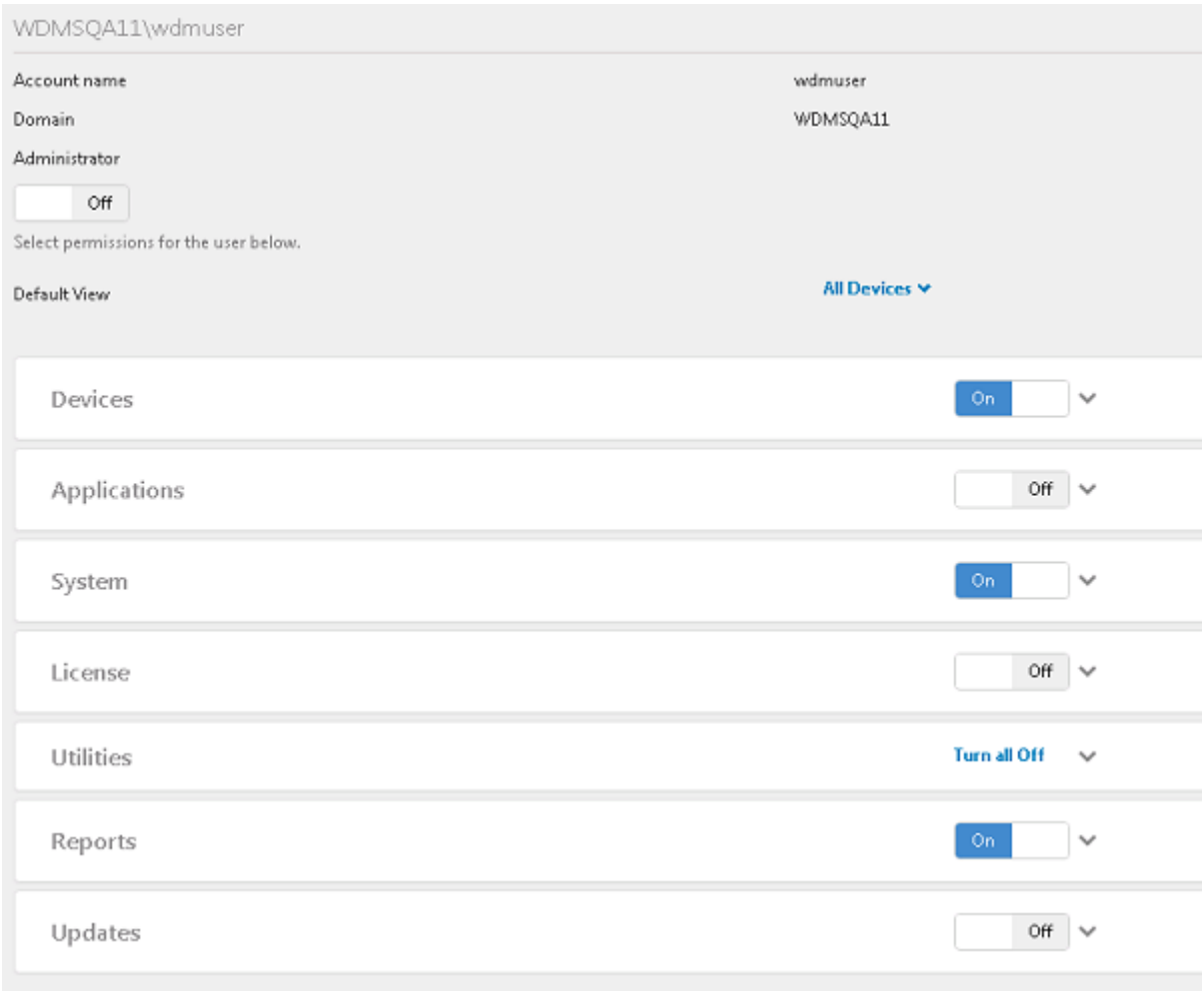


Figure 39. Accounts

NOTE: As an administrator, you can edit the permissions but the default Administrator will have all permissions and you cannot change it.

To edit user permissions:

1 In the WDM Console tree pane, expand **System**, and click **Accounts** option.
2 Click **Add** option to add user or user group.
3 Click **Local** tab to view the list of WDM users.
4 Select the user you want from the list of users and click **Add** to open the User Permissions dialog box.
5 Click On/Off option to enable or disable the **Administrator** option.

NOTE: If you enable the Administrator option, all permissions are selected.

6 Click On/Off option to enable or disable the following User Permissions:

NOTE:

On/Off permission of a group is changed based on the changes performed on specific permission under a group.

Group permission is set to Turn off all state, if one or more permissions are changed from ON to OFF state.

Group permission is set to OFF state, if all the permissions are set to OFF state.

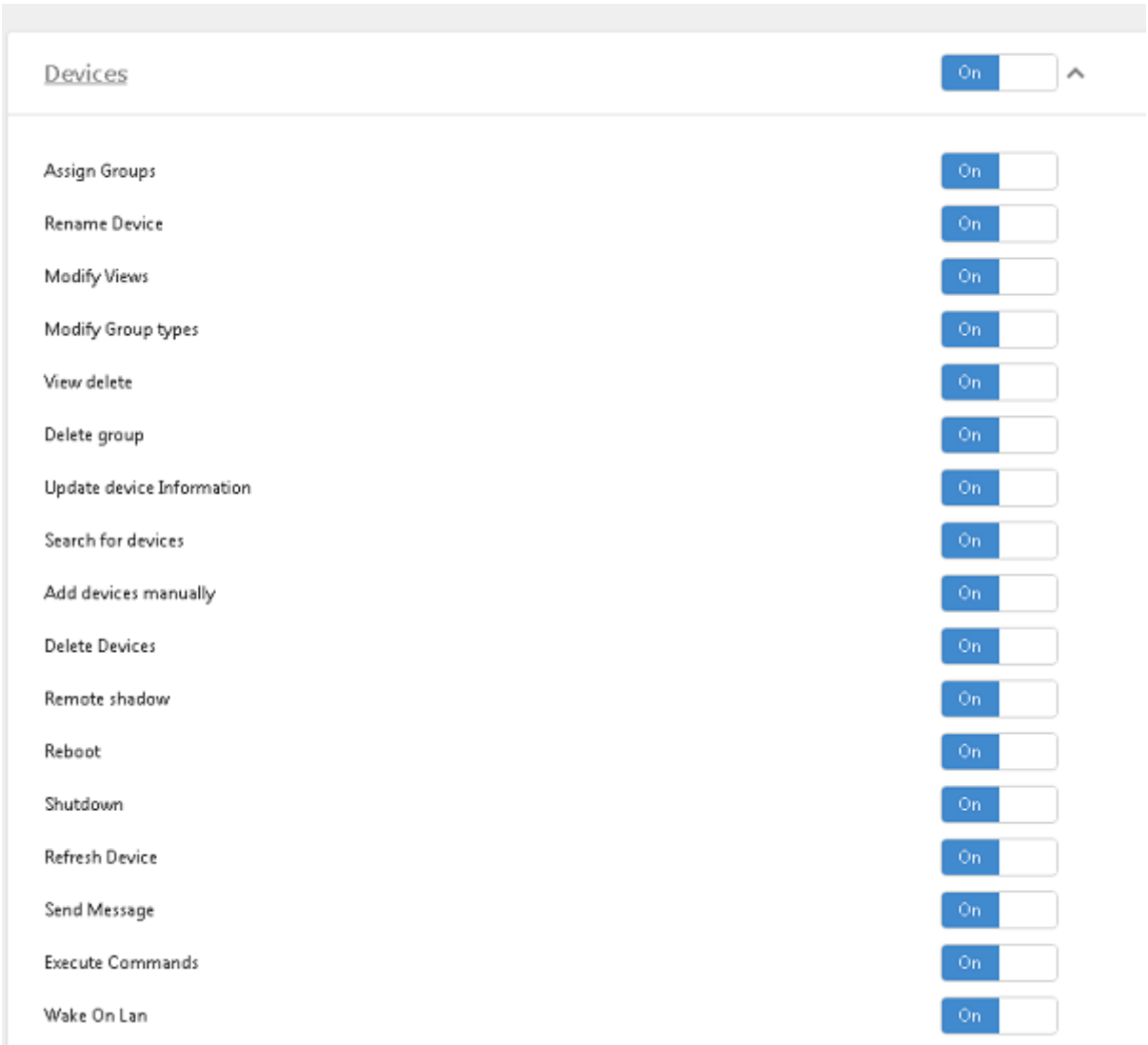


Figure 40. Devices

Table 14. Devices

Devices
Assign Groups
Modify Views
Modify Groups types
View Delete
Update Device Information
Search for devices
Update
Add devices manually
Delete Packages
Delete Devices

Devices
Remote shadow
Reboot
Shutdown
Refresh Device
Send Message
Execute Commands
Wake On Lan
Relay Wake On Lan
Exclude from PAD Repository
Include in PAD Repository
Create and View Log
Get Device Log
Get Image

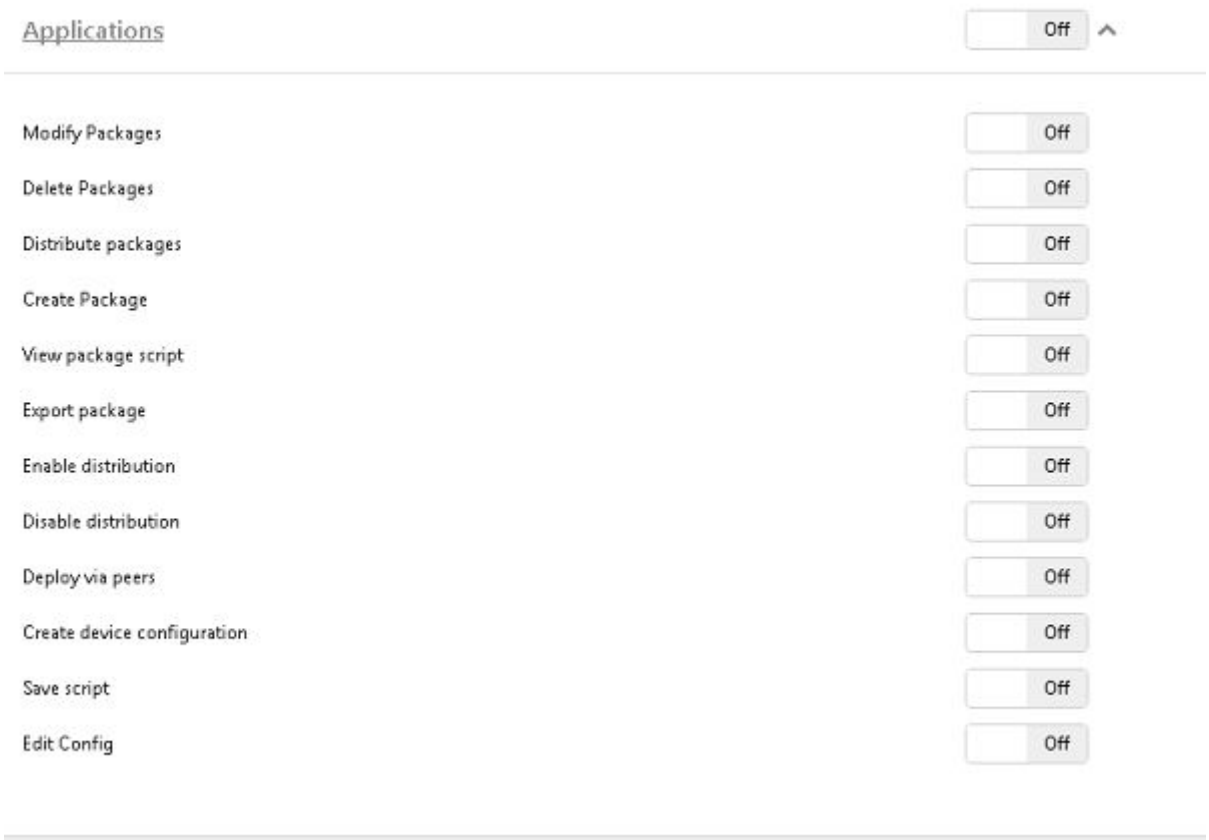


Figure 41. Applications

Table 15. Applications

Applications
Create Packages
Modify Packages
Distribute Packages
Configure Packages
Register Packages
View Packages Script
Export Packages
Disable distribution
Deploy via peers in subnet
Create new configuration
Save script
Edit Config

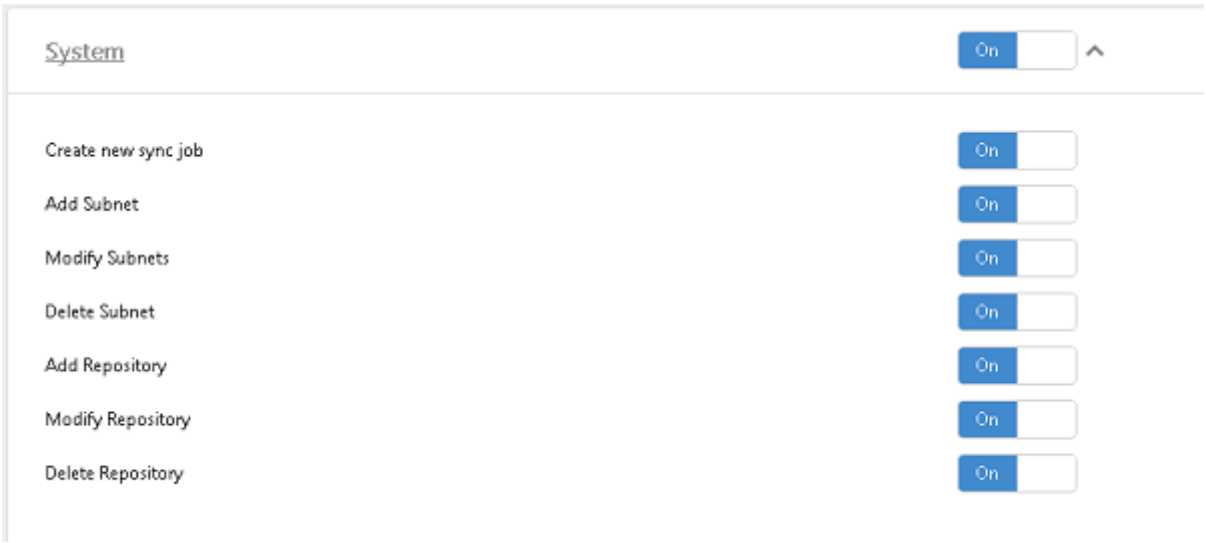


Figure 42. System

Table 16. System

System
Create new sync job
Add Subnet
Modify Subnets
Delete Subnet
Add repository
Modify Repository
Delete Repository

Figure 43. License

Table 17. License

License
Add License
Remove License

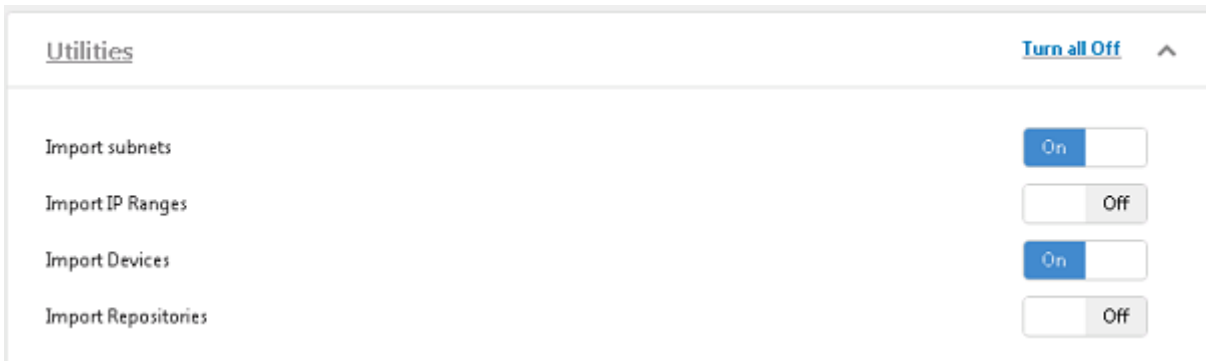


Figure 44. Utilities

Table 18. Utilities

Utilities
Inport Subnets
Import IP Ranges
Import Devices
Import Repositories

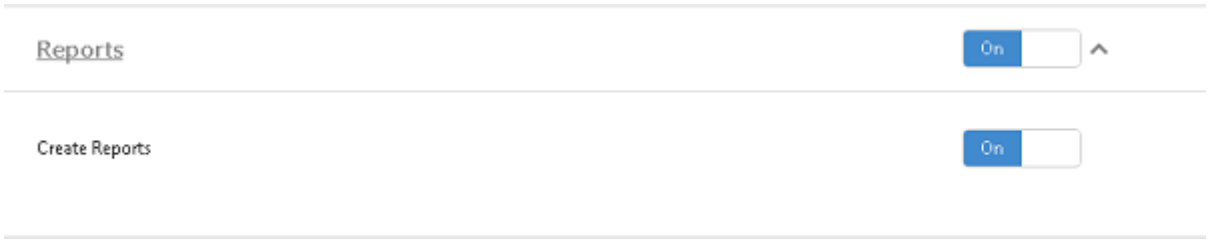


Figure 45. Reports

Table 19. Reports

Reports
Create Reports

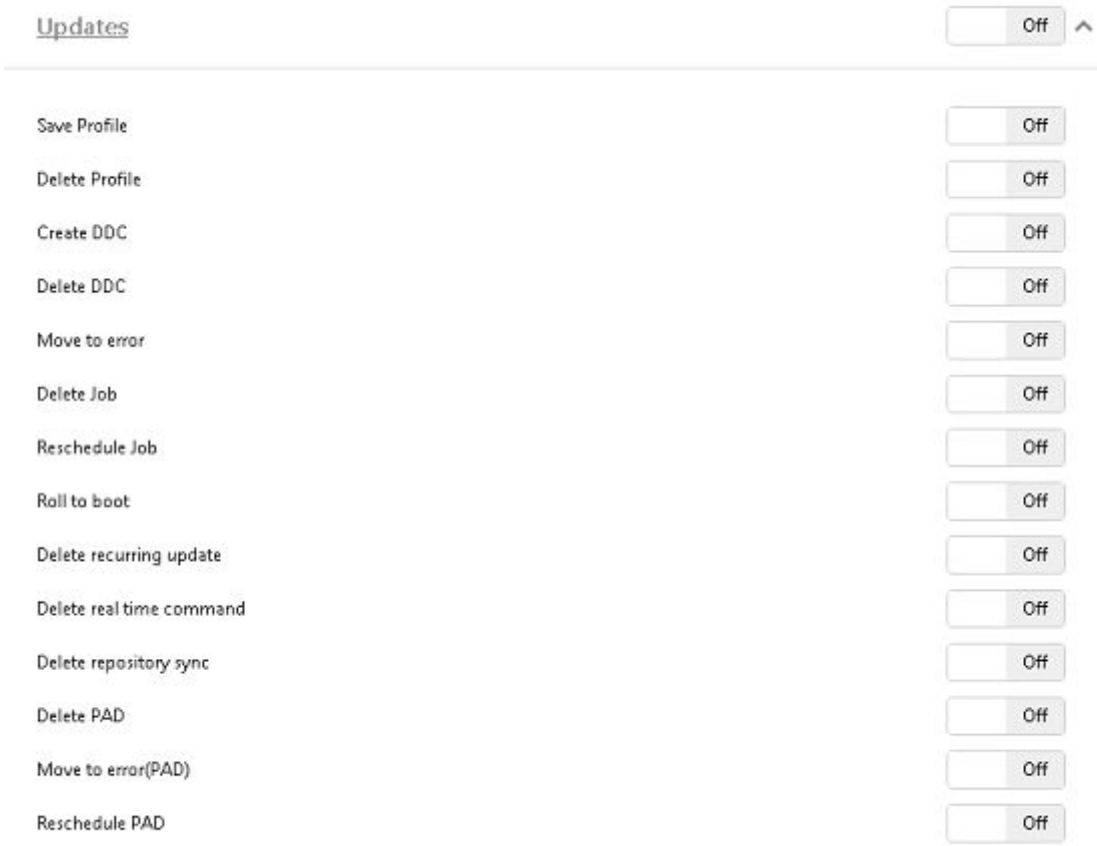


Figure 46. Updates

Table 20. Updates

Updates
Save Profile
Delete Profile
Create DDC
Delete DDC

Updates
Move to error
Delete Job
Reschedule Job
Roll to boot
Delete recurring update
Delete real time command
Delete repository sync
Delete PAD
Move to error(PAD)
Deploy via peers
Reschedule PAD

Deleting Users

As an administrator you can delete WDM users.

NOTE: You cannot delete yourself as a user.

To delete a user:

1 In the WDM Console, expand **System** and click **Accounts** to view the list of WDM users.
2 Select the check-box of the user you want to remove from the list of users, and select **Delete**.
3 Click **Delete** to confirm the deletion.

NOTE: When you delete a user, the private Device Views of the user are also deleted.

Console

Click the **Console** in the System list to view the device status.

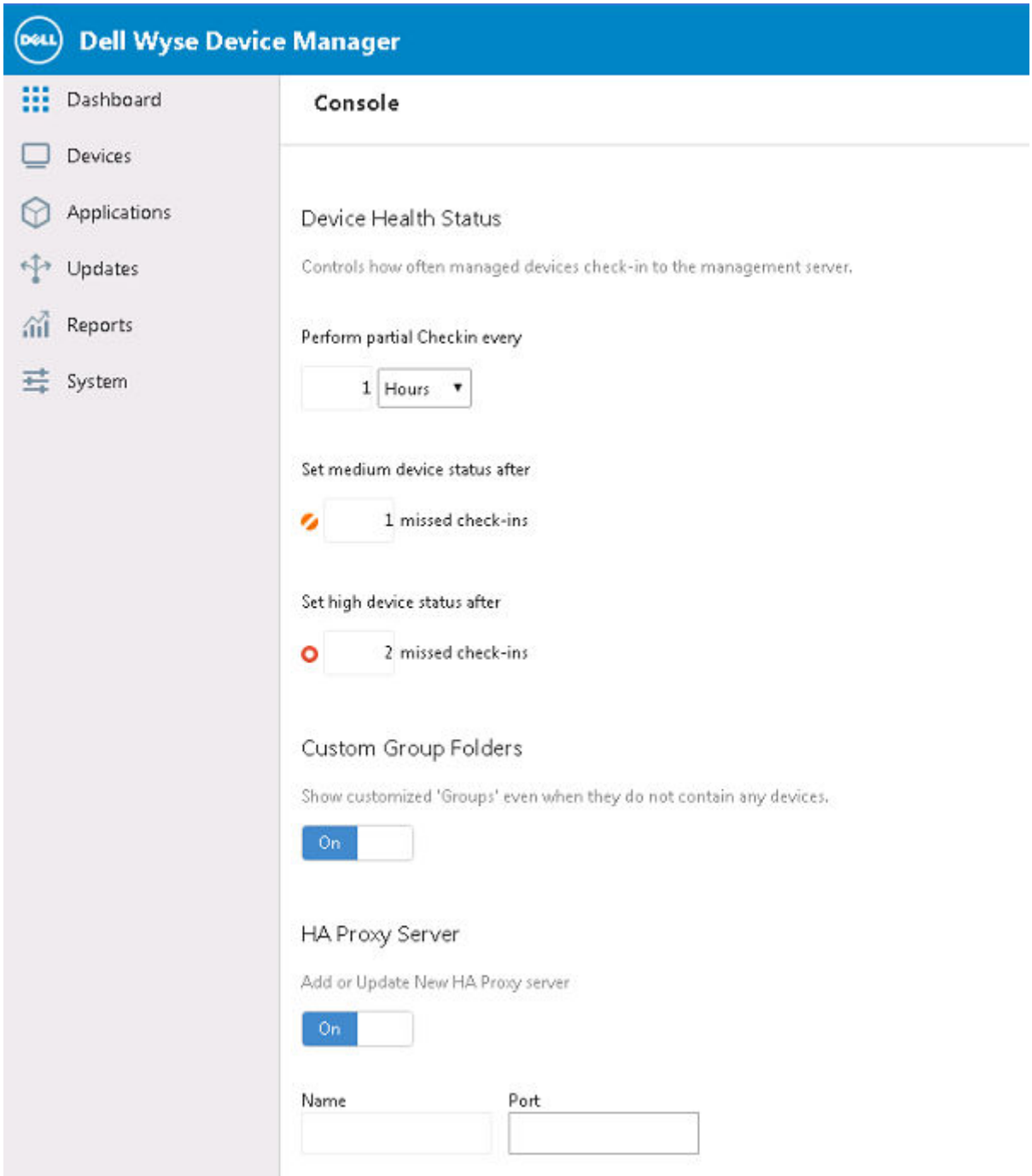


Figure 47. Console

1 Enter the following details:

- **Device Health Status**:
  - **Perform a partial check-in every** - Set the partial check-in frequency for all devices by selecting a number and a time unit (minutes, hours, days). The default is **1 Hour**. Partial check-ins occur regularly at the specified interval to ascertain device health status (red, yellow, green). Partial check-ins require less network bandwidth than a full check-in. This becomes important if your WDM installation contains thousands of devices. Changes to check-in frequencies will not take effect until previously set check-in time or the device is refreshed.
  - **Medium Device Status** - Select the number of missed check-ins to set the medium device status.
  - **High Device Status** - Select the number of missed check-ins to set the high device status.

