Notes, Cautions, and Warnings

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

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

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

Copyright © 2014 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell™ and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2014 - 04

Rev. A00
# Contents

1 Introduction .................................................................................................................. 9
   Key Features .................................................................................................................. 9
   Key Features of WDM Enterprise Edition ................................................................. 12
   What’s New .................................................................................................................. 13
   Support Information ................................................................................................... 16
   Dell Wyse Technical Support ..................................................................................... 19
   Related Documentation and Services ................................................................. 19
   Dell Wyse Online Community .................................................................................. 19

2 Wyse Device Manager Components ......................................................................... 21
   WDM Console ............................................................................................................ 21
   WDM Database ......................................................................................................... 22
      Desktop Engine or MS SQL Server ........................................................................ 22
      Connecting to the WDM Database ........................................................................ 23
      Importing Data ....................................................................................................... 23
   WDM Repositories .................................................................................................... 23
      Repository Synchronization .................................................................................. 24
   WDM Services .......................................................................................................... 24
   WDM Agents ............................................................................................................. 24

3 Device Manager .......................................................................................................... 25
   Adding Devices ......................................................................................................... 26
      Discovering Devices .............................................................................................. 27
      Manually Adding Devices to the Database ............................................................ 27
   Creating Device Filters............................................................................................. 28
   Device Locator- Find a Device in a View ................................................................. 30
   Deleting Devices from the Database ........................................................................ 30
   Updating Device Properties ...................................................................................... 31
      Updating Basic Device Information ...................................................................... 31
      Updating Network Properties ............................................................................... 32
   Viewing Device Properties ....................................................................................... 33
   Remotely Shadowing Devices .................................................................................. 33
   Pulling and Configuring Image Packages ................................................................... 34
   Imaging Devices ....................................................................................................... 35
      PXE-Based Imaging ............................................................................................... 36
      Non-PXE-Based Imaging ....................................................................................... 40
      Autogenic Imaging ................................................................................................. 53
   Using Advanced View Configuration Options for Delegated Administration .......... 58
4 Package Manager ........................................................................................................... 69
   Using the Package Wizard .......................................................................................... 71
      Registering a Package from a Script File (.RSP) .................................................. 72
      Registering an Image from a Device (Requires PXE) ............................................ 72
      Registering a Configuration from a Device ......................................................... 73
      Building and Registering a CE Image Plus Add-ons (CE Bundled Image) ............ 74
   Deploying an Image Using Merlin ............................................................................. 75
   Deploying a Package Using PAD ............................................................................... 76
   Viewing the Properties of a Registered Package ...................................................... 77
   Viewing and Editing the Package Script of a Registered Package ............................ 77
   Exporting the Package Script of a registered Package .............................................. 78
   Deleting Packages from the WDM Database .................................................................. 79
   Using the WDM Scripting Language ........................................................................ 80

5 Update Manager ........................................................................................................... 81
   Peer Assisted Deployment .......................................................................................... 82
      Pre-requisites for PAD ......................................................................................... 84
      Configuring PAD .................................................................................................. 85
      Viewing PAD Details ............................................................................................. 88
      Editing and Deleting PAD Schedules ................................................................... 90
   Updating Devices .................................................................................................... 91
   Distributing Device Updates through the Package Distribution Wizard .................. 92
   Distributing Device Updates using Recurring Scheduler ......................................... 96
   Editing Recurring Updates ...................................................................................... 98
   Editing Scheduled Device Updates .......................................................................... 100
   Deleting Scheduled Device Updates ....................................................................... 101
   Software Repository Synchronization ......................................................................... 101

6 Report Manager .......................................................................................................... 103
   Creating a Device Listing Report ............................................................................ 104
   Creating a Log Report .............................................................................................. 107
   Creating a Package Distribution Report .................................................................... 110
   Creating a Client Package Report ........................................................................... 111
   Creating an Installed Software Report ..................................................................... 112
7 Configuration Manager ................................................................. 123