- **Custom Group Folders** - Select this option if you want to view empty folders in the Device Manager when you create user-defined groups for your Device Views.
- **HA Proxy Server**- Select this option if you want to add or update a new HA Proxy Server. Enter the name and port details in the provided field to add or update a new HA Proxy Server.
- **Remote Sessions**- This option is applicable to Windows, Linux, and Thin OS (WTOS) devices, where you have configured remote sessions . If you select this option, then the details of the remote sessions for that device are listed in the **Remote Sessions** tab on the **Devices** page. This data is useful in charging the end users for the remote sessions.

  For Windows and Linux devices, click on **+** Add server button to add VMWare remote session server and Citrix remote session server.

  Enter the following details to add VMware remote session server:

  - Host or IP
  - Database Name
  - Database username
  - Database password
  - Authentication
  - Prefix

  Enter the following details to add Citrix remote session server:

  - Host or IP
  - Domain
  - Version
  - username
  - Password

  Click on the check mark to validate the information.

  You can also specify the number of days to delete older data. The default is 45 days.

2 The Default Device Configuration allows you to automatically distribute Firmware or SW packages or both to your thin clients devices, Assigning DDCs to groups of devices ensures conformity and allows you to target functional areas of your enterprise with tailored imaging and configuration.

3 Specify the following details:

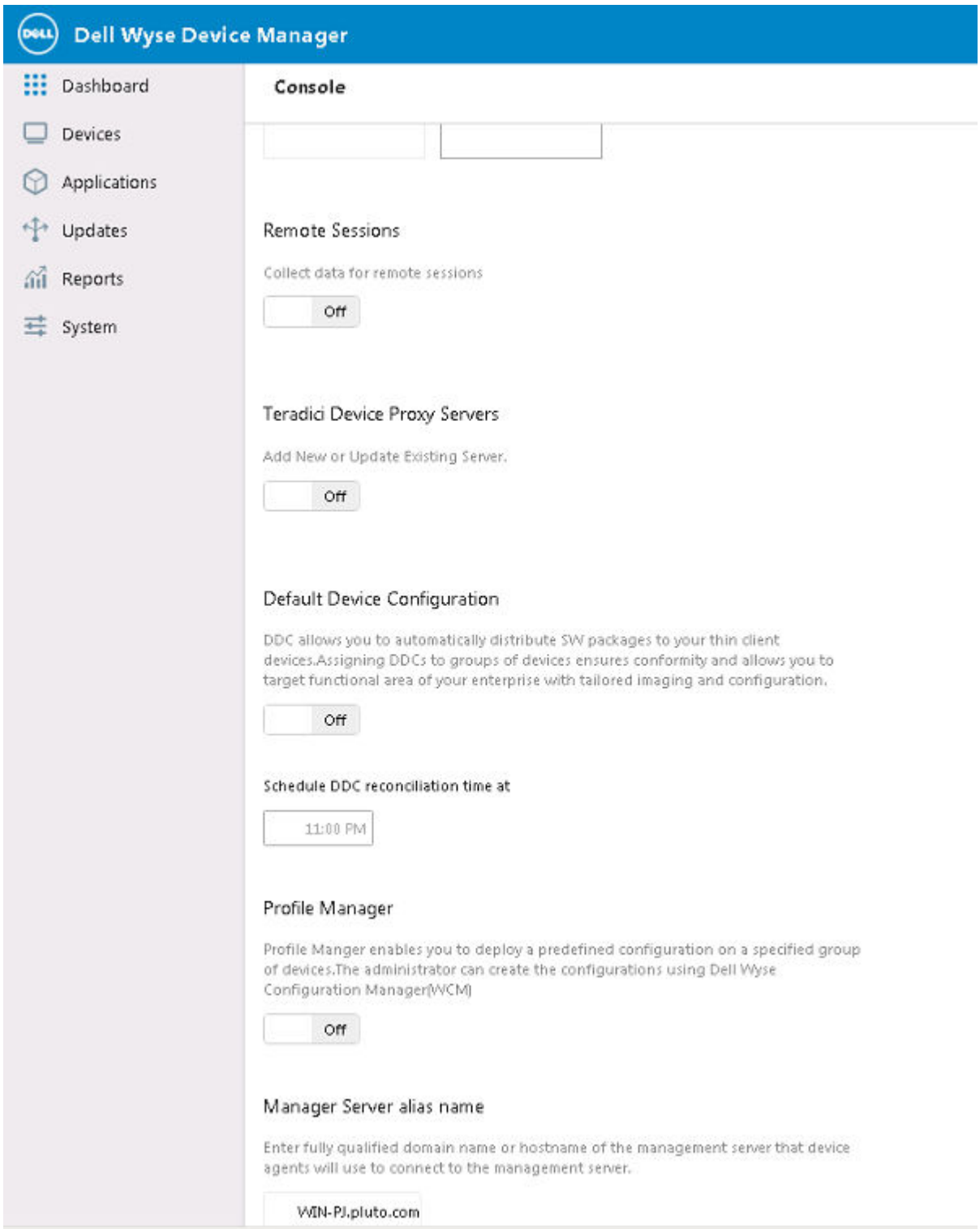


Figure 48. Console

- **Teradici Device Proxy Server** - Select this option to add a new server or update the existing server.

  Default Device Configuration - (WDM Enterprise Edition only.) This option allows you to automatically distribute software packages to your thin client devices. Assigning DDCs to group of devices ensures conformity and allows you to target functional area of enterprise with tailored imaging and configuration.

- **Schedule DDC Reconciliation at**: Enter the time.

4 Click **Profile Manager**

in the Device Manager tree to start **Profile Manager Preferences** window. Profile Manager enables you to deploy a predefined configuration on a specified group of devices. You can create the configurations using Dell Wyse Configuration Manager (WCM).

5 Specify the following details:

a Select **Enable Profile Manager** in the Profile Manager Preferences pane.

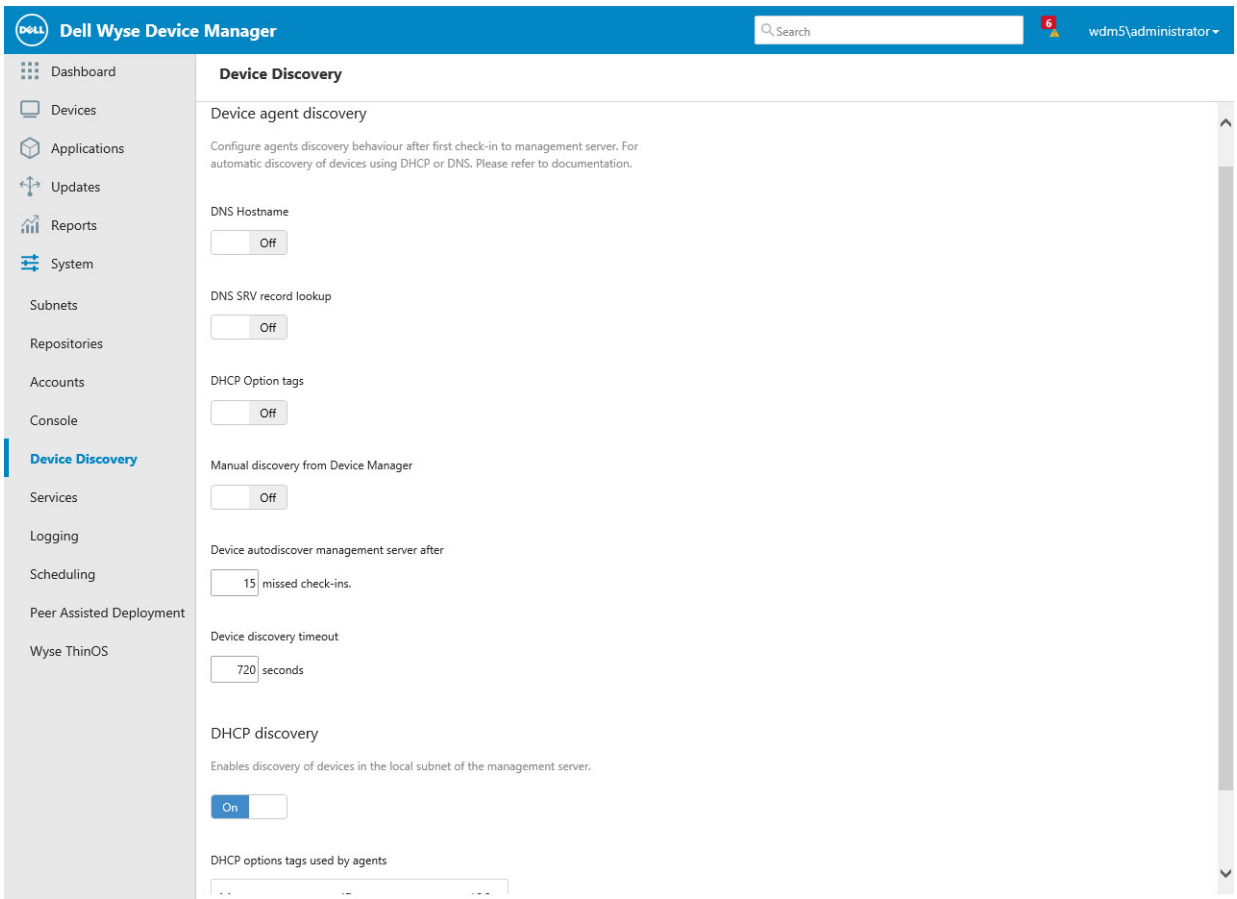
b Click **OK** to save your settings.

6 Click **Management Server alias name** option to enter fully qualified domain name or hostname of the management server that device agents will use to connect to the management server.

7 Click **Save**.

Configure Device Discovery

The Device discovery configures agents discovery behavior after first check-in to the management server.


Dell Wyse Device Manager
Search
6
wdm5\administrator
Dashboard
Devices
Applications
Updates
Reports
System
Subnets
Repositories
Accounts
Console
Device Discovery
Services
Logging
Scheduling
Peer Assisted Deployment
Wyse ThinOS
Device Discovery
Device agent discovery
Configure agents discovery behaviour after first check-in to management server. For automatic discovery of devices using DHCP or DNS. Please refer to documentation.
DNS Hostname
Off
DNS SRV record lookup
Off
DHCP Option tags
Off
Manual discovery from Device Manager
Off
Device autodiscover management server after
15 missed check-ins.
Device discovery timeout
720 seconds
DHCP discovery
Enables discovery of devices in the local subnet of the management server.
On
DHCP options tags used by agents

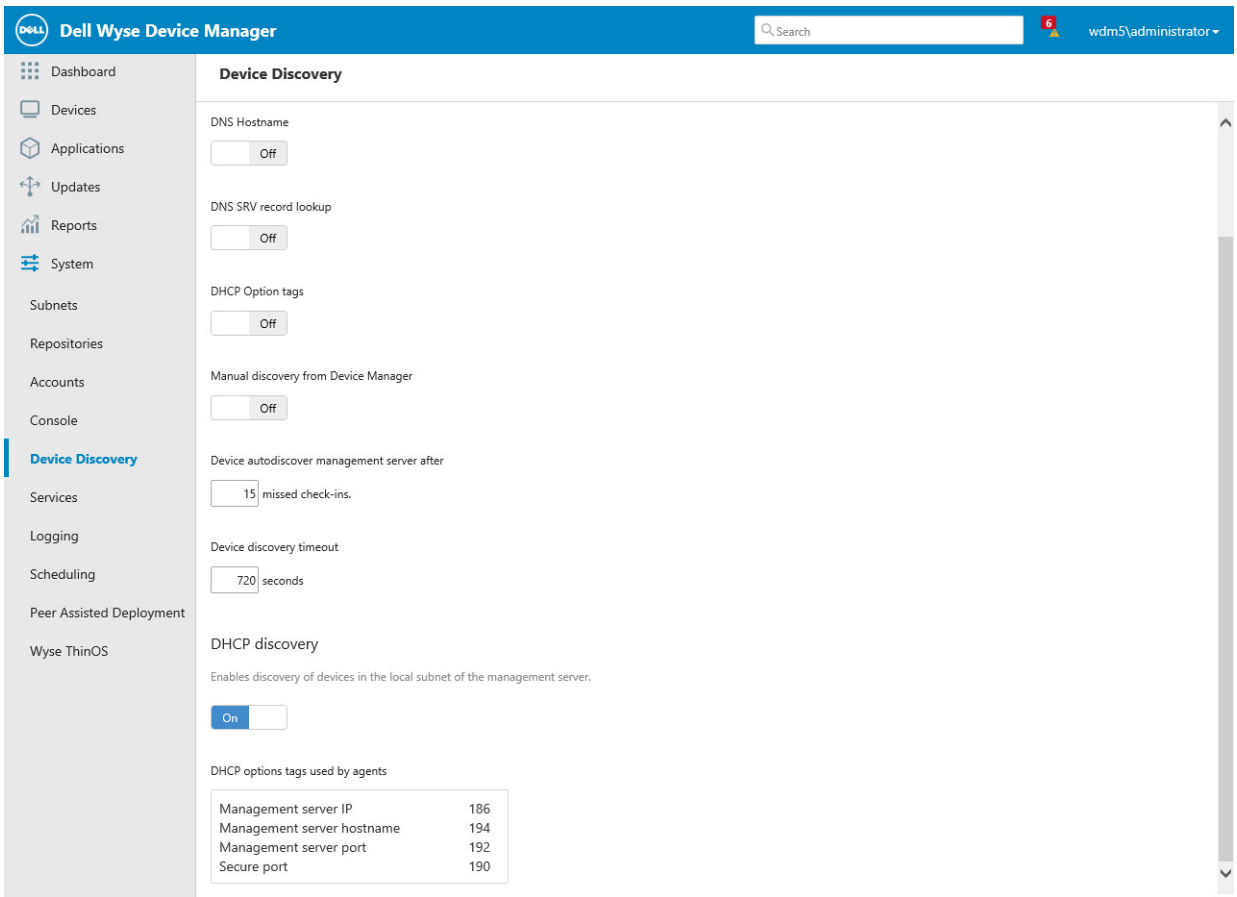

Dell Wyse Device Manager
Search
6
wdm5\administrator
Dashboard
Devices
Applications
Updates
Reports
System
Subnets
Repositories
Accounts
Console
Device Discovery
Services
Logging
Scheduling
Peer Assisted Deployment
Wyse ThinOS
Device Discovery
DNS Hostname
Off
DNS SRV record lookup
Off
DHCP Option tags
Off
Manual discovery from Device Manager
Off
Device autodiscover management server after
15 missed check-ins.
Device discovery timeout
720 seconds
DHCP discovery
Enables discovery of devices in the local subnet of the management server.
On
DHCP options tags used by agents
Management server IP 186
Management server hostname 194
Management server port 192
Secure port 190

Figure 49.

- **DNS Hostname**: Select if you want to allow devices to use DNS Hostname lookup method to discover WDM Server.
- **DNS SRV record lookup** : Select if you want to allow devices to use DNS SRV record lookup method to discover WDM Server.
- **DHCP option tags** : Select if you want to allow devices to use DHCP option tags to discover WDM Server.
- **Manual discovery from Device Manager**: Select if you want to discover the device uing IP Range or Subnet discovery methods in the Find Device window.
- **Device autodiscover management server after**: Select the number of missed check-ins to enable auto-discovery options. The device enables the auto-discovery method, if the number of missed check-ins crosses the specified value.
- **Device discovery timeout**: Enter the maximum time allotment for WDM to discover all the devices on your network.
- **DHCP discovery**: Enables the discovery of devices in the local subnet of the management server.

About Services

The Services page helps you to view the TFTP Server and the Wake on Lan details.

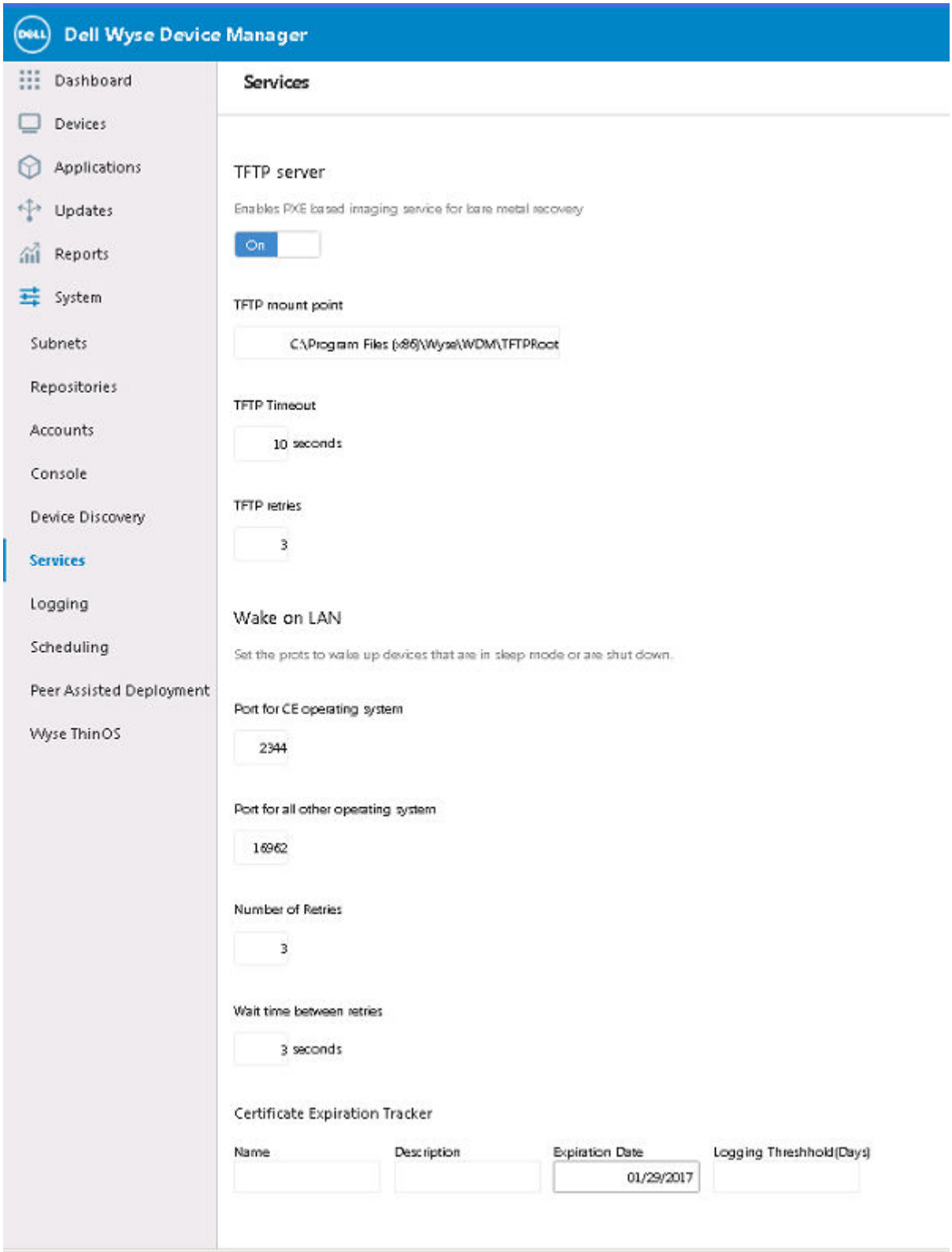


Figure 50. Services

- **TFTP Server**: Enable this option to allow WDM to use Trivial File Transfer Protocol (TFTP) when updating the device.
  - **TFTP Mount Point**: Displays the TFTP mount point that WDM set during installation. Typically, this is the TFTP root directory (WDM) below the FTP home directory used by the Master Repository.

- **TFTP time Out**: Specify the time interval (in seconds) that device waits for a connection to the TFTP service before attempting to reconnect.
- **TFTP retries**: Specify the number of times that device will attempt to connect to the TFTP service before failing.

- **Wake On Lan**: Allows you to wake up devices that are in sleep mode or are shut down.
  - Set the Wake On Lan tries. The number of times that the service attempts to perform a WOL command before stopping and the Delay between WOL Retries (Secs) . The length of time WDM pauses before it attempts another WOL command to the same device.

    For CE devices, the default WOL port is 2344 and for rest of the devices it is 16962. You can change it to some custom port, but make sure to put an exception on firewall port, if Firewall is turned on.
- **Certificate Expiration Tracker**: WDM provides a utility, which tracks expiration of CA certificates. WDM administrator has to manually enter basic information about CA Certificates including name, description, expiration date and logging threshold. WDM will track this information and warn the administrator about expiration of certificate. This information is logged to windows event viewer.
  - **Name** - Enter the name of the Certificate Expiration Tracker.
  - **Description**- Enter the description for the same.
  - **Expiration Date**- Select the Expiration date for Certificate Expiration Tracker.
  - **Logging Threshold(Days)** - This is time period you need to specify to receive the warning message on the expiration of Certificate. Suppose you certificate is going to expire on x date then suppose if you have specified the value for **Logging Threshold(Days)** as 30 days, then you will receive the warning message on Event viewer starting from x-30 date, one message per day. It will appear in Event Viewer as an error message displayed below:

Configure Logging Levels

This parameter helps you to view the following different configure logging levels. Higher logging level causes more data to be stored in the database. This could result in server slow down. The Debug and Informational levels should only be used during debugging.

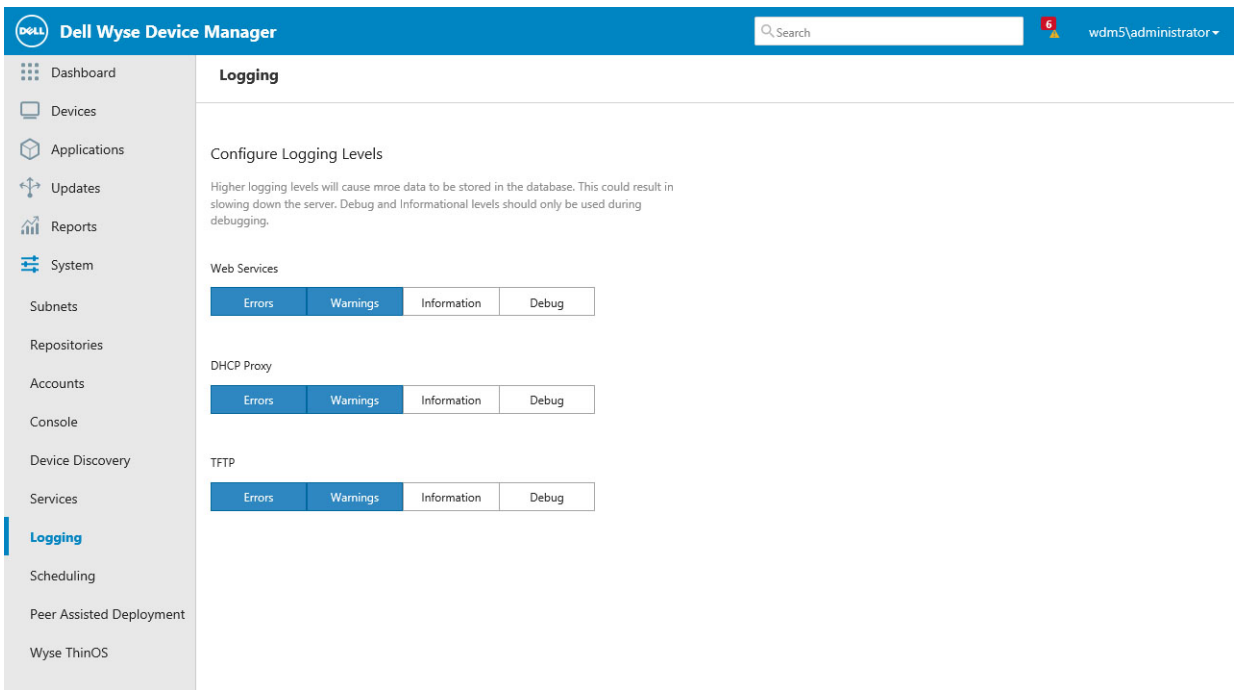


Figure 51. Logging

- **Logging Services area** - Select the logging level for each of the communication protocols.
  - **Errors**: Consisting of simple error messages.
  - **Warning** : Consisting of warnings in addition to error messages (this is the default option).
  - **Informational**: Consisting of error and warning messages in addition to other information items.

- **Debug**: Consisting of all information in Errors, Warning, Informational, and additional debugging data that might be useful to WDM developers, sales engineers, and administrators.
- **Web Services**: Details the activity of the WDM Web Services for device management.
- **DHCP Proxy**: Details the activity of the WDM Dynamic Host Configuration Protocol as it discovers the device.
- **TFTP**: Details the Trivial File Transfer Protocol activity for distributing software packages to devices.

Scheduling

The Scheduling page helps you to view the details such as maximum simultaneous updates, timezone of schedule updates, maximum retry attempts for rescheduling failed updates and auto sync remote software repositories.

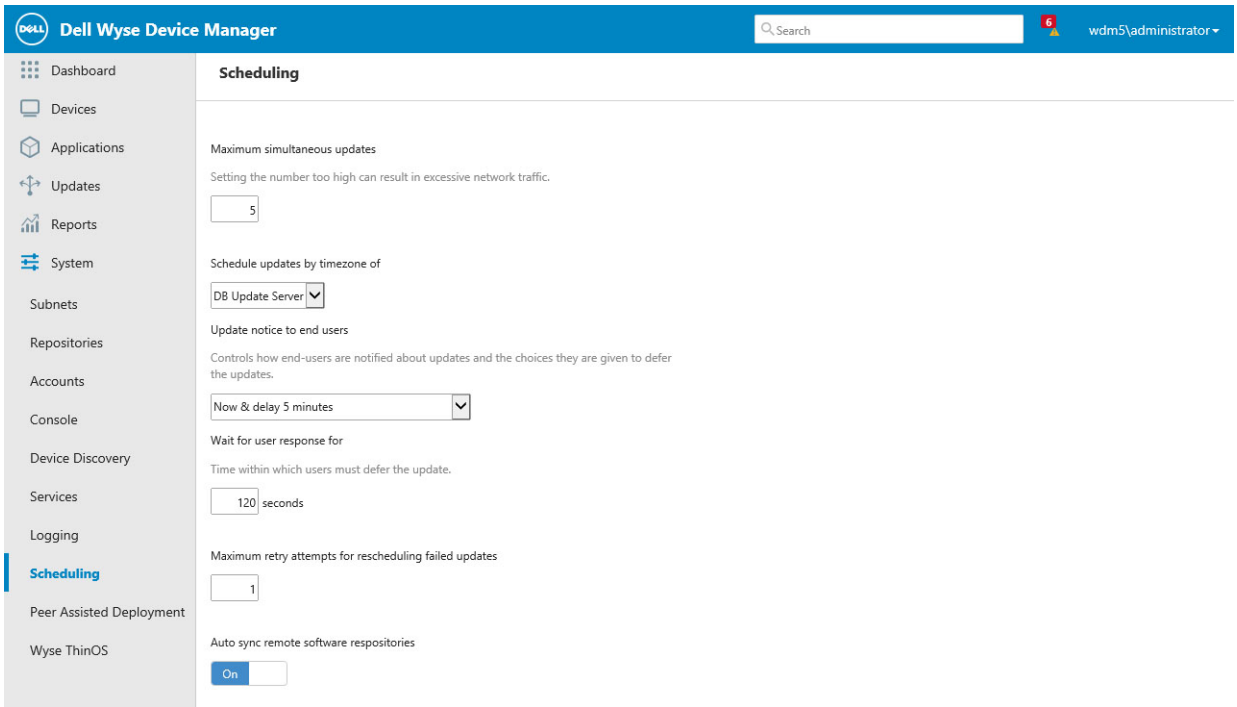


Figure 52. Scheduling

- **Maximum Simultaneous Updates**: The maximum number of device updates you can perform at the same time in the subnet.
- **Scheduled updates by timezone of**: Select the WDM Time Zone that will be in effect when you schedule device updates. Options include:
  - **DB Update Server** : The time zone defined by the physical location of the WDM Database.
  - **Console**: The time zone defined by the physical location of the WDM Console.
  - **Device**: The time zone defined by the physical location of the device that will undergo the actual update.
- **Update notice to end-users**: This is the setting to bring up the User Notification Query Window on the client device whenever an update package is scheduled for the client.
- **Maximum retry attempts rescheduling failed updates**: The Max. Retry Count specify the number of retries you want if package deployment fails.
- **Auto-sync Remote Repositories**: Select to enable WDM (Enterprise Edition only) to determine if Remote Repositories should be synchronized before performing an update to devices served by a Remote Repository.

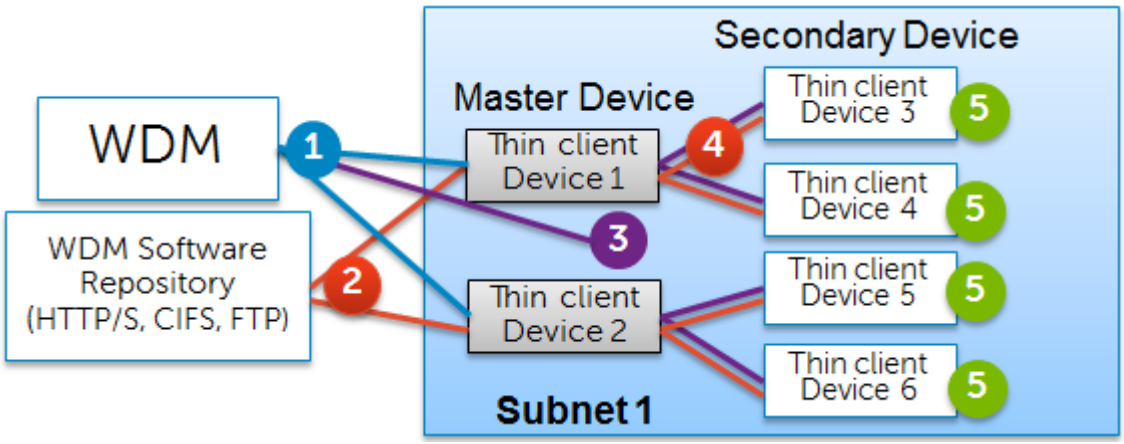
Peer Assisted Deployment

Peer Assisted Deployment (PAD) is a mechanism that provides imaging updates to thin client devices that are managed through the WDM server. This mechanism works best in an environment where the devices are spread across multiple subnets. In peer assisted deployment, the WDM server chooses a set of devices that act as the repository servers for other devices within their respective subnets. Therefore, updates are delivered from peer nodes to other devices and hence the term peer assisted deployment.

The PAD feature is applicable to the following platforms:

- SUSE Linux
- ThinLinux
- Windows Embedded Standard 2009
- Windows Embedded Standard 7 (WES7)
- Windows Embedded Standard 8 (WE8S)
- Windows 10 IoT Enterprise

The following diagram and workflows best describe the working of the PAD functionality.



Workflow from the WDM Server to the Repository Device

The image update process for the repository device configured for PAD consists of three basic steps:

- Self-imaging of the device.
- Making the device Repository-capable.
- Switching off the repository when the PAD schedule is completed.

The workflow can be defined in the following steps:

1 The device that first checks in to the WDM server, has the lowest flash size, and can accommodate the selected pad image becomes the repository device(s) for that subnet. The device should have the values for **Peer Capable** and **Repository Capable** properties set to **True**. For more information, see Prerequisites for PAD.

2 The repository device reboots and images itself from the WDM repository.

3 The repository device completes the imaging, boots up, and downloads the BIOS and becomes Repository Capable. The device then sends back the package completion (V02) status to the WDM server.

4 After the schedule range elapses, the WDM server sends an instruction to switch off the repository when the repository device checks in. It then switches off the application responsible for enabling repository capabilities on the device.

Workflow from the Repository Device to the Peer Devices

The image update process from the repository devices to the peer devices using PAD consists of the following steps:

1 WDM schedules the imaging job to peer devices with the repository device location and image download access credentials.

2 The peer devices download the images from the repository device.

3 After imaging is complete, the peer devices boot up with the new image.

For more information on the PAD functionality see:

- Prerequisites for PAD
- Configuring PAD

- Deploying a Package Using PAD
- Viewing PAD Details
- Editing and Deleting PAD Schedules

Pre-requisites for PAD

The PAD feature is supported both on Windows and Linux thin client systems. For any device to become a master device there are certain pre-requisites.

All Linux devices are PAD capable and can become master devices.

For Linux devices to become PAD capable, make sure that you download and install the latest released version of the OS image on the Linux device. This image should be a PAD Capable image. You can download the image from the Dell Wyse Support Site.

For more information on configuring the Windows devices for PAD, see:

- Making a Windows Device PAD Capable
- Making a Windows Device Repository Capable
- Creating PAD Capable Images for Windows Devices

Making a Windows Device PAD Capable

To make a Windows device PAD capable:

1 Make sure that the device has the latest released version of Windows.

2 For WES7, make sure you have Z, D, ZQ, DQ, or 3290-C90D7 class devices with a minimum flash drive capacity of 8 GB and a 2 GB RAM.

3 For WE8S 64–bit, make sure you have Z, D, ZQ, or DQ class devices with a minimum flash drive capacity of 16 GB and a 4 GB RAM.

4 Deploy the latest available version of **WES7WDAAgentUpgrade** on the WES7 devices,**WE8SWDAAgentUpgrade** on the WE8S devices, and **WIE10WDAAgentUpgrade** on the WIE10 devices.

5 Deploy the latest available version of **BootAgentUpgradeWES7** on the WES7 devices, and the latest available version of **BootAgentUpgradeWE8S** and **BootAgentUpgradeWIE10** on the WE8S devices.

To confirm whether a device is PAD capable or not:

1 In the Device page, select any device.

2 Click the **View details** tab view the details of the selected device.

3 In the view details page, check the Capabilities section.

If the device is not PAD capable the **PAD Capable** flag is set to **red** as shown below:

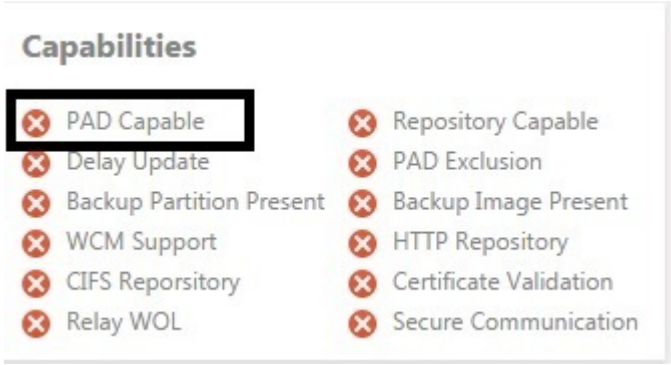


Figure 53. PAD Capable

4 After you configure the device to be PAD capable, the **PAD Capable** flag is set to **Green** as shown below:

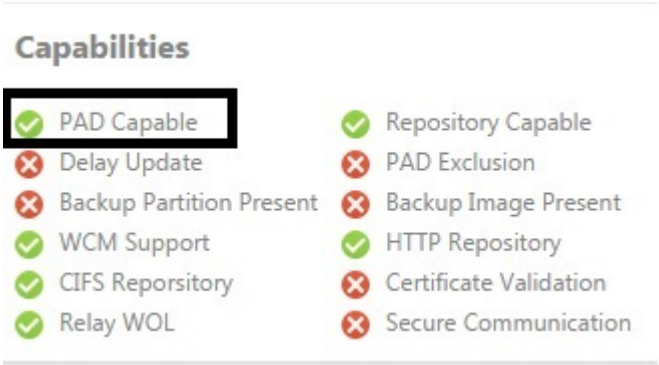


Figure 54. PAD Capable

Making a Windows Device Repository Capable

To make a Windows device Repository capable:

1 Deploy **PADService_SysprepScript_WES7** on the WES7 device.

2 Deploy **PADService_SysprepScript_WE8S** on the WE8S device.

3 Deploy **PADService_SysprepScript_WIE10** on the WIE10 device.

To confirm whether the device is Repository capable or not:

1 In the Device page, select any device.

2 Click the **View details** tab view the details of the selected device.

3 In the view details page, check the Capabilities section.

If the device is not PAD capable, the Repository PAD flag is set to **Red** as displayed below:

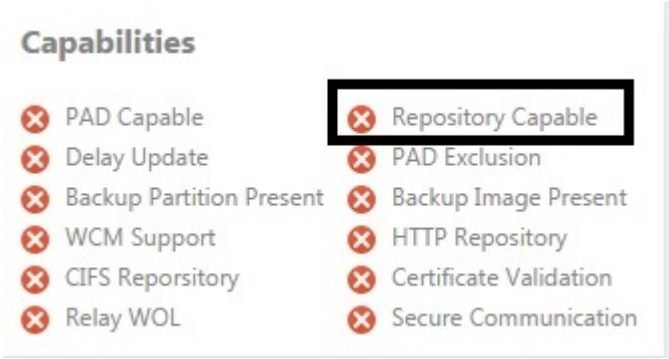


Figure 55. Repository capable

4 After you configure the device to be Repository Capable, the Repository Capable flag is set to **Green** as displayed below:

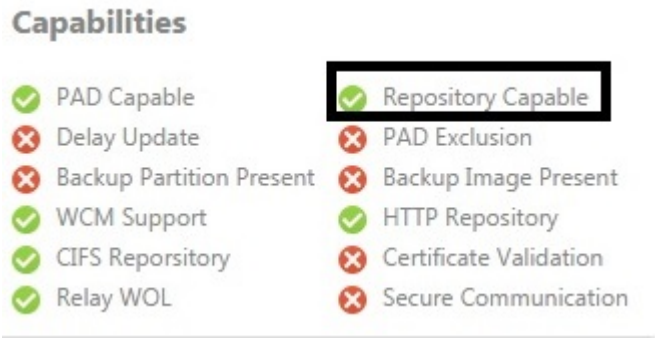


Figure 56. Repository capable

Creating PAD Capable Images for Windows Devices

To create a PAD capable image for **WES7, WE8S** and **WIE10** devices:

1 Set the device check-in interval to at least one hour in the WDM GUI Preferences.

2 Log in to the device as an Administrator, disable the Write Filter, log out , and log in again as Administrator.

3 Delete the **HagentSettings.ini** file from C:\Program Files\Wyse\WDA\config and run the following command in the command prompt for **WES7** devices:

```
Hagent.exe -Install
```

For **WE8S** and **WIE10** devices, you must log in as Administrator, navigate to C:\Windows\System32, right click the **Cmd.exe** file, and select the **Run as Administrator** option before running the above command.

4 For **WES7** devices, prepare the device to pull the image by navigating to the **C:\windows\setup** folder in the command prompt and running the following command:

```
WES7_CustomSysprep4man.bat -r
```

For **WE8S** and **WIE10** devices, prepare the device to pull the image by navigating to the **C:\windows\setup** folder in the command prompt and running the following commands:

```
Powershell.eexe c:\windows\setup\WIE10_CustomSysprep4man.psl -r
```

NOTE: For WE8S devices, you must run the command prompt as an Administrator. See Step 3.

5 Do not allow the device to boot to the OS, instead give the **Pull Image** command using the **PXE** mode for **WES7** devices, and the **Non PXE** mode for the **WE8S** and **WIE10** devices where the **sysprep** is running.

6 Log in to the system where the WDM console is running, and right click on a schedule from **Update Manager** > **Schedule Packages**.

7 Select the **Roll to Boot** option.

8 For **WES7** devices, press the **P** key, and boot the device through the **PXE LAN** mode. For **WE8S** and **WIE10** devices, press the **P** key, and boot the device through **Merlin Non-PXE** mode.

9 After the image is pulled, deploy the pulled image using the **Deploy via Peers in Subnet** option.

Configuring PAD

For the PAD feature to function, you need to configure the Subnet preferences. You can specify the number of devices that you want to serve as repositories and also specify the connection details to the master device.

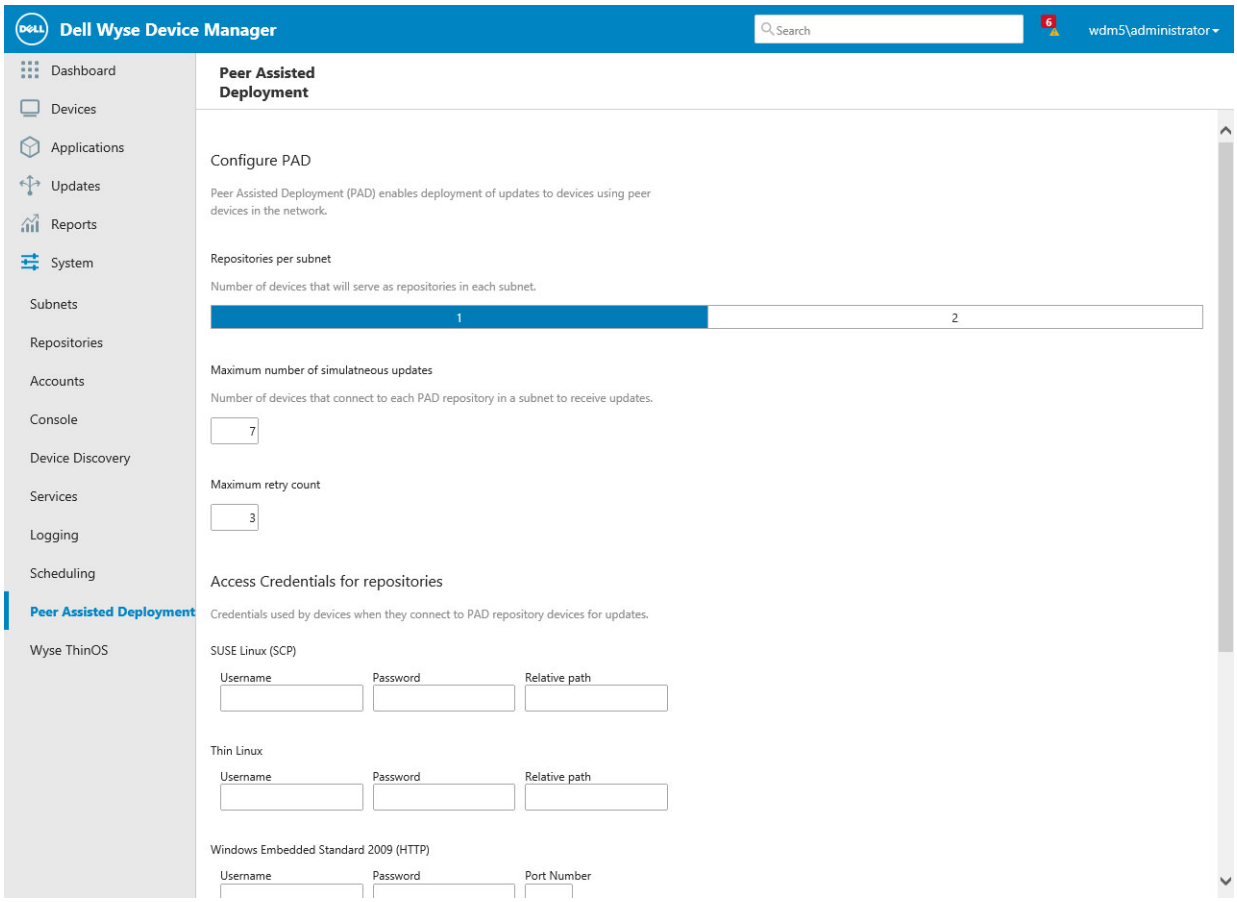


Figure 57. Peer Assisted Deployment

To configure PAD on WDM:

1 On the WDM Console, select **System → Peer Assisted Deployment**.

2 Specify the minimum number of required peer capable repositories as One or Two.

3 Change the maximum number of simultaneous connections to the master device if required. The default number of simultaneous connections is 7.

4 Change the maximum number of retry count to the master device if required. The default number of simultaneous connections is 3.

5 Enter the credentials for accessing the repositories. Specify the User Name, Password, and the relative path for the following device.

- **SUSE Linux (SCP)**
- **ThinLinux**
- **Windows Embedded Standard 7**
- **Windows Embedded Standard 8**

- **Windows 10 IoT Enterprise**

Deploying a Package Using PAD

To deploy a image with PAD:

1 On the WDM Console, select **Images** under **Application**.
The registered images are displayed.

NOTE: PAD can only deploy images, not application packages.