Group Types .................................................................................. 124
   Creating Custom Group Types ................................................ 124
   Editing Custom Group Types .................................................. 125

Device Views ................................................................................ 126
   Creating Device Views .............................................................. 127
   Editing a View .......................................................................... 129
   Deleting Device Views ............................................................. 132
   Switching Device Views .......................................................... 132
   Implications on Device Views .................................................. 133

About Default Device Configurations ............................................ 133
   Creating Default Device Configurations ................................... 134
   Managing the Default Device Configuration .............................. 137
   Deleting Default Device Configurations .................................... 138

Profile Manager ............................................................................ 139
   Identifying PM Supported Devices ........................................... 139
   Creating a WCM Configuration Package ................................. 140
   Enabling PM in Preferences ..................................................... 140
   Deploying a Configuration Package Using Profile Manager ........ 141
   Deleting a PM Configuration Package ...................................... 141

Activating WDM Sales Keys .......................................................... 142
Adding and Using Multiple WDM Sales Keys ............................... 142
Upgrading a WDM Workgroup Sales Key to an Enterprise Sales Key 143
Deleting WDM Sales Keys ............................................................. 144

Configuring Preferences .............................................................. 145
   Device Manager Preferences ................................................... 145
   Logging Preferences ............................................................... 148
   Service Preferences ............................................................... 151
   DHCP/TFTP Preferences ......................................................... 154
   Scheduling Preferences .......................................................... 155
   Subnet Preferences ............................................................... 156
   WTOS Preferences ............................................................... 158

Viewing the Installation Details ...................................................... 115
View the Component Details ......................................................... 119
Remote Sessions History Report .................................................. 120
Remote Sessions Summary Report ................................................. 121
Secure Communication (HTTPS) ..................................................................................................................158
Upgrading Older WDM Agents Selectively ....................................................................................................160
Using WDM Device Security .......................................................................................................................160
Registering Remote Repositories ..................................................................................................................161
Software Repositories List ............................................................................................................................165
Assigning Software Repositories to a Subnet ..................................................................................................165
Software Repository Service Preferences .....................................................................................................166
Network Configuration ...................................................................................................................................167
Setting Subnets Manually ...............................................................................................................................167
Setting IP Ranges Manually ............................................................................................................................169
User Management ........................................................................................................................................170
  Adding Users from Local Computer Accounts .............................................................................................171
  Adding Users and Groups from Active Directory ..........................................................................................171
  Editing User Permissions .................................................................................................................................171
  Deleting Users .............................................................................................................................................172
Utilities ............................................................................................................................................................173
  Importing Data ............................................................................................................................................173
  Importing Device Settings from Files ..............................................................................................................178
  Database Credential Manager .......................................................................................................................179
  Management Console Extractor .....................................................................................................................180
  WDM Imaging Tool ....................................................................................................................................180
  High Availability Configuration Utility ........................................................................................................181
  DNS-DHCP Lookup Utility ..............................................................................................................................181
Viewing the Diagnostic Report .......................................................................................................................182
Certificate Authority Expiration Tracker .........................................................................................................182

8 Advanced Administration ..........................................................................................................................185
Changing the WDM Security Certificate ........................................................................................................185
About the WDM Scripting Language ..............................................................................................................186
  WDM Package Structure ................................................................................................................................186
  Optional Arguments and HKEY_CURRENT_USER ..........................................................................................187
  Version .........................................................................................................................................................187
  Script ..........................................................................................................................................................189
Understanding the Script File Structure .........................................................................................................199
  Version .........................................................................................................................................................199
  Image Category Special Tags ........................................................................................................................219
  Script ..........................................................................................................................................................220
  Recommended Scripting Template ................................................................................................................220
Understanding WDM Agent Error Codes ......................................................................................................221
  File Transfer Protocol (FTP) Error Codes ......................................................................................................222
  Windows Sockets Error Codes ......................................................................................................................224
### Troubleshooting