2 Select an image, click and select **Deploy via Peers** tab.
The **Deploy via peers** window is displayed.

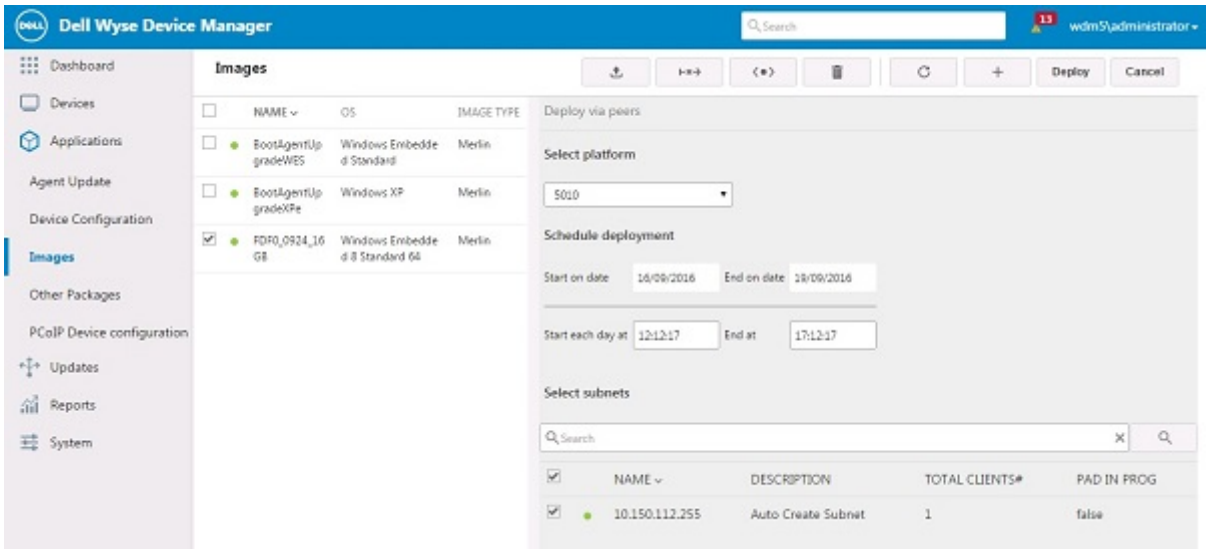


Figure 58. Deploy via peers

3 From the drop-down list, select your preferred platform.

4 Enter the start date, end date and timings in hh:mm:ss format to schedule a deployment.

5 Enter the subnet IP to select from the available subnets.

NOTE: At least one subnet need to be selected for creating PAD schedule.

6 Click **Deploy**.

Viewing PAD Details

You can view the PAD details such as the PAD schedules, the clients that have been selected as Master repositories, and the image update process summary.
To view the details:

1 On the WDM console, expand the **Peer Assisted Delivery** node under **Updates**.
The node displays the **Jobs**, **Repositories**, and **Summary**.

2 To view the list of clients that serve as Master repositories, select **Repositories** under **Peer Assisted Delivery**.
The list of clients are displayed.

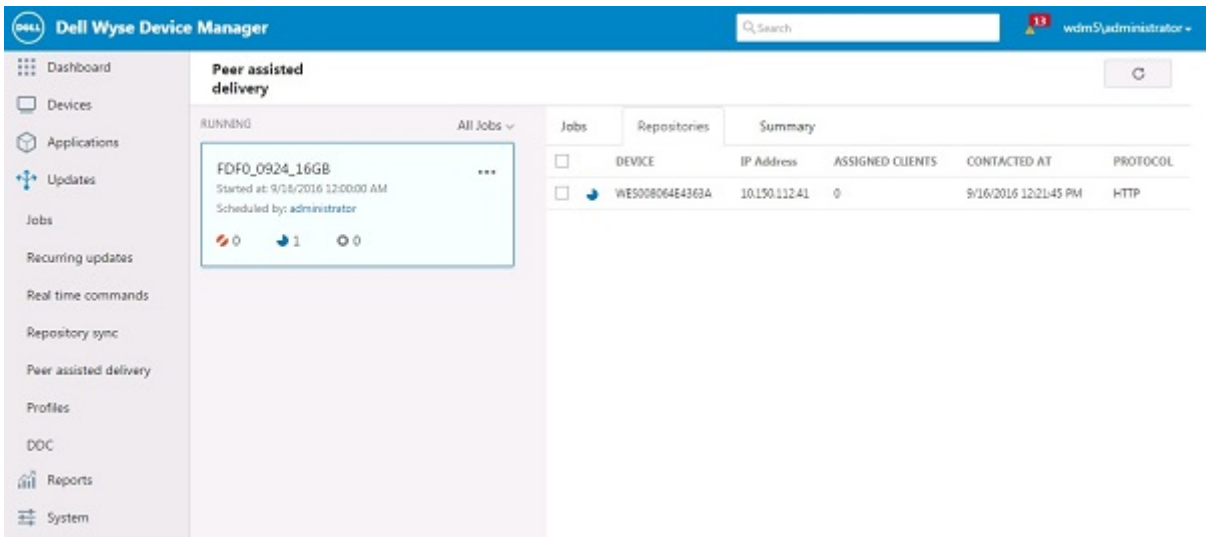


Figure 59. Repositories

3 To view the PAD schedules, select **Jobs** under **Peer Assisted Delivery**.
The list of package deployment schedules are displayed.

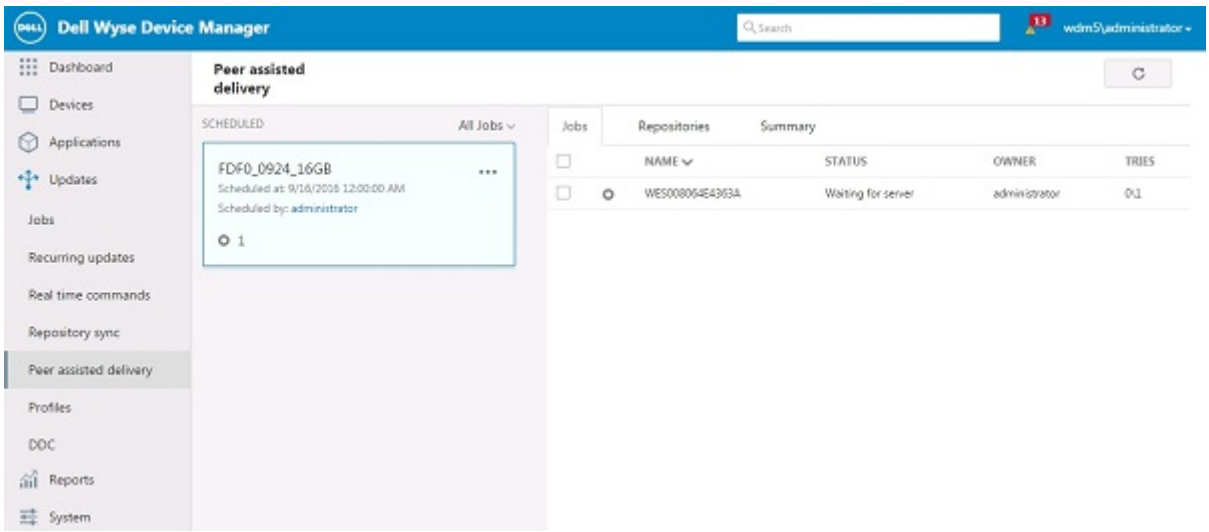


Figure 60. Jobs

4 To view the PAD Image update process, select **Summary** under **Peer Assisted Delivery**.
The progress is displayed.

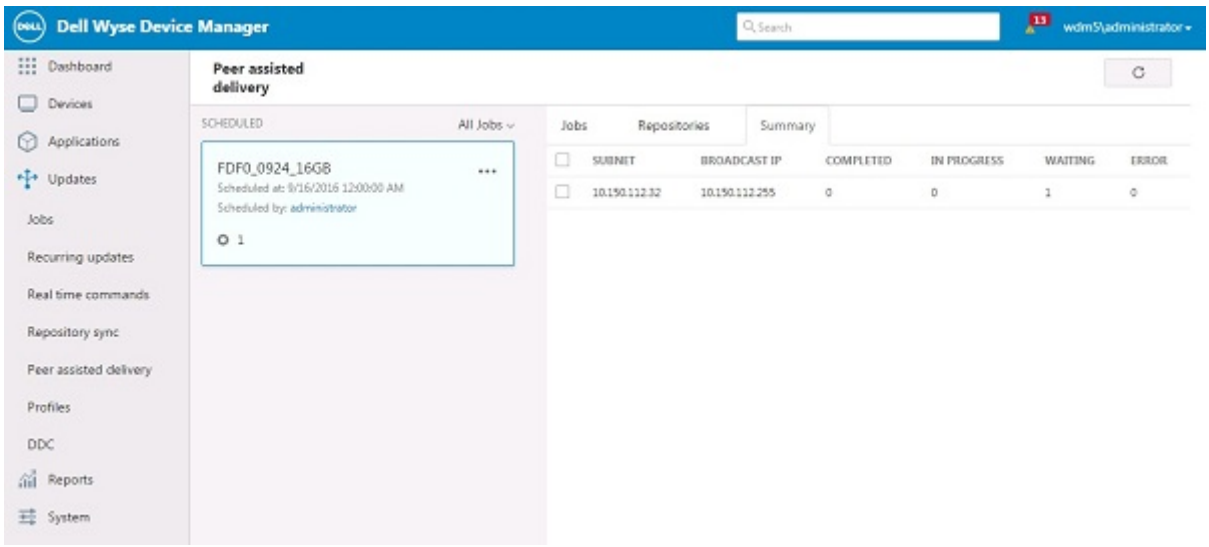


Figure 61. Summary

Editing and Deleting PAD Schedules

You can edit and delete PAD schedules on the WDM console.

1 To edit a PAD schedule:

a On the WDM console, expand **Peer Assisted Delivery** under **Updates** and select **Jobs**.
The jobs are displayed.

b Select a job, click the three dots displayed and select **Edit**.
The **Edit** window is displayed.

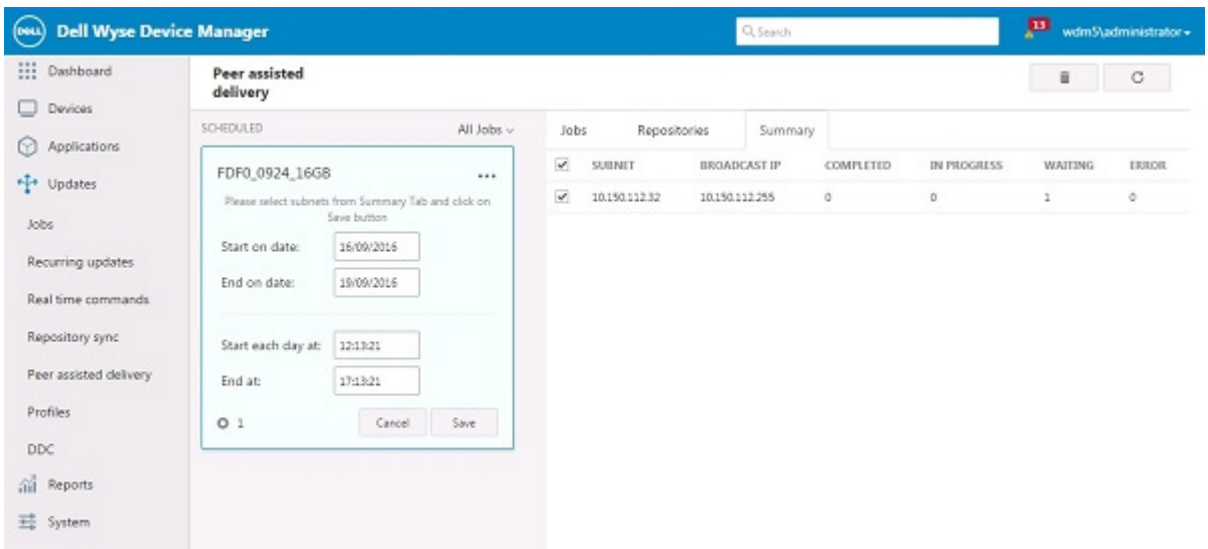


Figure 62. PAD Edit

c Change the date and time ranges as required and click **Save**.
The scheduled job displays the new date and time.

2 To delete a PAD schedule:

a On the WDM console, expand **Peer Assisted Delivery** under **Updates** and select **Summary**.

The schedule summaries are displayed.

b Select a summary, click **Delete** tab.

The schedule is deleted.

Wyse ThinOS

This parameter helps you to view the WTOS INI root path.

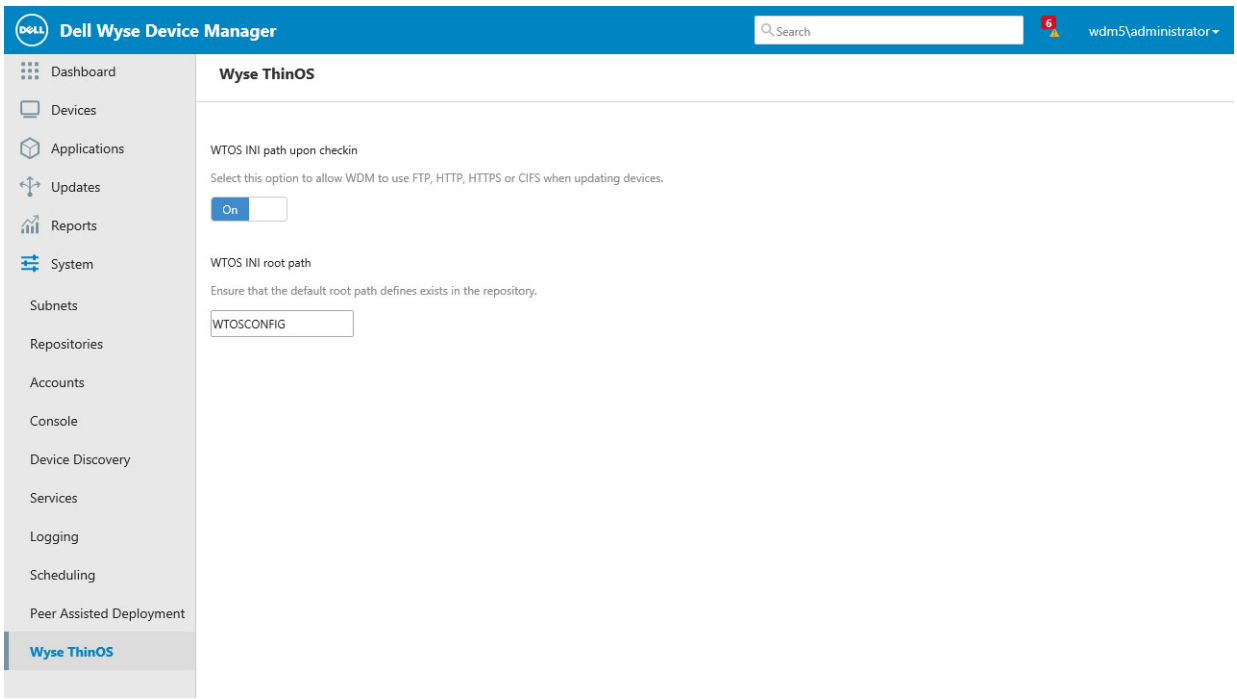


Figure 63. Wyse ThinOS

- **WTOS INI path upon checkin** : Select to allow WDM to use FTP, HTTP, HTTPS, or CIFS when updating devices.
- **WTOS INI Root Path** : Enter the WTOS INI root path.

10

Management of Teradici device using WDM

Pre-requisite: Make sure you have already installed a WDM server with ThreadX support for the 5.x firmware.

This section provides the information about the infrastructure changes needed for devices to discover, and register with management servers including Wyse Device Manager (WDM).

Supported Platforms:

Supports the following Teradici based Dell WYSE devices:

- Wyse 5030 zero client for VMware
- Wyse 5050 AIO thin client with PCoIP
- Wyse 7030 zero client for VMware

Firmware versions:

- 4.x
- 5.x

NOTE: The following instructions are based on windows 2012 R2 DNS. The exact settings may look different depending on the version of windows.

Topics:

Steps to create a DNS_SRV record

The firmware 4.x uses either DNS_SRV record or DHCP record to locate its management console.

NOTE: Do not use DNS_SRV record and DHCP record at the same time to locate firmware 4.x management console.

The instructions described in this section mainly focuses on DNS_SRV record. The DNS record is _tcp_pcoip-tool in the domain that the client is configured to communicate with, and the configurations are expected to be done on the DNS server.

In the following example the domain name is delldemo.int, and WDM server is dell-wdm55.delldemo.int

1 Navigate to _tcp under your domain, then right click and select **Other new records**.

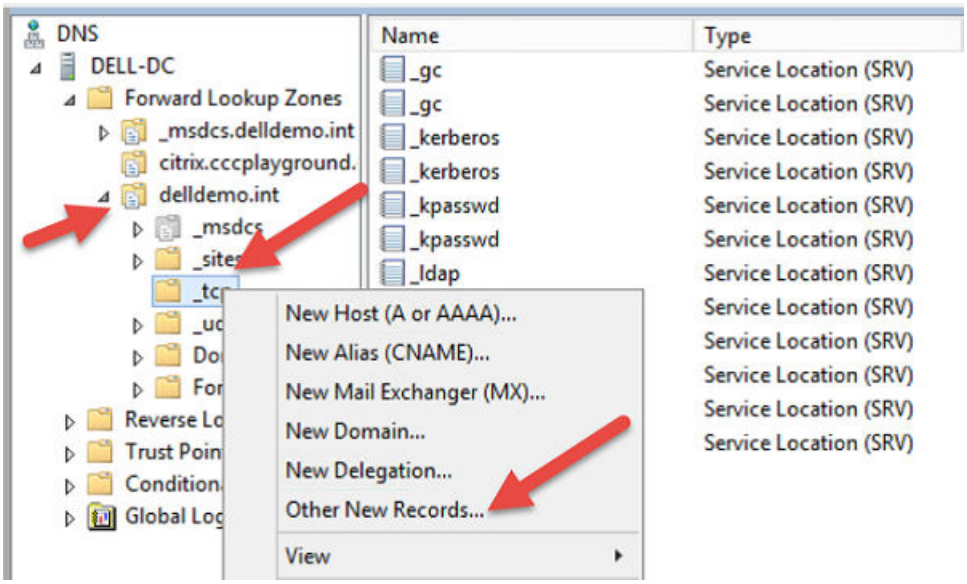


Figure 64. DNS SRV record

2 Select **Service Location (SRV)** from resource record type list.

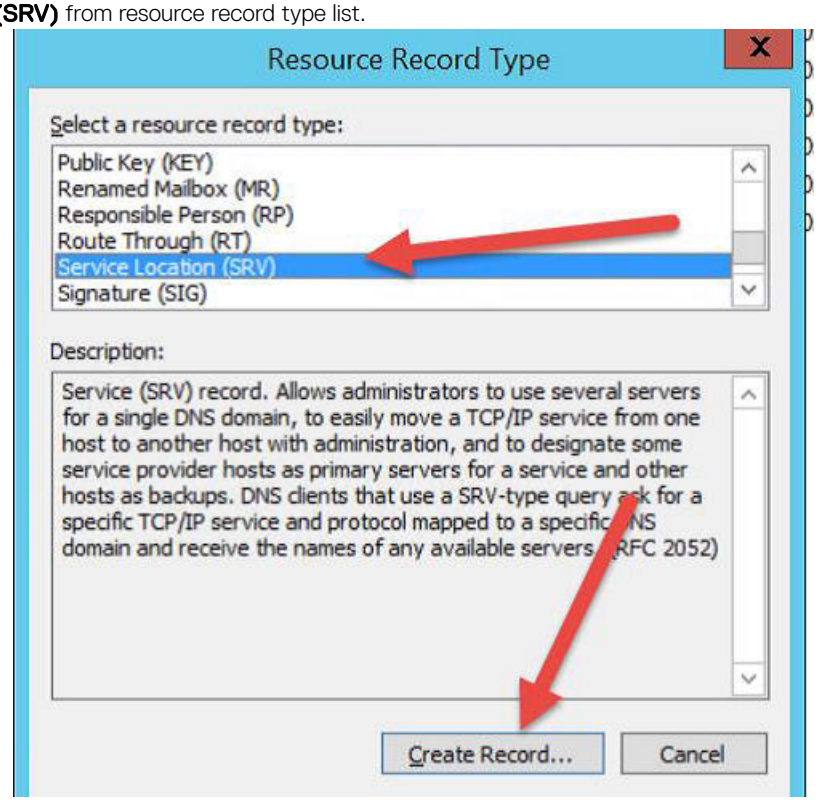


Figure 65. Resource Record Type

3 Click **Create Record...** option.

4 Enter the following values in the provided fields:

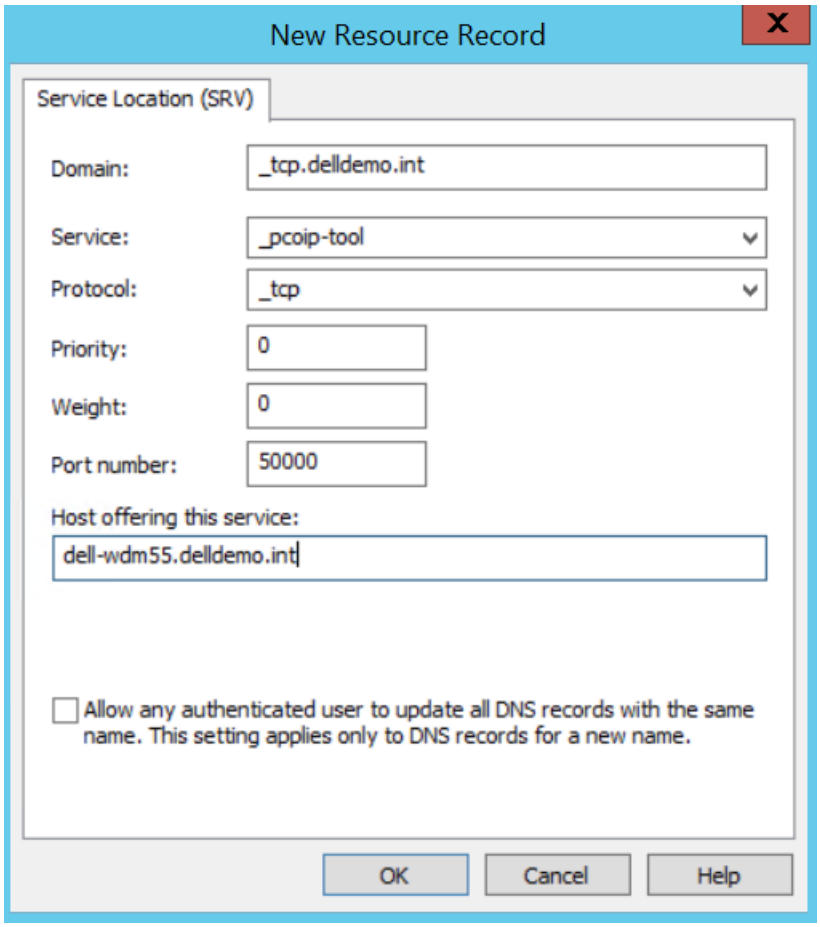


Figure 66. New Resource Record

Table 21.

Parameter	Description
Domain	delldemo.int
Service	_pcoip-tool
Protocol	_tcp
Priority	0 (Zero)
Weight	0 (Zero)
Port Number	50000
Host offering this service	Enter the name or IP address of the WDM server

5 Click OK.

NOTE: A trailing . is automatically added to the host line by windows.

Monitoring and Troubleshooting

The easiest way to monitor the device is using the web UI of the device and the event logs.

1 Connect the browser to the https://IP address of the device.

2 Enter the default password of the device. The default password is **Administrator**.

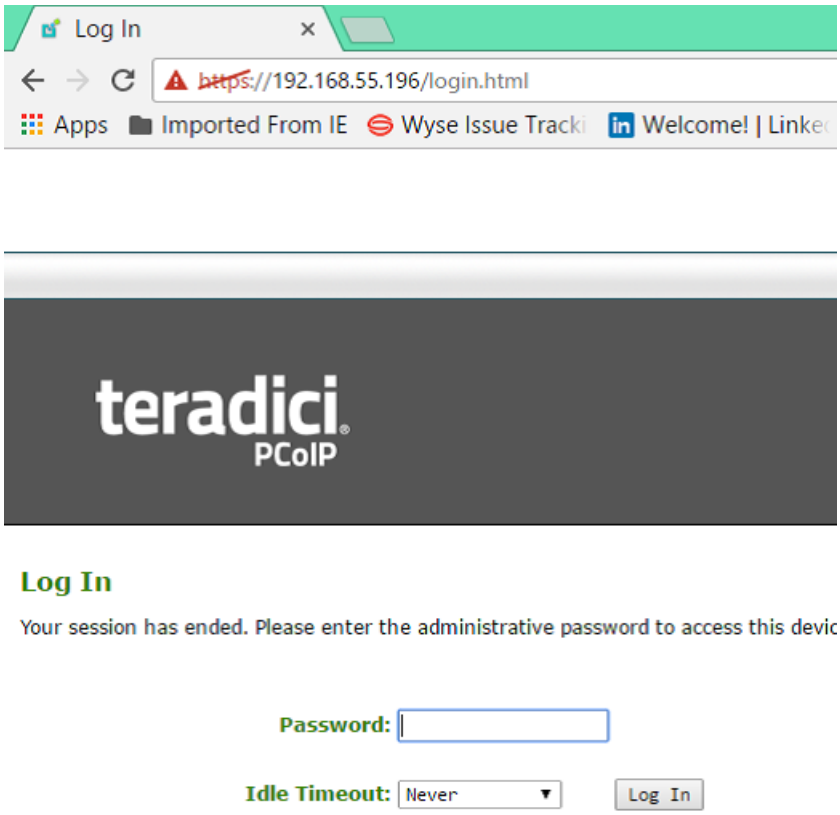


Figure 67. Log In

3 Select **Diagnostics** option.

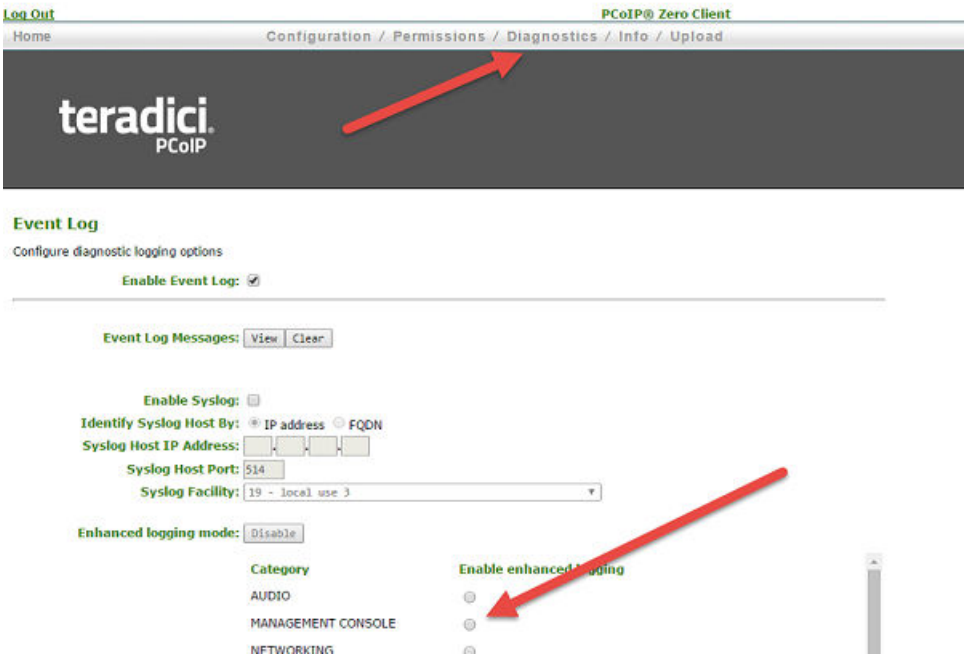


Figure 68. Diagnostics

4 Enable the event log option to configure the diagnostic logging options.

5 Select the radio button of **Management Console** option.

6 Click **View** option to view the event log messages.

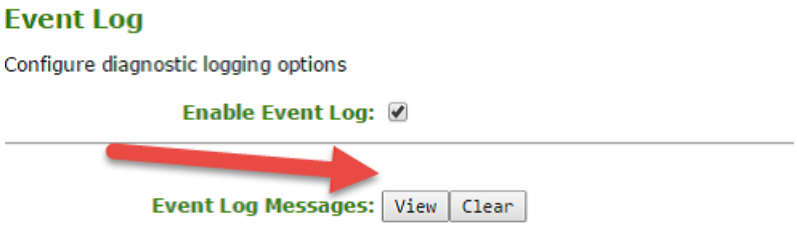


Figure 69. Event Log

7 Search for DNS SRV information from the log and specifically for MGMT_DISC_DNS. In this example search for properly discovered intended WDM server which has the name dell-wdm55.delldemo.int and IP address of 192.168.251.65

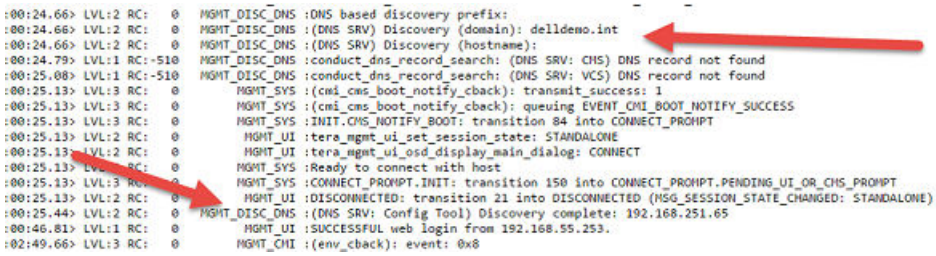


Figure 70. Logs

8 Check your management console (WDM) to confirm that the device is appearing or listed.

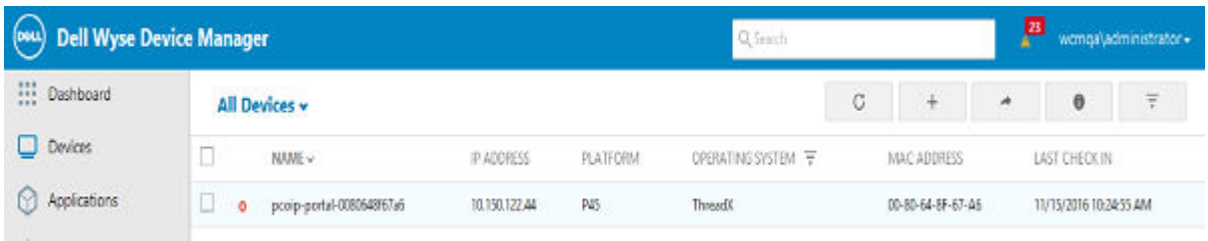


Figure 71. Dell Wyse Device Manager

NOTE: The firmware 4.x teradici has a known limitation in the communication of devices registering with the WDM. It may take 15-30 minutes for the device to display in the console even after the log shows it has registered.

Configuring firmware 5.x

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.

After creating the DNS_SRV record, for more information see, Steps to create a DNS_SRV record then complete the following steps:

1 The first record required is a DNS_SRV record for _pcoip-bootstrap. The record must point to the name of the management console (WDM).

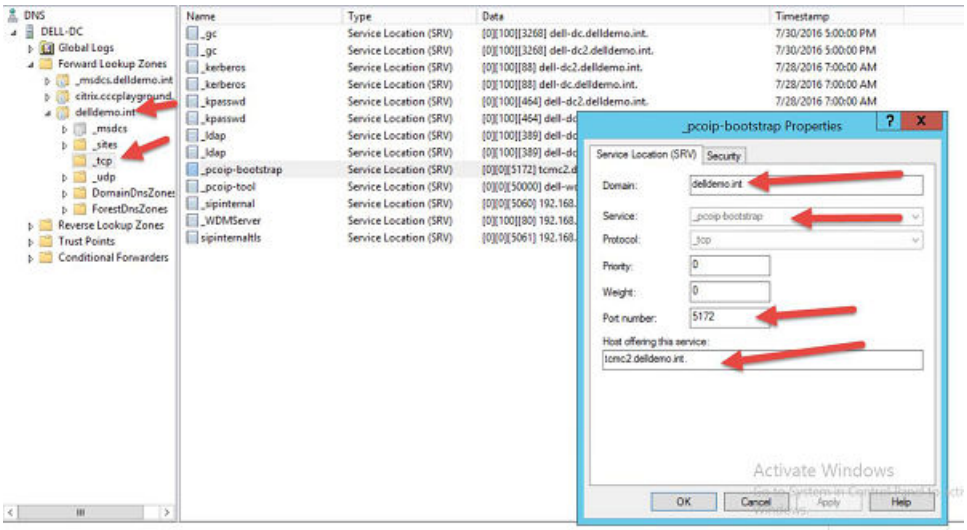


Figure 72. DNS_SRV record for _pcoip-bootstrap

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

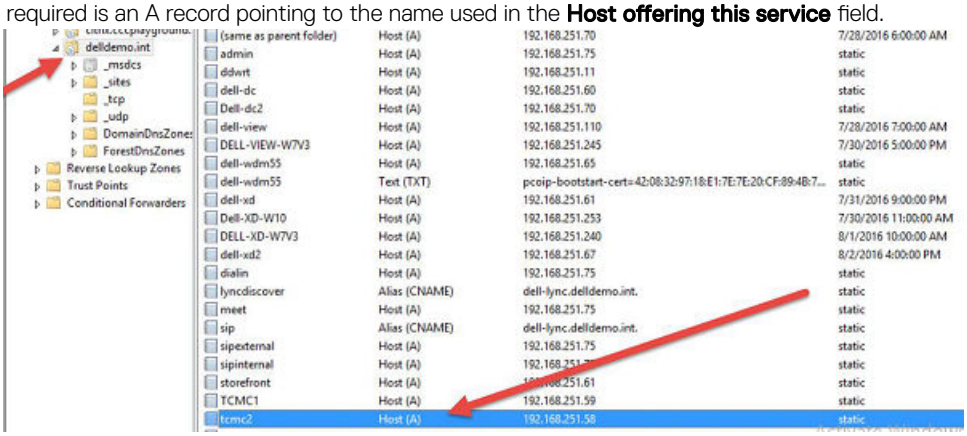


Figure 73. Host Record

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.

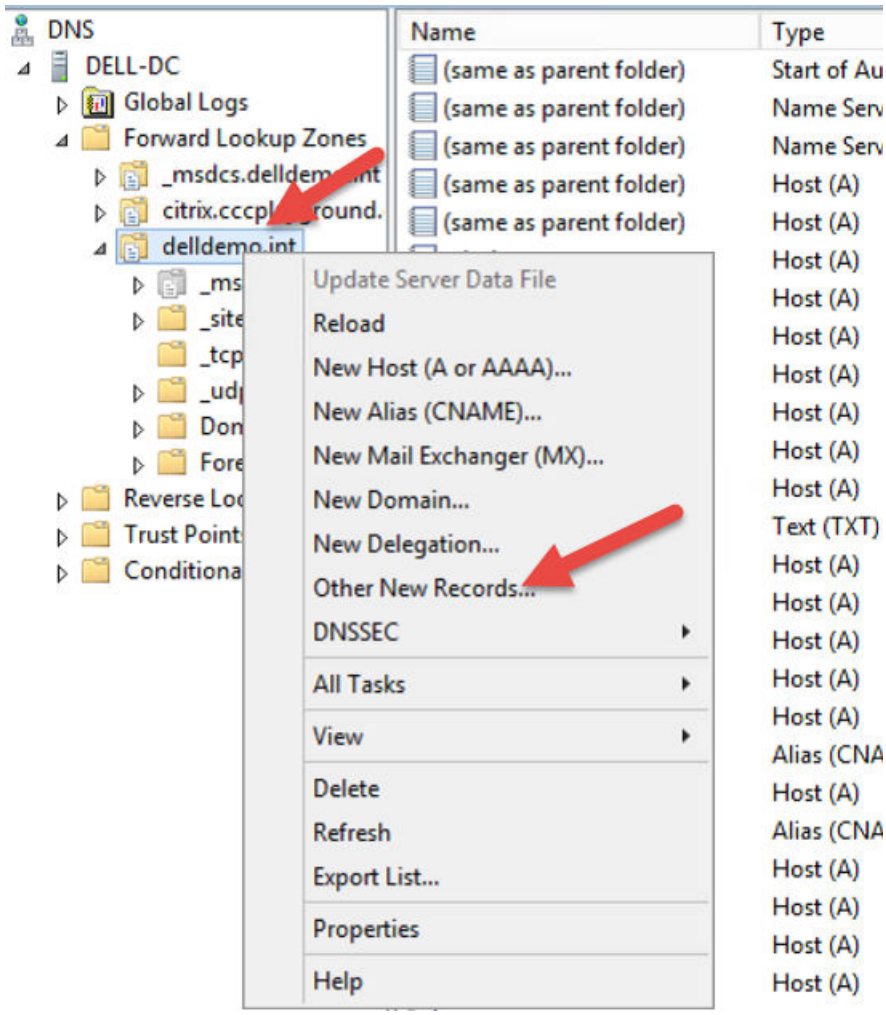


Figure 74. Create TXT record

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.

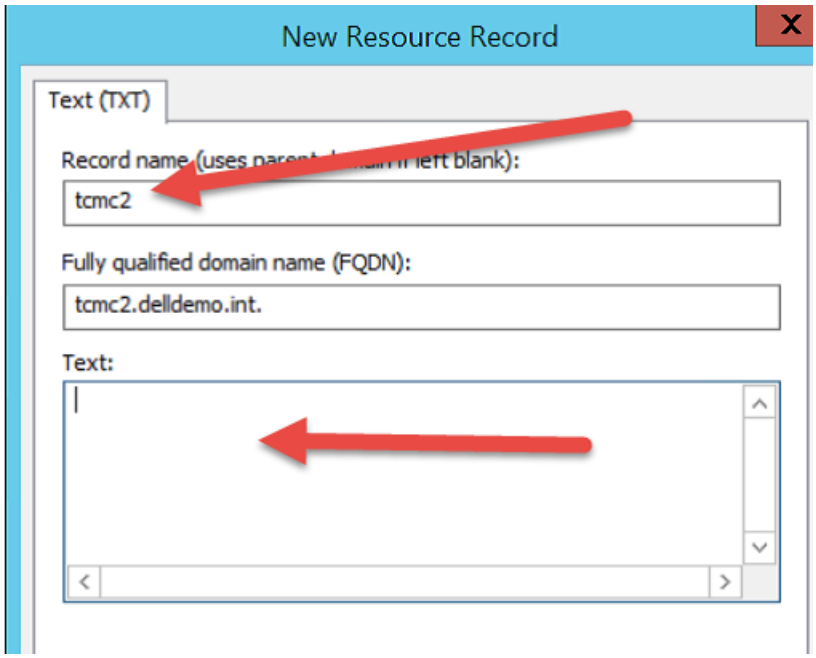


Figure 75. New Resource Record

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**.

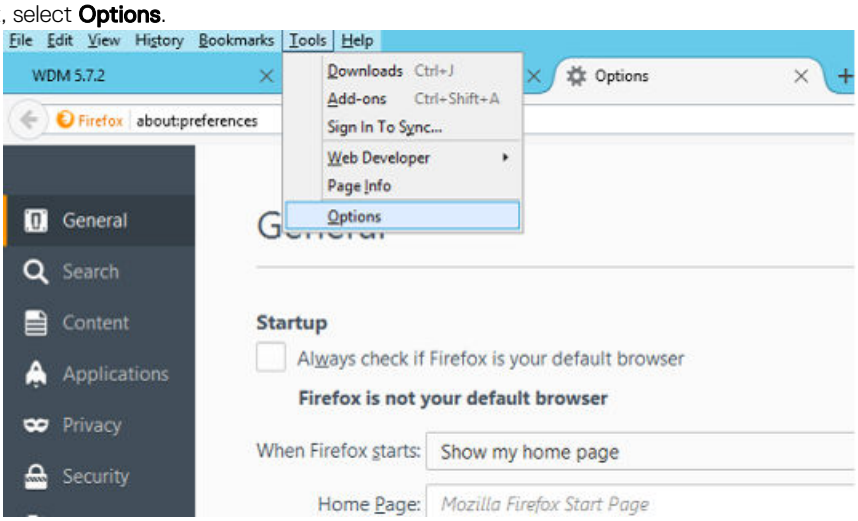


Figure 76. General Tab

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

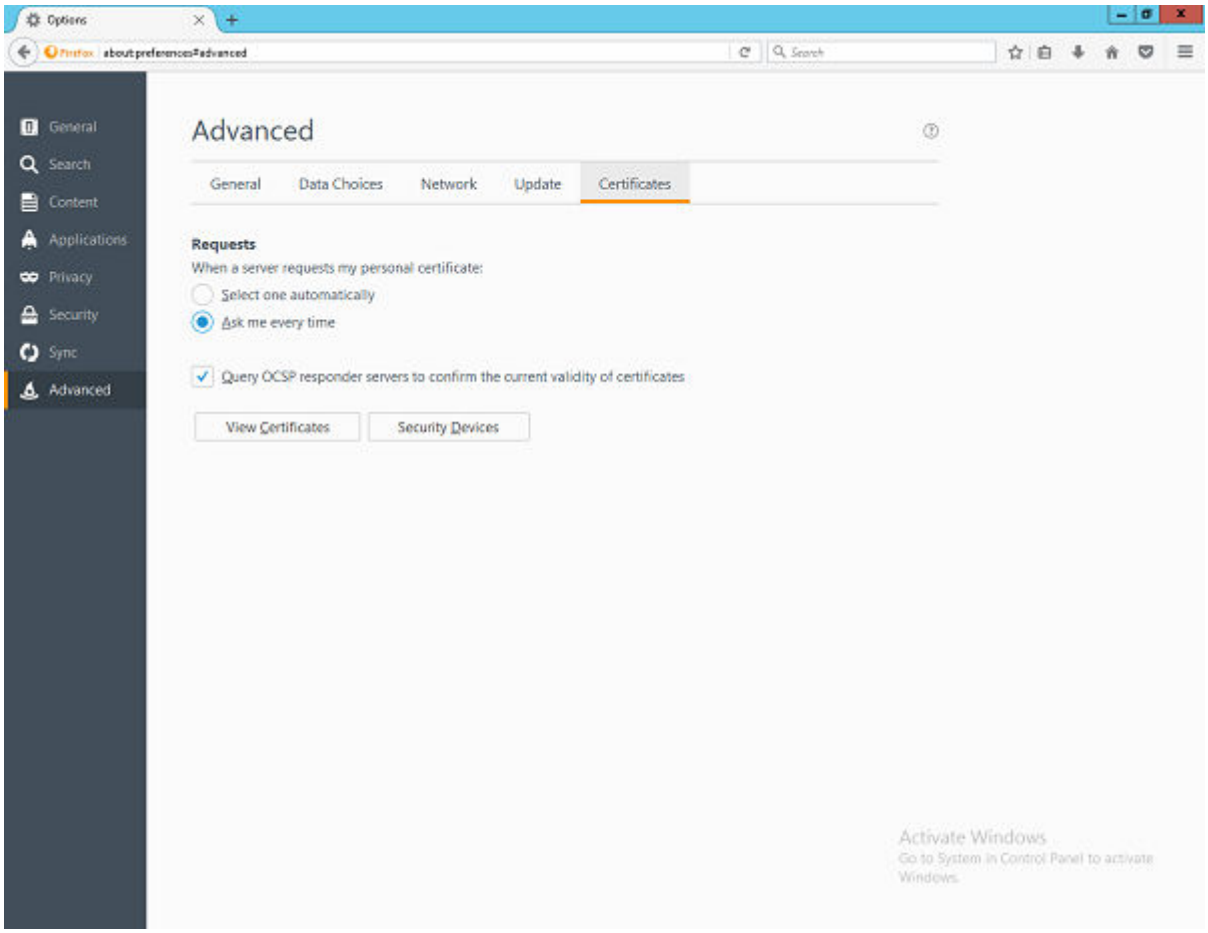


Figure 77. Advanced

4 Click **View Certificates** to open the Certificate Manager window.

5 Select the **Authorities** tab on the **Certificate Manager** window and click **Import**.

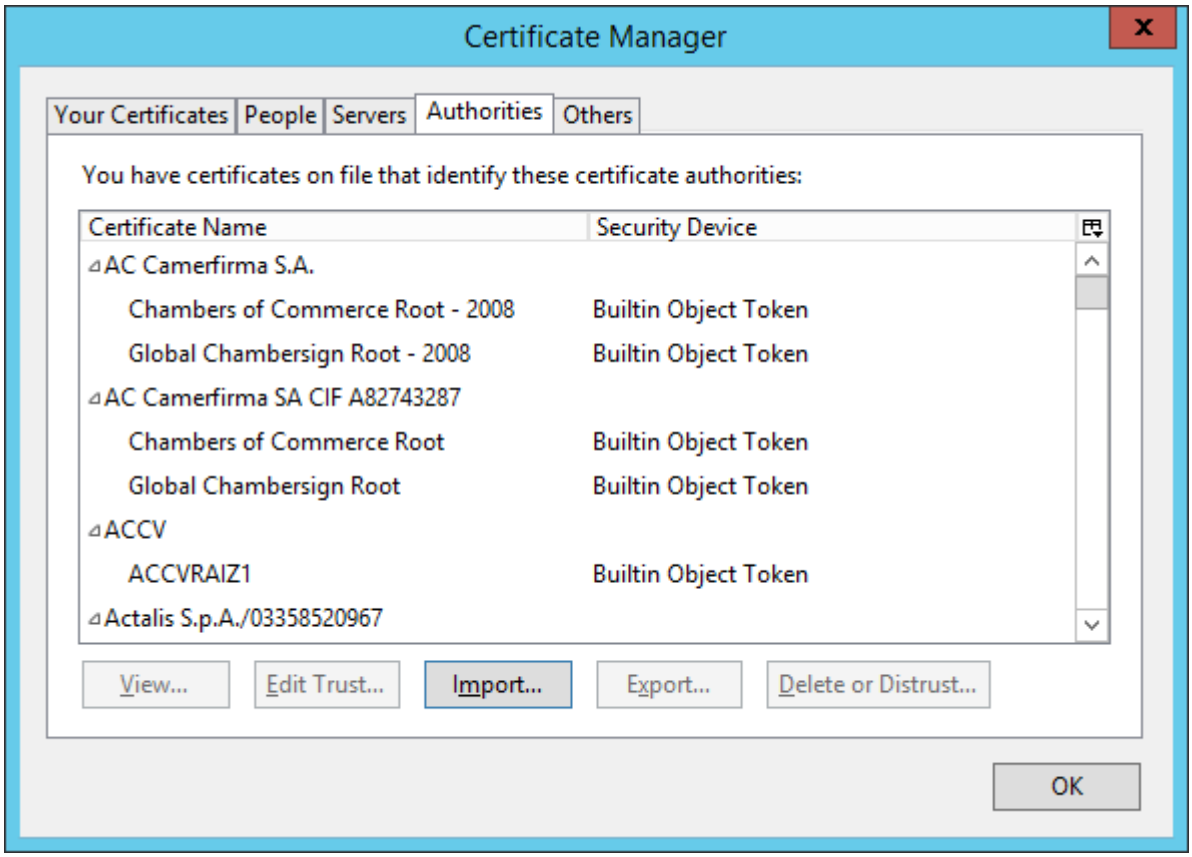


Figure 78. Certificate Manager

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.