- **WDM Installation Failure** ................................................................. 227
- **Problems with Discovering Devices** .............................................. 227
- **Problems with Discovering PXE Devices** ...................................... 227
- **Package Errors** ............................................................................ 227
- **Setting the Correct Logging Levels** ............................................... 228
  - **Viewing Service Logs** ................................................................. 228
- **Problem With HServer Init Requests** ............................................. 231
- **Wake on LAN Command Does Not Reach Remote Devices** .......... 233
- **Changing the IP Address of the WDM Server** ................................ 233
- **Peer Assisted Deployment Issues** .................................................. 233
- **Profile Manager Issues** ................................................................. 234
- **Tips to Troubleshoot the Repository** .............................................. 235
- **Troubleshooting T50 and WTOS Errors** ........................................ 236
- **Troubleshooting WCM Issues** ....................................................... 238
- **Package Update Fails When CIFS Repository is Enabled** ............... 238
- **PAD Imaging and Drag and Drop Features Not Working on Linux Devices** .................................................. 239
- **Default Device Configuration Does Not Display Exported Images** 239
- **VNC Log Not Generated** ............................................................... 239
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, Windows CE, Linux, Wyse ThinOS, Xenith, P-Class 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. Its intuitive, simple and powerful user interface is built to operate as a standard snap-in to the Microsoft Management Console (MMC). Wyse Device Manager (WDM) includes a simple to use console to manage all of your network devices.

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 in time. WDM can also be configured to automatically provide you with up-to-date status information on all of your devices.

- **Asset Information Collection** - WDM monitors and stores all asset information about each of the devices that includes hardware asset information and information on the software 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, reboot, 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.

- **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 that has all of the software that is needed across an installation and then 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, up to 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.

• **Non-PXE Default Device Configuration** - You can create different configurations that can be deployed to a device using the non-PXE option.

• **Device Configuration Capture** - You can easily capture device configurations to prepare for deployment.

• **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.

• **WDM Scripting Language** - WDM provides you with an advanced scripting language to give you complete control when creating and deploying your own software and image packages.

• **Administrator Console** - The WDM Administrator Console has several easy-to-use features including:
  - **Multiple Panes** - Allows you to quickly view a list of your devices (on the top pane) as well as the details of your devices (on the bottom pane).
  - **Pagination** - Allows you to view sets of your devices, rather than a long list, for faster navigation (especially important when viewing large scale deployments).
  - **Search Utility** - Allows you to search for devices in the current view using a search string or any one of 20 prior searches.
  - **Performance Improvements** - Several enhancements have been included to increase performance (for example, a faster refresh rate of device details shown on the WDM Console).
  - **Display Improvements** - The “About Wyse Device Manager” window now displays the WDM version and build number, as well as the numbers of all installed Hot Fixes. The Administrator Console General Info tab now displays the Write Filter status for XPe devices. The network tab displays all communication information between different components of WDM. In the Administrator Console, Disk Details tab displays detailed information about all the disks in the device. The Device Manager display shows the supported communication protocols for each device and its associated repositories.
  - **Device Filter** - Allows you to view a subset of all the devices in a view that match their desired filtering criteria.
  - **Find Device in View** - Allows you to find out in which View a particular device is located.

• **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).

• **Improved 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.

• **Manually Add WDM Users** - If you do not have domain users or use Active Directory, you can use this feature to easily create a WDM user (especially useful for creating administrators without depending on an external infrastructure).