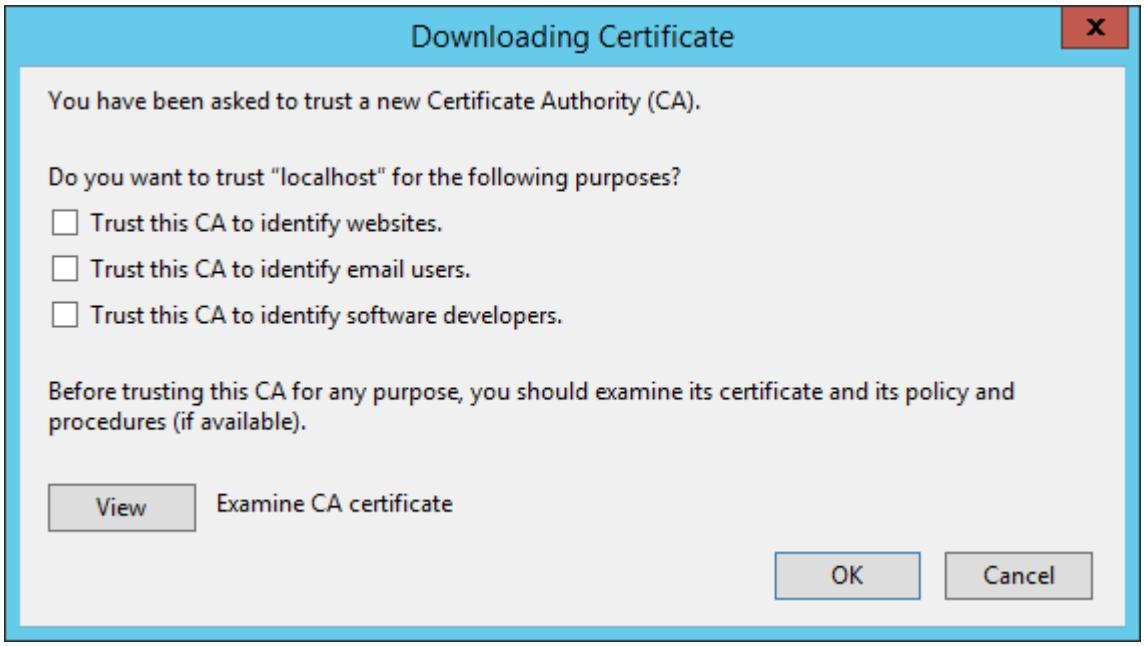


Figure 79. Downloading Certificate

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

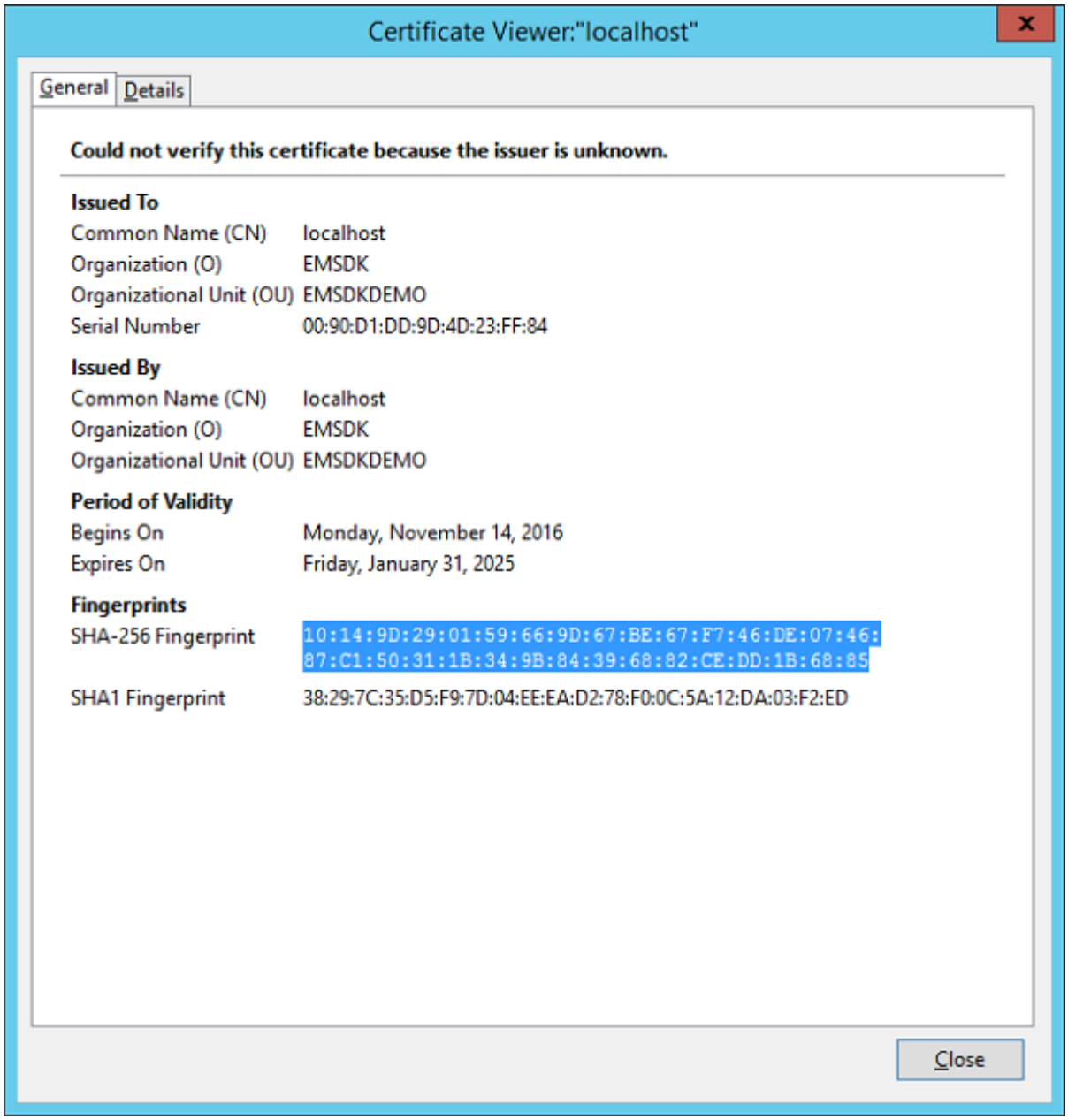


Figure 80. Certificate Viewer

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:

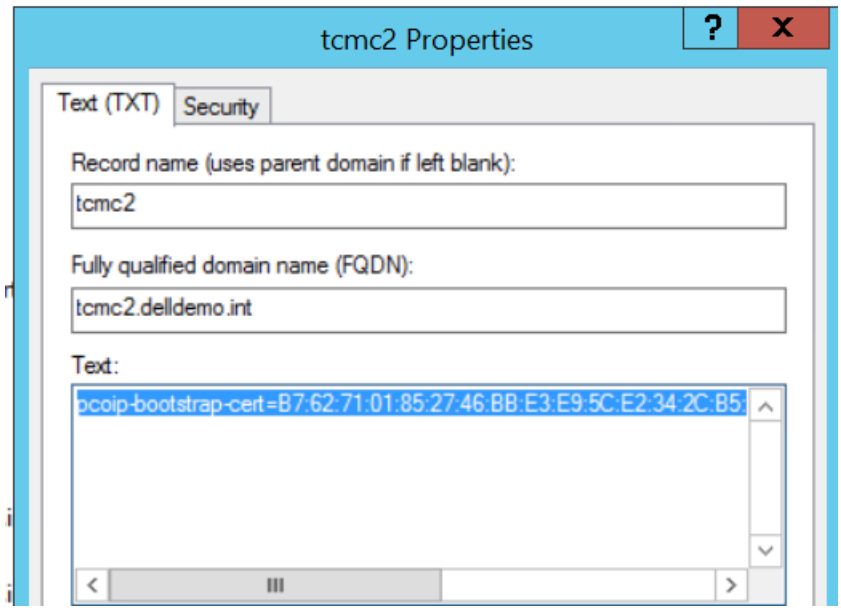


Figure 81. tcmc2 Properties

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

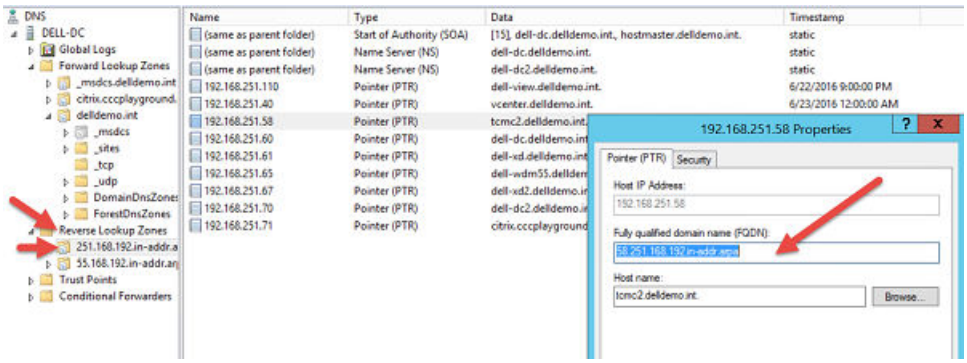


Figure 82. PTR Record

11 The zone must match the subnet that the host is in, and the record is the IP address assigned to the management console.

12 Once the DNS_SRV configuration is done, refer to Upgrading Teradici firmware from 4.x to 5.x using WDM for upgrading the firmware.

Upgrading the ThreadX 4.x devices to ThreadX 5.x from WDM

This section defines the steps to follow while upgrading the existing ThreadX 4.x devices to ThreadX 5.x devices from WDM. This helps you to continue the management of ThreadX 5.x devices from WDM after upgrading, using the new ThreadX management solution.

The following are the pre requisites to upgrade the ThreadX 4.x devices to ThreadX 5.x from WDM:

- ThreadX 5.x latest released firmware in the form of **.rsp** package should be available to upgrade.
- The FQDN of the WDM server should be available for **DHCP** or **DNS** configurations.
- Cert.pem which is available in the following path **WDM Installed directory** > **Wyse** > **WDM** > **Teradici**. This is not required, if the thumbprint is added to DHCP option tag or through DNS_SRV record as mentioned in previous chapters.

NOTE: Cert.pem is used to create certificate package and deploy to the ThreadX 4.x clients.

Before upgrading the ThreadX devices, use the following guidelines:

- To discover ThreadX devices using DNS SRV record: Adding the DNS SRV Record
- To deploy the certificate to ThreadX 4.x devices :Deploy the certificate to ThreadX 4.x Devices
- To upgrade the ThreadX devices: Upgrading the client firmware to ThreadX 5.x

Deploy the certificate to ThreadX 4.x Devices

To deploy the certificate to ThreadX 4.x devices, do the following:

1 Launch the WDM GUI and login to WDM with administrator privilege.
2 Go to **Applications** > **PCoIP Configuration Packages**.
3 Click the + button and download the **PCoIP configuration manager utility**.
4 Launch the utility which is downloaded and select **Version 4.x** radio button.
5 Click the **Security** option, and enable certificate checkbox.
6 Copy the **cert.pem** certificate contents including the first and last line (Begin certificate and End certificate).
7 Paste the **cert.pem** contents in the text box provided.
8 Enter the name and the description for the package in the respective text box.
9 Click on **Register** menu and **save** the configuration.
10 Go to **Devices** page in WDM Web UI and select the desired device using the check box provided.
11 Click on the **update** button, select the created configuration package from **PCoIP Configuration Packages** category and click **save**.
12 Go to **Jobs** page and confirm that the package deployment is successfully completed.

Upgrading client firmware to ThreadX 5.x

Deploying Teradici image version 5.x
To update the zero clients running 4.8.0 firmware version that has been updated with the new WDM 5.7.2 certificate or, if the security mode on the client is low, the Teradici firmware update Repository Support Package (RSP) must be created with the OLD OS type as TDC. This is required for upgrading the firmware from compatible 4.x version to 5.x.
To create RSP package, do the following:

1 Go to the Teradici support site, and download the latest ThreadX 5.X firmware.
2 Create a file with the following contents, save the file in **.rsp** format and provide the file name as *number* value in the file.

NOTE: The value of the *Number* field is the name of the firmware file. In the following example, the value is `522r5_2@39075.03b193e.5957929`.

```
[Version]
Number=522r5_2@39075.03b193e.5957929
Description=PCoIP Tera2 Firmware Release 5.2.2 for P25, P45, and 5050 AIO
OS=TDC
ImageSize=0
ImageType=merlin
Category=Images
[Script]
RB
```

3 Create a folder and place the **.all** file.

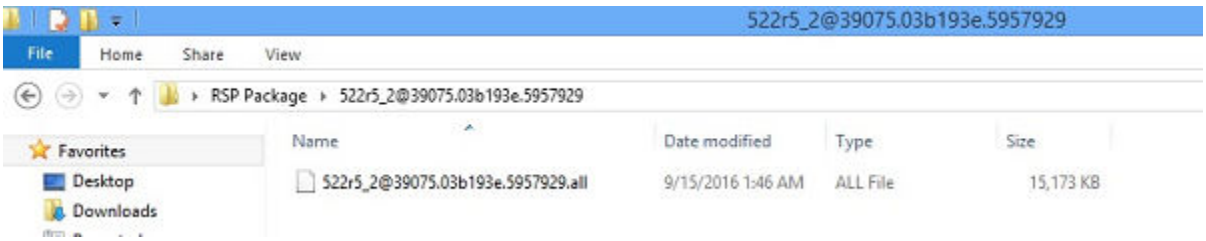


Figure 83. RSP package folder

4 Rename the folder name as *number* value in the **.rsp** file.

5 Place the **.rsp** file outside the folder.

NOTE: The file name of .rsp file, package folder name, and number value must be same.

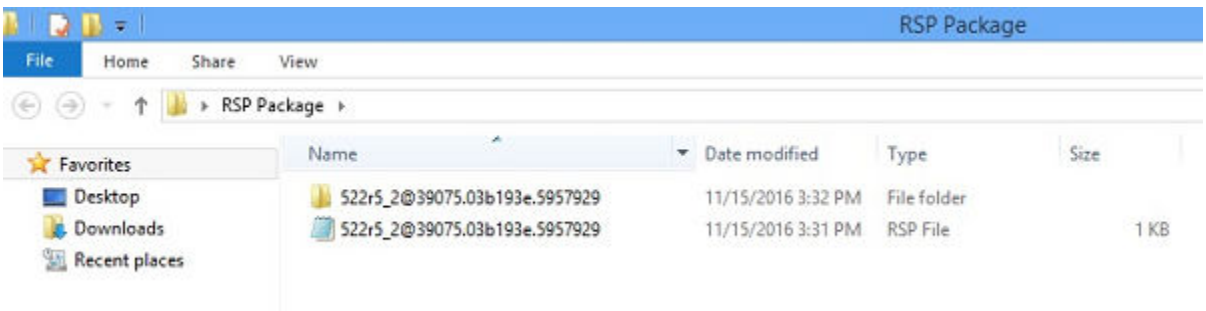


Figure 84. RSP package folder

After deploying the created RSP package through WDM as described in the Deploying Teradici image version 5.x from 4.x firmware using DDC in WDM and Deploying Teradici image version 5.x using selected devices in WDM, the client checks in to WDM as a 5.x device after the successful firmware upgrade to 5.x, and WDM recognizes them as ThreadX 5.x devices. Future 5.x firmware update RSP requires the new OS type TDC5 (OS=TDC5).

NOTE: All management features of ThreadX 5.x devices (devices having WDM compatible 5.x firmware) including the deployment of RSP packages with TDC5 as operating system type (OS Type) can be deployed through WDM web UI only and is not supported using desktop version of WDM.

Prerequisite on WDM repository for deployment of firmware and OSD logo using WDM web UI for ThreadX 5.x devices

Deployment of firmware package with OS Type TDC5 and package containing OSD (On Screen Display) logo for ThreadX 5.x devices, it is mandatory to have CIFS protocol enabled to upload the files from WDM repository.

Make sure the Software repository test connection for CIFS is successful. To test CIFS connection, do the following:

1 Open the WDM web UI, and log in as administrator.

2 Go to **System** > **Repositories**.

3 In the CIFS section, click the **Check Connection** link.

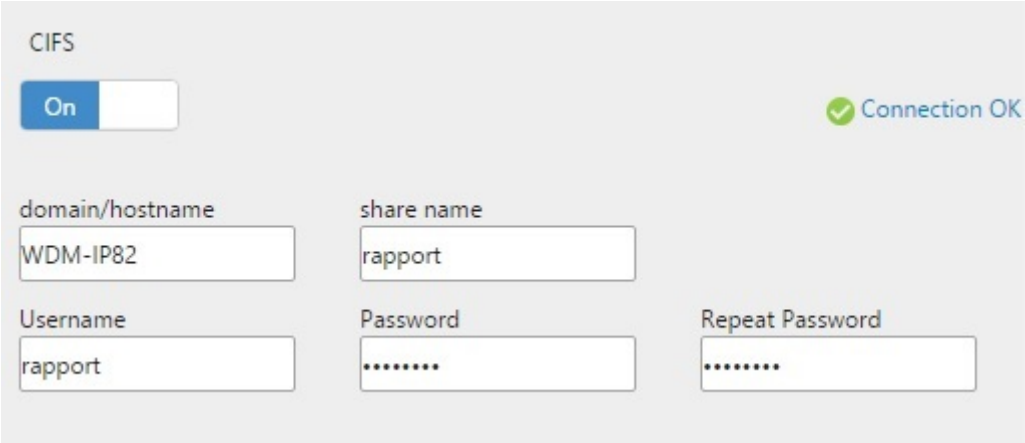


Figure 85. CIFS

After testing the CIFS connection, add the following accounts to **Rapport** ftp folder, and share permissions on the machine where WDM repository is configured:

- System account of the server where ThreadX 5.X component is installed.
- User account that is used to install WDM.

NOTE: If the repository is installed on a different server, then add the computer account of the ThreadX 5.x server instead of system account, along with the user account.

To give permissions to the **Rapport** folder available in the WDM repository, do the following:

1 Go to the **ftproot** folder location where you can find the **Rapport** folder.

2 Right-click the **Rapport** folder, and select **Properties**.

3 Click the **Sharing** tab, and then click **Advanced Sharing**.

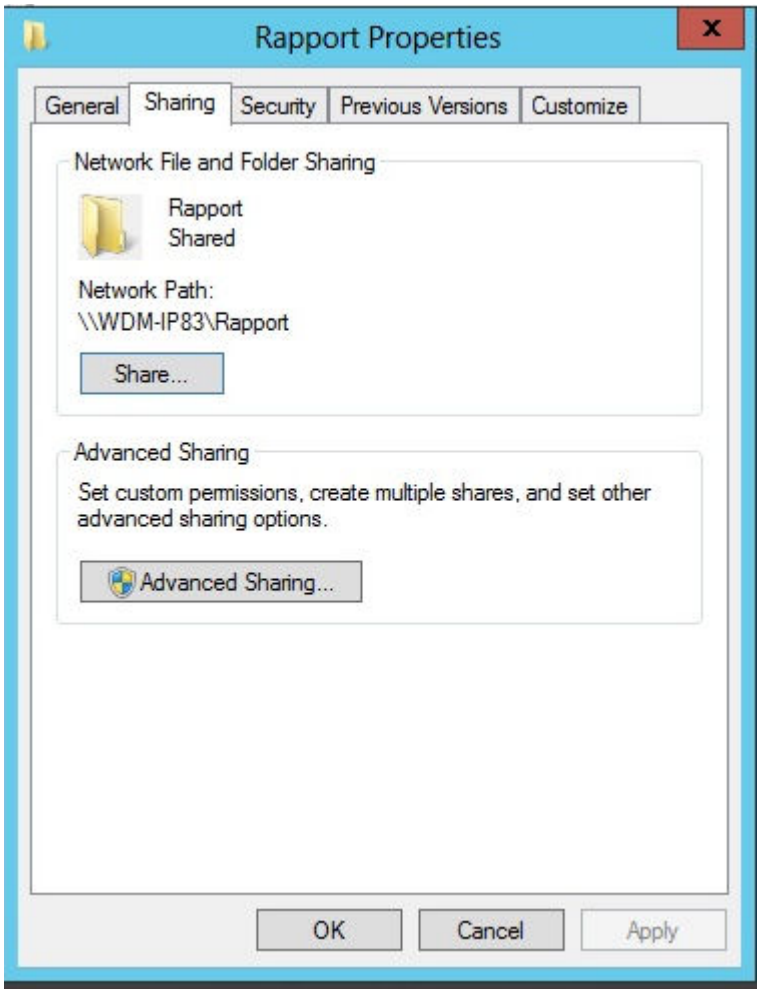


Figure 86. Rapport Properties

4 In the **Advanced Sharing** dialog box, click **Permissions**.

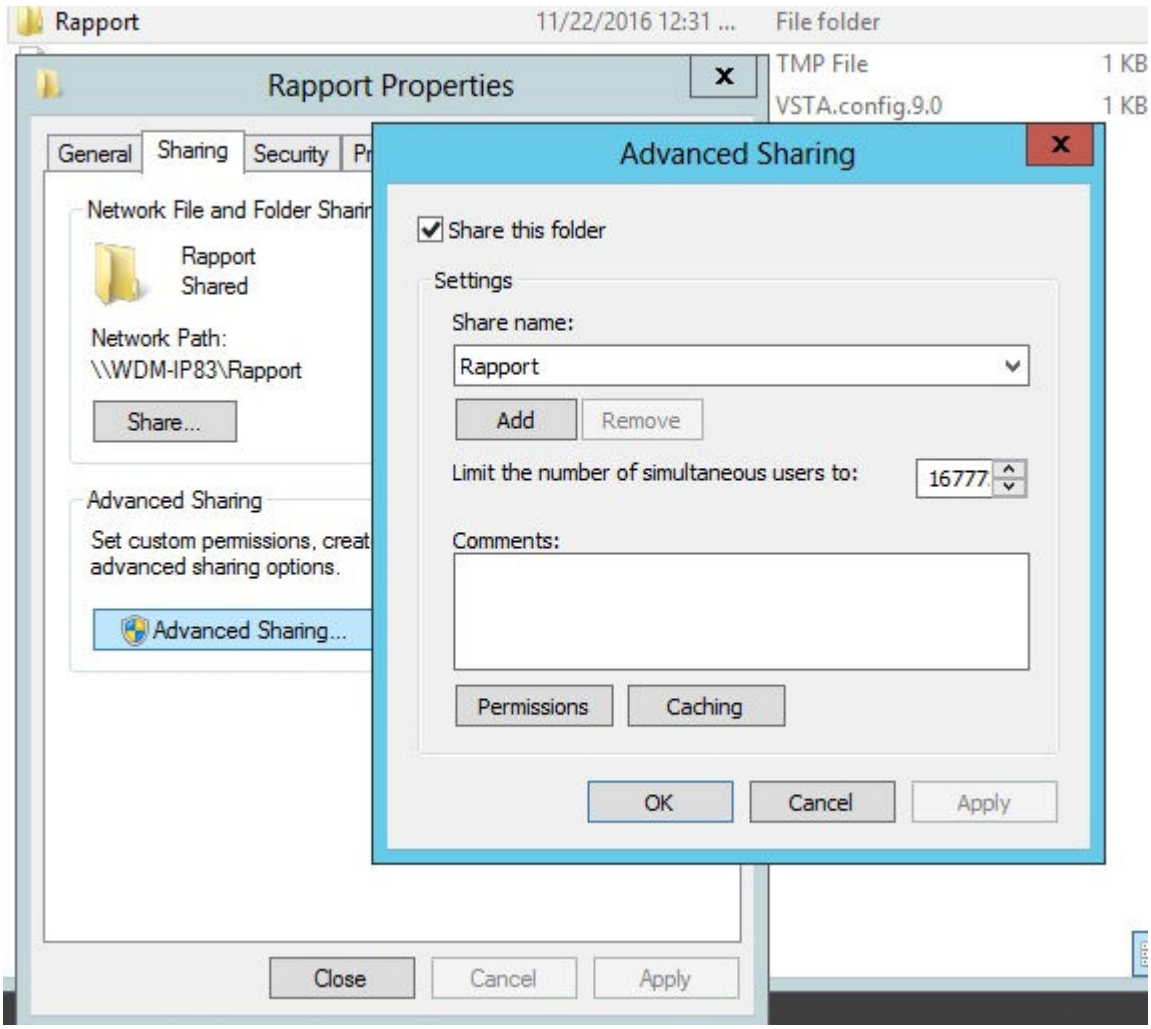


Figure 87. Advanced Sharing

5 Click the **Add** button, and give full permissions to the above mentioned users.

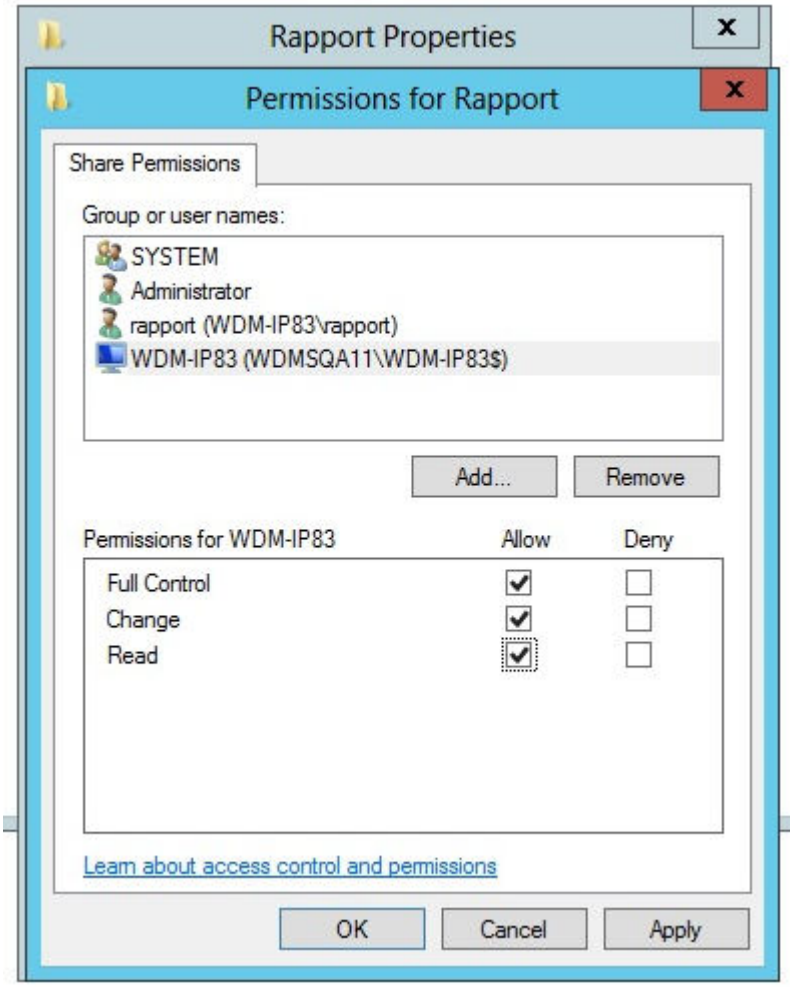


Figure 88. Permissions for Rapport

Deploying Teradici image version 5.x from 4.x firmware using DDC in WDM

To deploy the Teradici image version 5.x from 4.x firmware using DDC in WDM, do the following:

1 Open WDM Web UI and login as administrator.
2 Go to **System** > **Console**, and enable **Default Device Configuration (DDC)**, and click the **Save** button.
3 Go to **Updates** > **DDC**, and click the**+** button to add new DDC.
4 Select ThreadX as operating system from the **Select Operating System** drop-down list.
5 Select the preferred media size from the **Select Media Size** drop-down list.
6 Select the preferred view from the drop-down list.
7 Click **Add** to include the new DDC to the groups.
8 Select the registered image from the Image drop-down list.
9 Select the registered certificate package from the Packages drop-down list.
10 Select the device check-in from the Execute DDC drop-down list.
11 Click the **Save** button to save DDC.
12 Go to the **Devices** page and refresh the device information. The device gets rebooted and discovered to WDM automatically as ThreadX_5x devices.

Deploying Teradici image version 5.x using selected devices in WDM

To deploy Teradici image version 5.x using selected devices in WDM, do the following:

1 Open WDM Web UI and login as administrator.
2 Go to **Applications** > **Images**, and click the **+** button to download the package registration utility
3 Click the **RSP** button from the package registration utility.
4 Click the **Browse** button, and upload ThreadX 5.x firmware package to WDM.
5 Go to WDM Web UI again, and go to **Devices** page.
6 Select the devices which are required to upgrade using the check box.
7 Click the **Update** button, and select the registered package from the Images category.
8 Click the **Save** button to schedule package deployment. The package gets deployed.
9 Go to **Jobs** page and confirm whether the package deployment is successfully completed. The device gets rebooted and discovered to WDM automatically as ThreadX_5x devices.

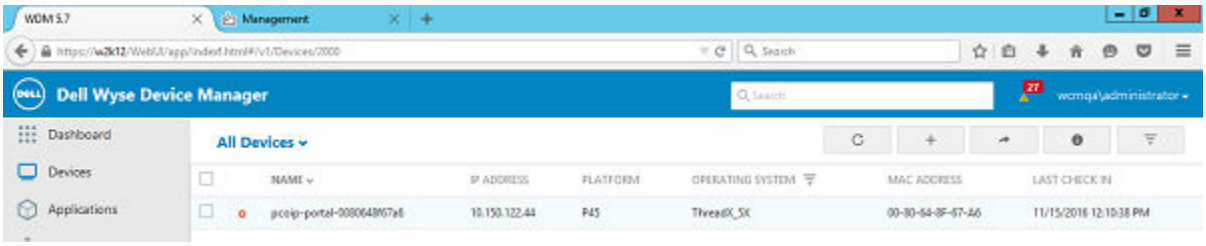


Figure 89. Devices

NOTE: After successful deployment of the 5.x firmware on the client, if the devices are not appearing on the WDM as ThreadX5x devices, refer to EMSDK fails to start due to port number to resolve port conflict of the ThreadX 5x software components, and see if the problem is solved.

11

Troubleshooting

This section provides troubleshooting information for WDM.

Topics:

Problems with Discovering Devices

Problem: You are having problems with discovering devices.

Solution: Ensure that the:

1 Device service is running correctly
2 Server service is running correctly
3 Path between the device service and the server service is running correctly (use ping)

4 Subnet and IP ranges are defined correctly (when you are attempting to discover devices by subnet or IP range)

You can also run the **DNS_DHCP_Lookup Utility** to verify if the WDM server is reachable or not.

Problems with Discovering PXE Devices

Problem: You are having problems with discovering PXE devices.

Solution: Ensure that:

1 port 4011 is open in all routers
2 IP-Helper addresses are defined and pointing to the WDM-Server
3 the PXE devices have re-booted at least one time after being discovered by WDM (before WDM recognizes them as PXE devices, the PXE devices must be re-booted at least one time after being discovered)

Package Errors

Problem: You are receiving package errors.

Solution: Try the following:

1 Verify the scripting syntax
2 Edit the script (*.rsp) and re-mark out LU command (have target device available)
3 Make use of Network Sniffer
4 Ensure that the WDM Server IP address has not changed
5 Ensure that the Repository information is correct
6 Ensure that you can manually FTP a file to the Repository
7 Ensure that you can run an unattended install
8 Ensure that the package structure is correct (Folder = *.rsp name = scripts'NUMBER'value)

Wake on LAN Command Does Not Reach Remote Devices

Problem: The HServer is unable to send the WOL command to the remote devices.

Solution: Enable port forwarding for UDP port 16962.

Peer Assisted Deployment Issues

This sections describes some common issues or questions you may have with respect to Peer Assisted Deployment.

Determining whether the HTTP Application used for PAD is Running and Responding

The HTTP application used for PAD accepts the V99 command that can be sent to a system through the browser. The response to the V99 command from the HTTP Application would be &00. For example, if the HTTP application is running on a system with the following URL 10.150.202.101 and it listens on port 9980, the V99 command would be:

```
http://10.150.202.101:9980/V99
```

and the response to this command would be:

```
&00
```

NOTE: The system does not use any basic authentication for the V99 command.

Running the HTTP Application Manually

To run the HTTP Application Manually:

1 Launch the command prompt on the system where you have installed WDM.

2 Type the following command:

```
Wyse-Http-server.exe -u  < Username>  -p  <Password > -Po  <Port number>
```

where **— u** is the user name for basic authentication, **—p** is the password for basic authentication, and **—po** is the port number on which the HTTP Application is running.

Peer Device is unable to download an Image file

If the peer device is not able to download the **bios.img** or the **cmos.img** files, then you must check if the files are available on the PAD master device under the following folder path: **C:\Program Files\WDM**.

Determining whether the WDM Agent and WDM Server Communication is related to the PAD Schedule

All communication between the WDM Agent and the WDM Server that is related to the PAD Schedule would have the PAD tag set to **1** as part of the request or response.

Profile Manager Issues

This section describes the issues you could face with Profile Manager and the steps to troubleshoot them.

WCM Application does not launch during the creation of the Profile Manager Package

This could happen if the WCM application or its components are corrupt or are not available in the Installation folder.

Profile Manager Package does not get deployed

To troubleshoot this issue:

1 Check if Profile Manager is enabled in preferences. For more information.

2 Check if Profile Manager deployment is supported by the client system. For this:

   a Select the **Device Manager** node on the tree pane of the WDM Console.

   b On the right-hand pane, select the device to which you want to deploy the package.

   c In the **Device Properties** pane click the **Hardware Info** tab.

   d The **WCM Support** field should be set to **True**. If it is set to **False**, then it indicates that the client does not support Profile Manager package deployment and you need to update the WDM Agent on the Client.

3 Check if there are some scheduled packages that are yet to be deployed. Wait till the packages are deployed successfully.

4 Check if there are some scheduled packages in **Error** state. If there are such packages, then delete them.

5 Check if the client is already updated with the profile manager package prior to the deployment. To verify the same, configure Profile Manager to deploy another package with a different configuration.

Tips to Troubleshoot the Repository

General Tips:

If repository test connection fails, make sure the following settings are as per requirement for repository to work:

- Make sure the user id and password for the repository is correct.
- Go to rapport user and check the option **Password never expires**.
- Make sure the IP address/host name of the repository server is correct.

Tips when Transfer Type FTP:

If repository test connection fails in case of FTP, make sure the following settings are as per requirement for repository to work:

- FTP service is up and running.
- FTP site is created.
- FTP site has “Read” and “Write” permission for all users with “Basic” and “Anonymous” authentication.
- Try to connect to FTP using command prompt.
  - ftp <ip address> <userid>
  - It will ask for the password and will connect to the FTP directory.

Tips when Transfer Type HTTP:

If repository test connection fails in case of HTTP, make sure the following settings are as per requirement for repository to work:

- Make sure the virtual directory exist. If not follow the below mentioned steps to create it:
  - On the taskbar, click **Start->Administrative Tools->Internet Information Services (IIS) Manager** to open the **IIS Manager Window**.
  - In the tree pane, right click on **Sites->Default Web Site** and then select **Add Application...** to begin creating a Virtual Directory.
  - Enter the **Alias** (the name of virtual directory e.g. **MyWDM**), select the **Physical path** as FTP root directory (e.g. c:\inetpub \ftproot) and then click **OK**.
  - Select **Sites->Default Web Site->MyWDM** and then double click on Authentication, select Basic Authentication and enable it from the “Actions” Panel.
  - To verify the virtual directory is configured or not, in the tree pane, select **Sites->Default Web Site->MyWDM** and then on right pane click on **Browse*:80(http)**. It will open the ftp directory in the browser (IE).
- Look for the following setting in IIS to verify the following Role Services are installed:
  - WebDAV Publishing
  - Basic Authentication
  - Windows Authentication
  - IIS Management Console
  - IIS Management Scripts and Tools
- Make sure the in IIS following Role Services are not installed:
  - Request Filtering
  - Static Content Compression
  - Dynamic Content Compression
- In Advanced Settings of DefaultAppPool in the Application pool list, make sure the following:
  - In the General section, ensure that Enable 32-Bit Applications is set to True
  - In the Process Model section, ensure that Idle Time-out (minutes) is set to 0 (zero)

Tips when Transfer Type HTTPS:

If repository test connection fails in case of HTTPS, the steps to make sure that the configurations are correct are the same as HTTP. For HTTPS:

1. Launch the IIS Manager, and right-click on **Default Web Site**.
2. Select **Bindings** on the menu options.
3. In the **Site Bindings** window, check if **https** is specified under Type.
4. Check if the default port number is displayed as **443**.

Tips when Transfer Type is CIFS:

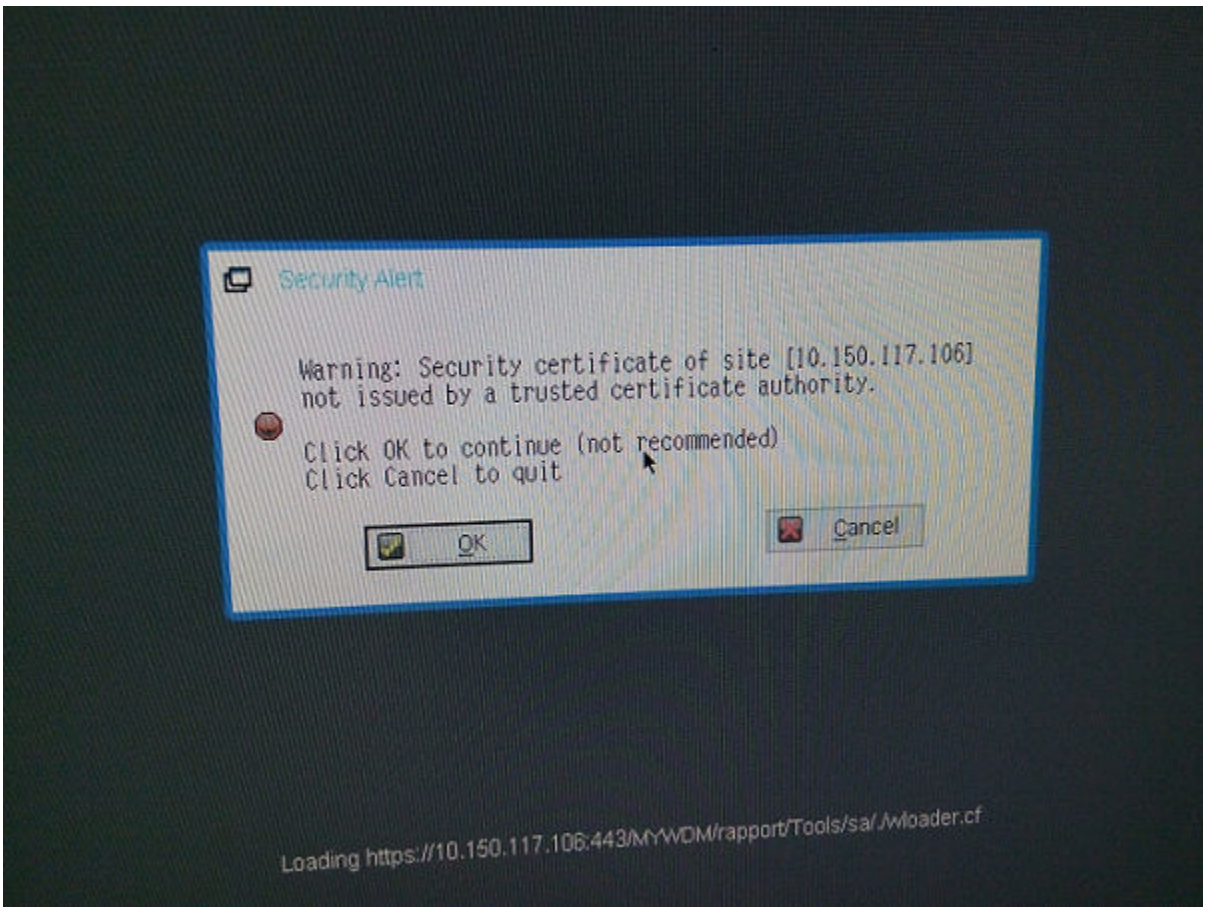
If repository test connection fails in case of CIF, make sure the following settings are as per the requirements for the repository to work.

- The **Rapport** folder is shared
- The **Rapport** folder has **Read** and **Write** permission for **Everyone** or specific users.
- Enter the hostname/domain name, user name and password to access the shared folder, and try to connect.

Troubleshooting T50 and WTOS Errors

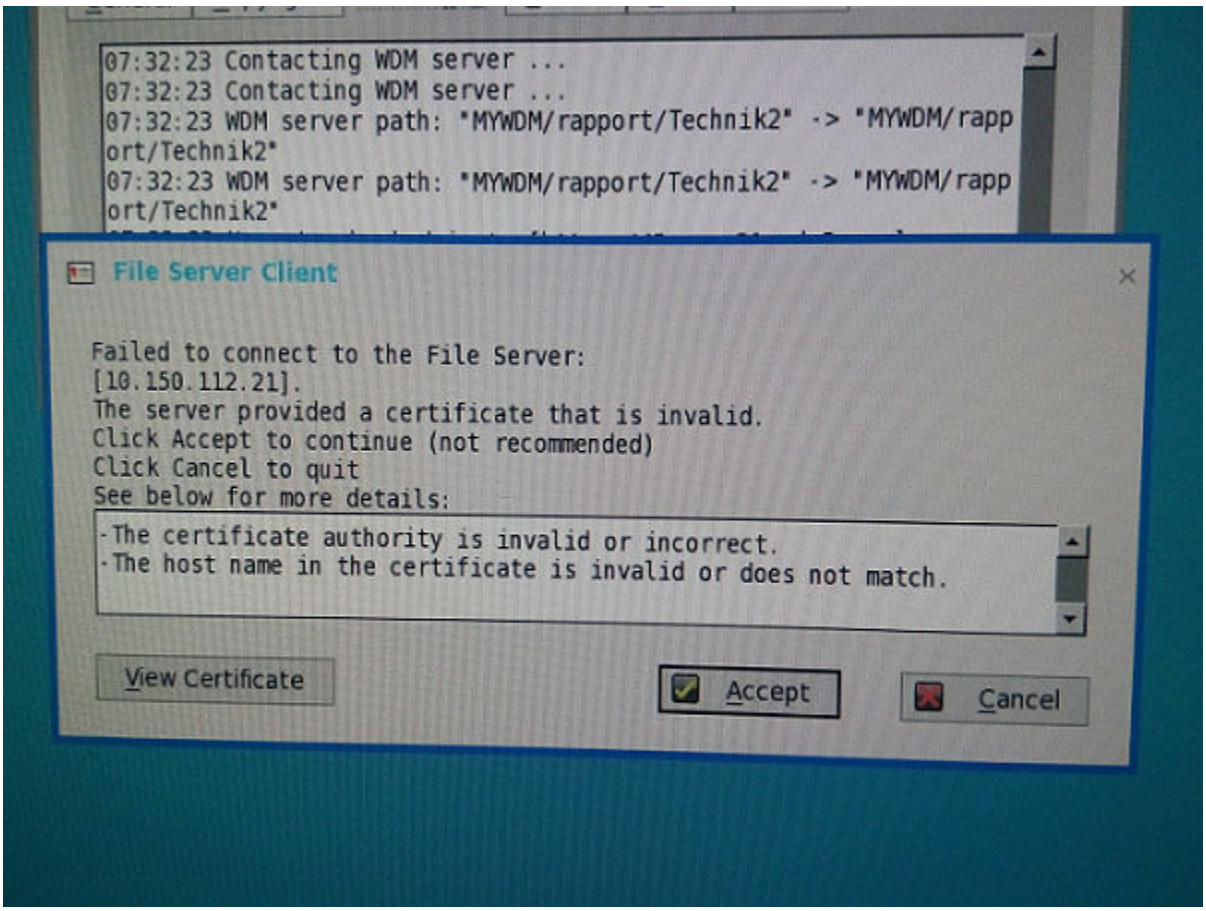
When T50 devices are checking in the WDM 5.0 security alert messages may be displayed.

For Ubuntu T50 devices, the following message is displayed:



Click **OK** to continue.

For WTOS devices, the following message is displayed:



Click **Accept** to continue.

Troubleshooting WCM Issues

When you use WCM from WDM to create configuration files to be deployed to devices, you may come across the following issue:

When you select all the configuration items and create the **configuration.xml** file, the relative path is missing from the XML file. The solution for this issue is that when you create WCM packages, you must not have any space in the file name. For example, if you want to name your configuration file as **WCM Config**., it should be specified as **WCM_Config**.

Package Update Fails When CIFS Repository is Enabled

Problem: When you enable CIFS Repository for any package update and deploy the package to some WES7, WES7P, WE8S, or WES2009 devices, then the package update could fail. This could happen when the WDM Agent is an older agent and does not support the CIFS protocol.

Solution: You must update the WDM Agent to the latest available version on all the devices where the package update fails.

PAD Imaging and Drag and Drop Features Not Working on Linux Devices

Problem: The package drag-and-drop feature and PAD Imaging does not work on SUSE Linux devices with the MR3 build and the latest WDM Agent version 5.3.06, when Windows Authentication is enabled on WDM with the HTTPS protocol enabled in the software repository.

Solution: Enable Basic Authentication in IIS Manager or change the protocol to CIFS in the software repository.

Default Device Configuration Does Not Display Exported Images

Problem: When you export a pulled image and re-register it in WDM, the DDC window does not display the image.

Solution:

1 Navigate to the folder where the **.rsp** file is located.

2 Open the file in notepad and make the following change:

```
Command=%imageread% to Command=%imagewrite%
```

3 Save and close the file. The image is displayed in the DDC window when you launch it in the WDM Console.

VNC Log Not Generated

Problem: The VNC Log may not be generated when you are using the FTP repository.

Solution: You must disable the firewall or add a specific inbound rule to generate the VNC log.

'Update Now' window is not displayed to the user for WCM-Linux

Problem: Update Now window is not displayed to the user immediately after pushing the WCM file for Linux devices.

Solution: RebootQU is scheduled along with WCM configuration for Linux devices. This RebootQU is run when the device does partial or Full check-in or Administrator must refresh the device manually.

Not able to push pulled image back to T50 device

Problem: Not able to push pulled image back to T50 device having 8MB MICRON chip.

Solution: Re-register the pulled image by removing <wdmMessage><\wdmMessage> tag from the .rsp file.

PCoIP Language package deployment failed

Problem: Language package created using **PCoIP Configuration package** creation tool failed to deploy.

Resolution : If both **Connection Management interface** and **VMware View server** details are given at a time, Deploying the language package is failed. Because both settings are mutually exclusive.

Devices not checking in Japanese OS

Problem: If we have Hagent older than 6.3.2.54 in the devices then devices will not check in to Japanese OS.

Solution: Update the Hagent to latest and then discover the devices in the WDM Server (Hagent should be greater than or equal to 6.3.2.54).