• **Enhanced Report Support** - Additional reports on device data includes:
  - **Package Distribution Report** - Provides a parameterized report of the status of all devices that have been scheduled for a specific package.
  - **Client Package Report** - Provides a parameterized report summarizing all of the packages that have been deployed to each client/device.
  - **Client Downtime Report** - Provides a parameterized report (based on captured diagnostics) summarizing the time that each client/device has been down.
  - **Package synchronization Report** - Provides a parameterized report summarizing the synchronized packages, not synchronized packages as well as orphaned packages.
  - **Installation Details** - Provides the important information about the installed components of WDM.
  - **Component Details** - Provides the information about all the running components of WDM.
  - **Diagnostic Report** - Provides hardware and software summary information and a list of running processes.
  - **Get and View Device Logs** - Allows you to create a device logs (e.g. OS, Agent and VNC logs) and view them according to the selection criteria.

• **Remote Sessions History Report** —

  Provides the connection information on all devices in WDM based on the filter criteria defined during report generation.

• **Remote Sessions Summary Report** —

  Provides a summary of the remote session connections by all the devices in WDM during a specified time period.

• **Scheduling Preferences** - Customize the scheduling options to meet your requirements. You can enable or disable the Time Bound Rollout in Scheduling Preferences.

• **Time Bound Rollout** - This check box enables and disables the garbage collector feature for scheduled updates. When this field is checked, the settings of the Global Schedule Time-out and the Client Response Time-out will determine whether the scheduled updates enter an error state, or remain in the scheduled state indefinitely.

• **Logging Improvements** - You can receive warnings when log entries exceed a configured threshold, and configure the service log to start or stop during WDM start up.

• **Autogenic Imaging** - WDM will provide the support for the Autogenic Imaging. The purpose of Autogenic Imaging (image backup mechanism scheme) is to image a device with the image residing on the flash or hard drive of the device.
IPv6 dual-stack support - Supports setup of WDM components in IPv4, dual-stack and IPv6 mode, i.e. all components of WDM (server, database, GUI and remote repositories) can run/connect over the selected option. At present none of the WDM platform management agents (hagent) support management over IPv6. Support for running WDM in IPv6 is experimental, and not fully supported. Reboot is required to make this change in effect.

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.

- Merlin, the New Imaging System - Provides HTTP, HTTPS and CIFS based imaging, as well as 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 for the use of 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 speeds up 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 located on your network.

- Default Device Configuration - The Default Device Configuration functionality 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 will revert 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 - Use this feature to automatically place any new device that has been added to the system into the pre-defined groups that you want.

- Support for Multiple Databases - Multiple database support when installing WDM for either an SQL 2005 or 2008 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.

- Autogenic Imaging - Allows you to image the device with the image residing on flash or hard drive of the device.
What’s New

This section describes the new features that are included in WDM version 5.0.

• **New WDM Installer** — WDM now comes packaged in a new installer with enhanced features that include:
  - New look and feel of the installer.
  - Simplified installations for both workgroup and enterprise versions of WDM.
  - License key is pre-populated for the 30 days Enterprise Evaluation and the Workgroup versions.
  - Support for installing services such as the DHCP Proxy, TFTP, and ThreadX.
  - Windows authentication support for WDM Database (Rapport DB).
  - Default installation of secure communication mode (HTTPS) for WDM.
  - Support for CIFS and HTTPS protocols for the software repository during installation.
  - Customized user option for software Repository and WDM Database.
  - Provision of detailed installation logs under the folder you have specified for WDM Installation. For example, C:\ProgramFiles\Wyse\WDM. The files are Detail_WDMInstall and Summary_WDMInstall.
  - The Administrator installing WDM must provide passwords for the WDM database and software repositories. There are no default passwords. The WDM database password is also set for the SQL administrator ‘sa’, which must be used for uninstallation.

For more information, see the *Dell Wyse Device Manager Installation Guide*.

• **High Availability (Clustering) support for the WDM database** — WDM Enterprise edition supports scalability to manage tens of thousands of devices using distributed architecture for WDM server, WDM database and remote software repositories. For higher reliability in managing devices WDM can be configured to use a clustered database setup and load balancing with multiple WDM servers. Devices connect to the virtual WDM server and the load balancer assigns an available, active, WDM server. If a particular WDM server is unavailable, other WDM servers are used to manage the devices.