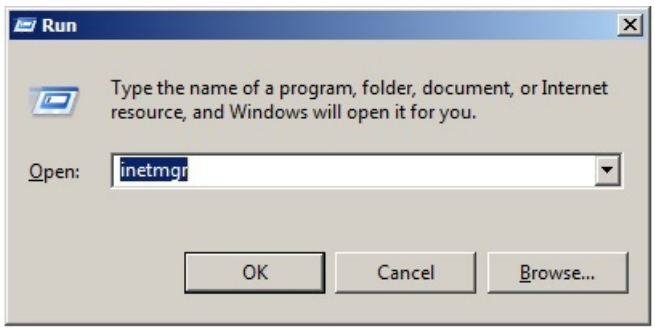
After Upgrading WDM from version 5.5 or MR to 5.7 Application Failure

Issue: When you start the WEB UI after Upgrading the WDM from version 5.5 or MR to 5.7, an error message is displayed as **Application not found**,

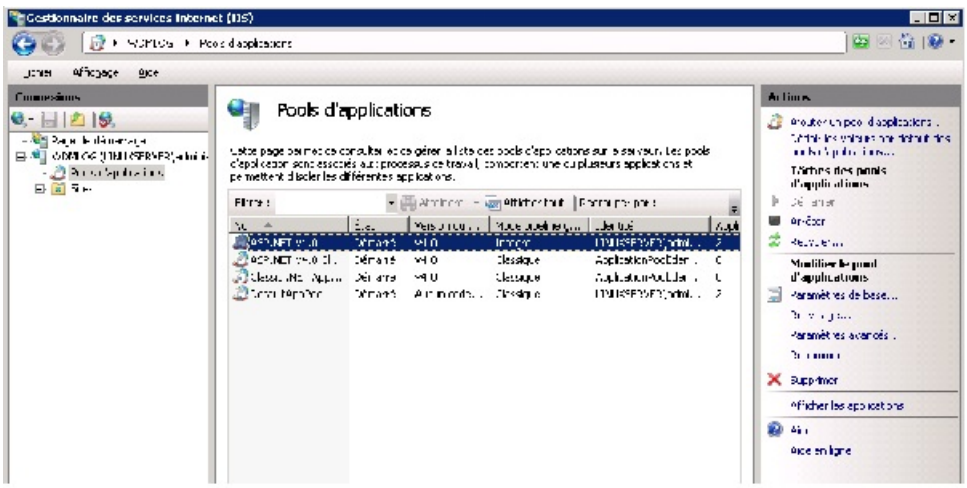
Reason: This issue happens when the apppool identity is not properly set, and the password gets expired or corrupted.

Solution:

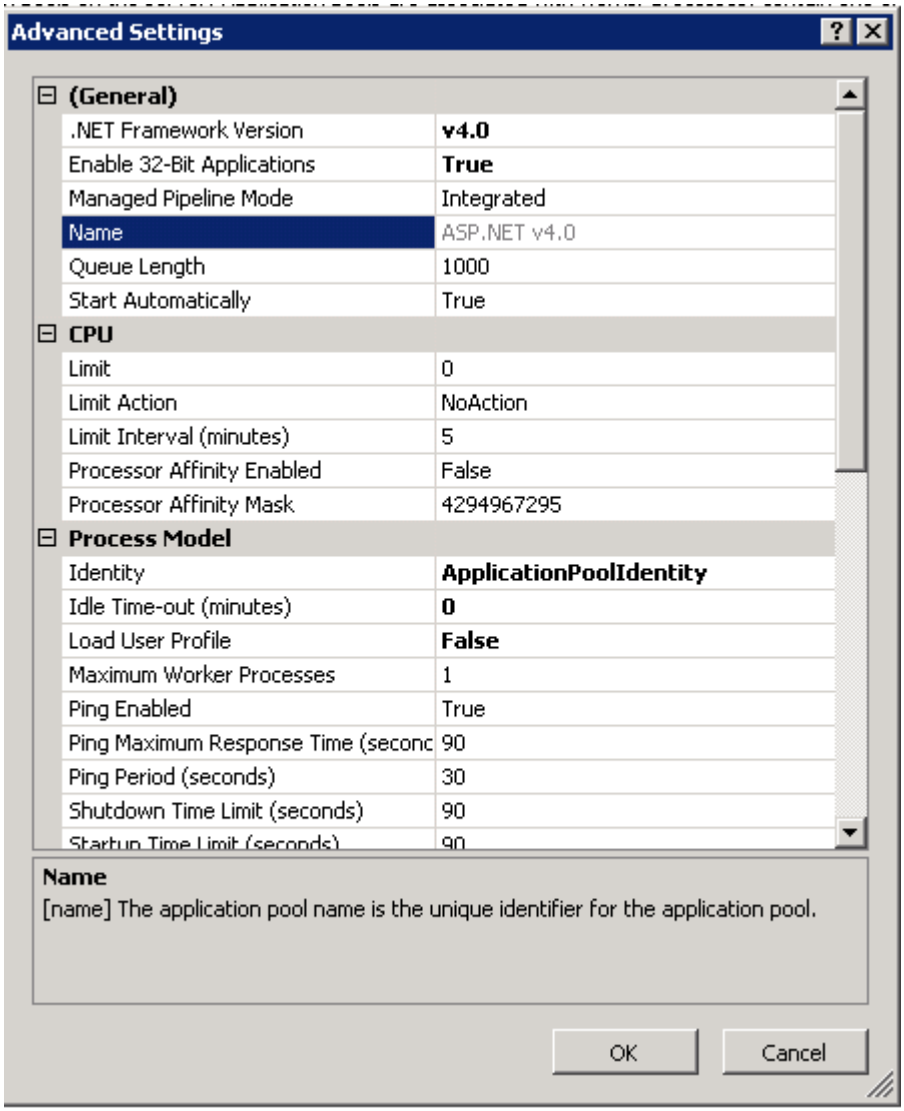
1 Go to IIS manager (type `inetmgr`in `Run` under windows).

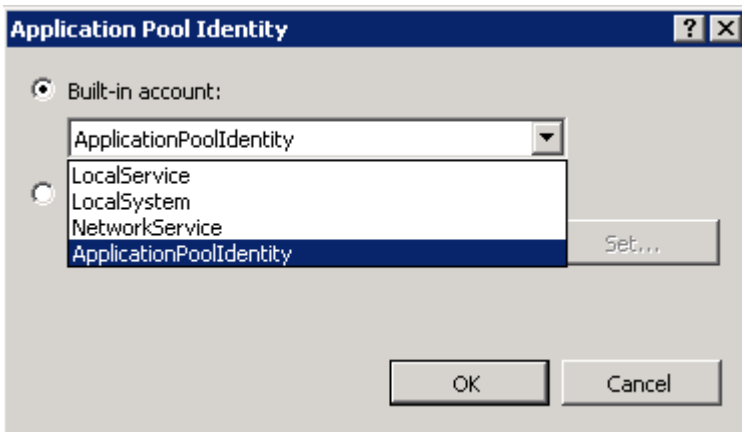


2 Navigate to the **ASP.NET v4.0** App pool and select the advanced settings. If you are performing this troubleshooting for the first time, you must note down the Identity value (for example, see image)LINUXSERVER\administrator)



3 Change the Identity property from to ApplicationPoolIdentity.





4 Apply the settings and start the Application pool to run the WDM Web UI to see if the application starts.

- If the application shows login screen, follow Step-5.

5 Now follow the steps 1 to 2 and change the Identity of the **ASP.NET v4.0** App pool to the original setting, there is a prompt to enter the password and confirm it. After entering the password, apply the settings and start the app pool. Once this is done, start using the Web UI.

ThinOS device stops check-in to the WDM server

Problem: ThinOS device stops check-in to the WDM server, due to untrusted certificate and then you can't manage it.

Solution: We need to send the following ini setting to the device in order to make it work:

securitypolicy=low

Steps to deploy it to the device:

- Create a folder named **wnos** in **ftp** location.
- Create an ini file with the name **wnos.ini** in the **wnos** folder and in the **ini** file add the content as **securitypolicy=low**.
- Provide the **ftp** server location on the device end.
- Device downloads the ini file and apply the settings.

Issue in Discovering the devices having old HAgents (6.3.2.54 & below) on Localized WDM Server

Problem: Not able to Discover the devices having old HAgents (6.3.2.54 & below) on Localized WDM Server.

Pre-requisites: If the Rules are added to **RequestFilteringModule**, then you should export the rules by following given steps. .

Solution:

1 Click **IIS** Root.
2 Select **Modules** on the right pane.
3 Right —click **RequestFilteringmodule**, and select **Unlock** to continue.
4 Select **Rapport HTTP Server** on IIS left pane
5 Double-click **Modules** on right pane, select **RequestFilteringModule**, and delete the **Module** to continue.
6 Restart **Rapport HTTP Server**.
7 Restart the **Devices** ,or the Agent would check-in to WDM Server.
8 Update the **HAgent** to the latest available package.
9 Add **RequestFilteringmodule** to follow this steps.
10 Select **Rapport HTTP** Server, double-click **Modules**, and select **Revert** to parent from right menu.
11 Select **RequestFilteringmodule**, and click **OK**

to continue.
12 Go back to **IIS Root**, select **Modules**, right-click **RequestFilteringmodule**, and then select **Lock.**
13 Restart the Rapport HTTP Server.

After finishing all the steps import the rules back to the module

Login page not appearing in the WEB UI

Problem: While connecting to the Web UI using IE Browser, login screen does not appear for the first time and the screen appears blank.

Solution: Refresh the browser to see the login page.

Issue While logging in to WEB UI

Problem: Login to WDM Web UI is not possible, If the WDM server is joined to the Windows Server 2012 domain controller.

Solution: The **GetAuthorizationGroups()** function fails on groups (SIDs) which are added to you by default, when a 2012 domain controller is involved.

Installing KB2830145 on the WDM server will resolve the issue.

EMSDK fails to start due to port number

Problem: EMSDK component uses port number 49155 by default for its communication. If the startup of EMSDK fails due to non-availability of the mentioned port, then user shall manually stop the EMSDK server which is running in the console of the machine where software is installed, and provide a available port number in the following files:

Solution:

1 Go to Program files path where EDM file is installed **\Wyse\WDM\Teradici\EMSDK**, open the **emsdk.properties** file in notepad and assign the available port number in the field **emserver.serverPort=49155**, For example, 49159.

2 Set the new port number in the file **C:\inetpub\wwwroot\ThreadXApi\Web.config**, by opening the same file in the text editor and replace the port number under the following tag:

- **<appSettings><add key="EmSdkPort" value="49155"/></appSettings>**

3 Restart the machine.

Domain user login and HApi Log Failure

Problem : Domain user login failure. The following HApi Log error message is displayed:

An error (1301) occurred while enumerating the groups. The group's SID could not be resolved.

Solution:: Install the Microsoft hotfix from the link and then try using WDM: www.support.microsoft.com/en-us/kb/2830145

Problem: Web UI login error occurs, if you prefix machine name to user credentials name.

Solution: Enter the user name and log in credentials.

Problems with accessing Device Page

Problem: You are having problem while accessing the device page. It gets logged out when you try to access the page.

Solution: Clear the cookies and cache of the system and try to login again.

OSD Logo Configuration/Firmware Push Failure on ThreadX 5.X Devices

Problem: Failed to push OSD logo configuration or firmware upgrade.

Solution: Make sure Software repository test connection for CIFS is successful.

Add the following accounts to rapport folder sharing permissions:

- System account of the server where ThreadX 5.X is installed.

- User account which is used to install WDM.

To give permission to the user, do the following:

1 Right-click the rapport folder from repository and select properties.
2 Click the **sharing** tab.
3 Go to advanced sharing option and click **permissions**.
4 Click the add button and give full permissions to the above mentioned users.

ThreadX 5.X devices moves to Offline state

Problem: ThreadX 5.X devices are moving to Offline after few days of discovery.

Solution:

1 Go to IIS management console.
2 Navigate to Application Pools.
3 Right click the ASP.NET v4.0 application pool and click **Stop**.
4 Right click the Advanced Settings of ASP.NET v4.0 application pool.
5 Scroll down to Recycling section.
6 Set the value of **Regular Time Interval(minutes)** to 0.

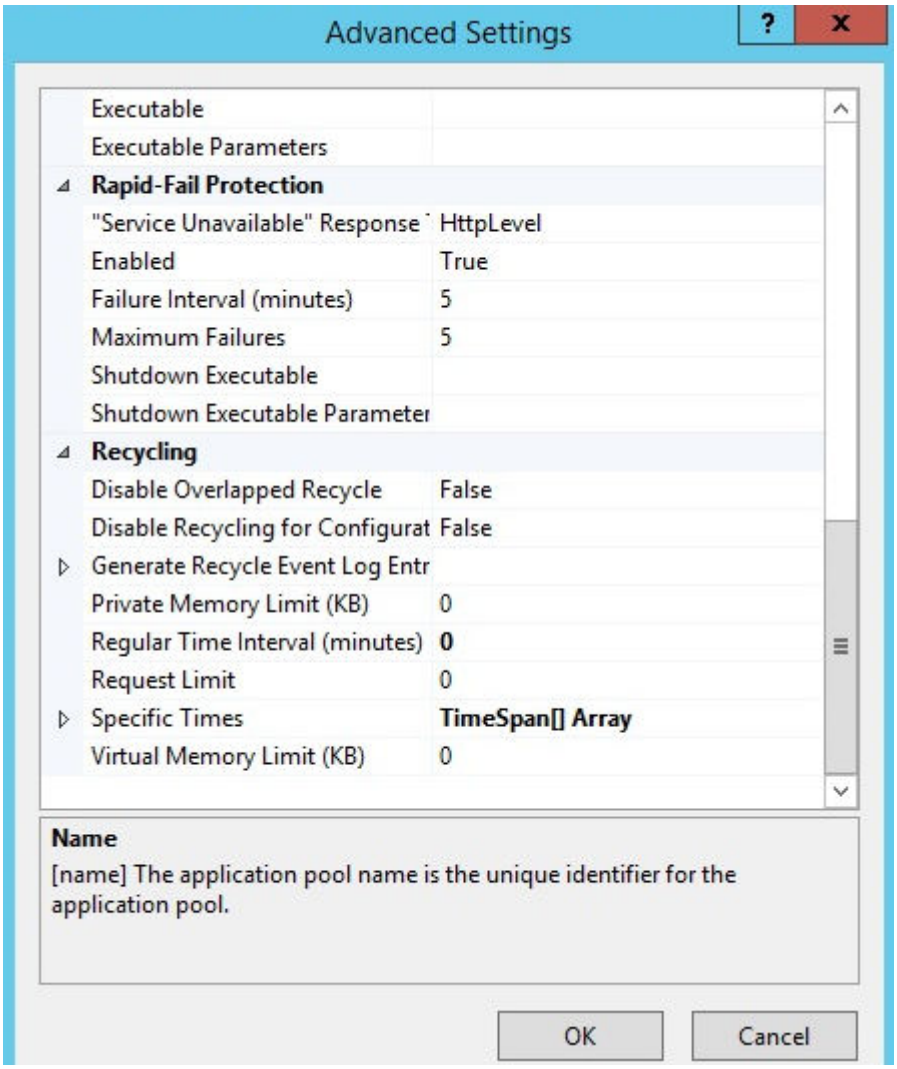


Figure 90. Advanced Settings

7 Right click the ASP.NET v4.0 application pool and click **Start**.

Manually configuring the ThreadX 5.X devices using teradici client management console when automatic way does not work

Pre-requisite: Make sure that EMSDK and ThreadXApi are installed and running successfully on the device.

1 On the management console of ThreadX device, select **Upload Menu** > **Certificate**, and browse for the certificate **cert.pem** installed at **<Wyse install folder>\WDM\TeraDici\cert.pem** where WDM is installed. After selecting the file, click **Upload** button.

NOTE: Uploading the cert.pem certificate is important for the client to establish the connectivity with the EMSDK server, as the EMSDK server validates the certificate data from the client when it attempts to connect to the server. Any mismatch in the certificate data, the server rejects the connection request from the device.

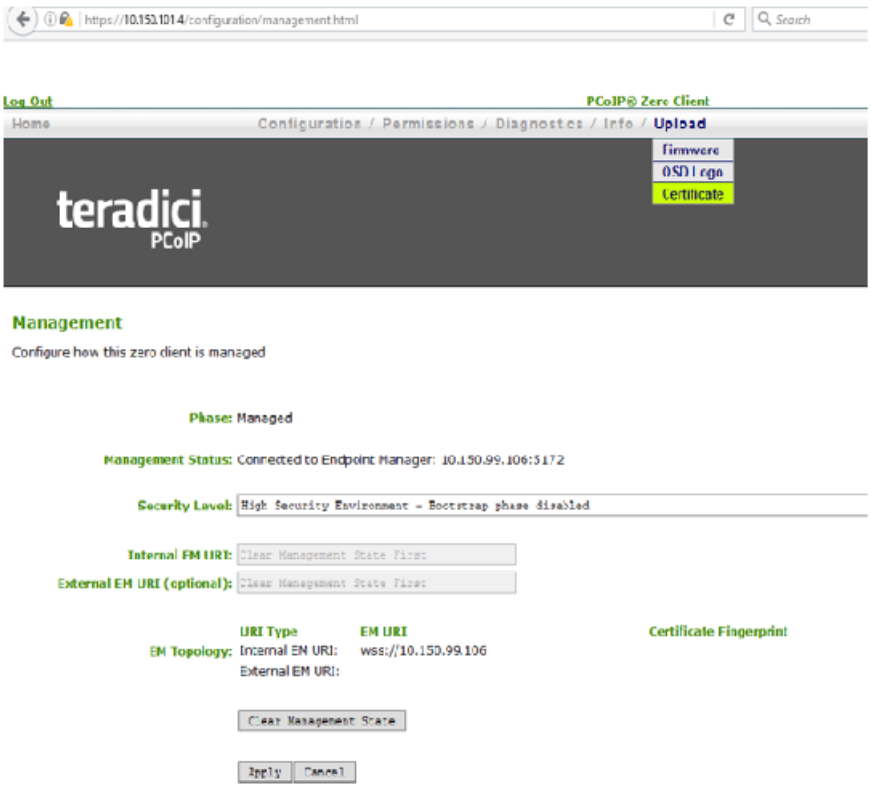


Figure 91. Certificate Configuration Screen

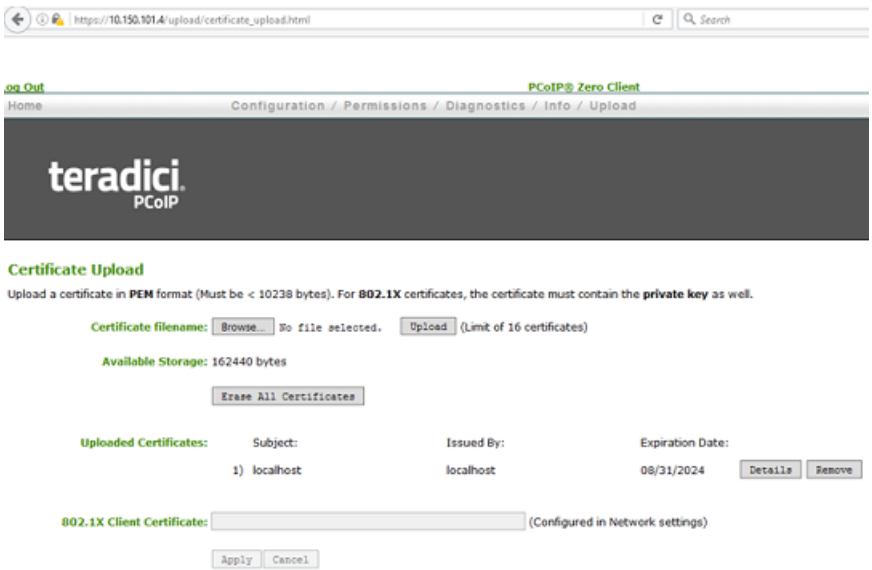


Figure 92. Certificate Upload Screen

2 The successfully uploaded certificate is listed in the Certificates Upload section.

3 In Configuration menu of the ThreadX devices management console, select **Management sub menu** > **Security Level** > **High Security Environment – Bootstrap phase disabled** option.

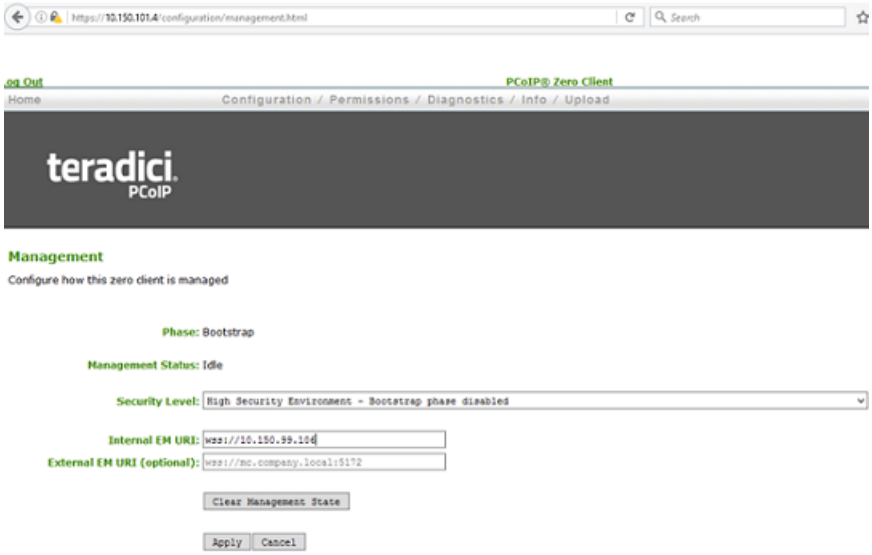


Figure 93. Management Screen

In the **Internal EM URI** field, provide the uri of the EMSDK server as **wss://<IP Address** of ThreadX 5.X installed machine and click **Apply** button.

4 Click **Continue** button to continue the process..

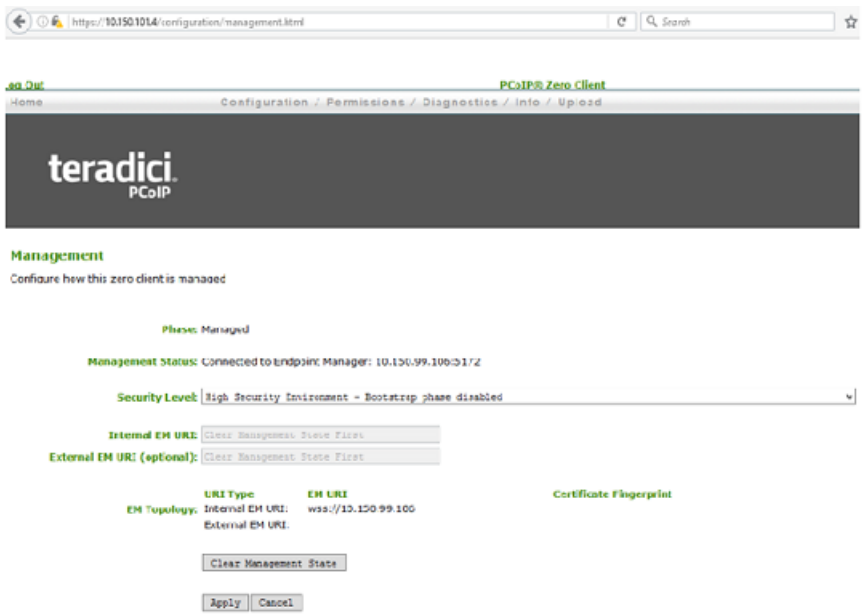


Figure 94. console connected to the EMSDK server Screen

NOTE: Devices are not discovered in the WDM, if clients are connected before the ThreadXApi service is started. So if you can not view devices getting discovered after the clients are in connected state to the EMSDK. you have to see the ThreadXApi service is running byviewing into its log file located at C:\inetpub\wwwroot\ThreadXApiwith filename ThreadXApi.txt

After completing the process of checking into WDM server successfully, you can view the discovered devices in the WDM UI. You should execute the **Reboot**, and **Shutdown** real-time commands after it is visible in the Web UI.