For more information, see the *Dell Wyse Device Manager Installation Guide*.

• **Load balancing** allows for distributing workloads across multiple resources. In this setup, you can install and run multiple instances of WDM servers on different computers and configure the load balancing feature between them. WDM uses the Microsoft Application Request Routing (ARR) of IIS 7 to perform load balancing, using DNS round-robin selection or other methods, between the available WDM management servers.

For more information, see the *Dell Wyse Device Manager Installation Guide*.

• **CIFS (SMB) Protocol support** — WDM now supports the CIFS/SMB protocol in the software repository. The WDM Agent can now use the CIFS protocol for repository communication along with the existing FTP, HTTP, and HTTPS protocols. You can now use a Windows file server as a CIFS repository. WDM also supports the CIFS/SMB protocol for Merlin Imaging. The WDM Agent now has the following preferences for communicating with the repository:
  - HTTP(s)
  - FTP
– **CIFS**

**Relay Wake On LAN** —

This feature is used to send Wake On LAN (WOL) messages to one or more devices in different subnets. You can now send WOL packets to the devices across subnets.

**Send Message** —

This feature provides the ability to send specified messages to the registered thin clients through WDM.

**Reset OS Settings** —

You can now reset the OS settings for the device to the Factory settings by deploying the `ResetOSSettings` package on Linux and WTOS devices.

**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. 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. For more information, see [Peer Assisted Deployment](#).

**Integration of Dell Wyse Configuration Manager** —

Dell Wyse Configuration Manager (WCM) can now be launched from WDM and you can create and apply configuration files to thin client devices that are managed through the WDM server. This feature requires WCM 1.3.1 client to be installed on the devices. For more information, see the [Dell Wyse Configuration Manager Administrator’s Guide](#) available on the [Dell Wyse Support Site](#).

**Profile Manager** —

Profile Manager enables you to deploy a predefined configuration on a specified group of devices. These configurations are those that you create using WCM and save them in a specified repository. For more information, see [Profile Manager](#).

**Chargeback Accounting** — This feature is supported on Wyse Thin OS (WTOS) devices. It collects and stores remote session information from thin clients. The information is stored only if this feature is enabled in `Configuration Manager → Preferences → Device Manager Preferences`. This feature:

- Displays the remote session information for WTOS in the **Remote Session Asset Information** tab on the WDM Console. For more information, see [WDM Console](#).

⚠️ **Note:** To get the user name and the domain name in the Chargeback Accounting report, you must provide the user name and domain name in the connection manager when you create the RDP and ICA settings. If you do not specify these details, the WDM Agent does not report the user name and domain name and these details are not reflected in the `wnos.ini` file.
Displays the remote session information for ThinOS in the Remote Session Asset Information tab on the WDM Console.

**Supported features for P-class Devices**

- WDM provides a detailed set of features for managing P-class zero clients (P20, P25, P45) for VMware Horizon View environments. In addition to normal management functions WDM Enterprise class features such as automated policy-based management (DDC), administrator delegation, role-based management and others can be used with P-class.
- Automatic discovery (via DNS SRV record _pcoip-tool on port 50000)
- Inventory that includes hardware, software, and network
- Real-time commands (reboot, shutdown, wake-on-LAN)
- Firmware updates
- Asset tags, grouping, and views

**New PCoIP Device Configuration for P-Class Devices** — WDM 5.0 now supports new PCoIP Device configurations. For more information, see Package Manager.

**Utilities** — A complete installation of WDM includes the utilities that can be accessed from Start → All Programs → Wyse Device Manager → Utilities

Some of these utilities are also available under Configuration Manager → Utilities on the WDM Console. The list of utilities are:

- **Configuration Manager** — WCM provides a simple solution to create and apply configuration files to Wyse thin clients running Microsoft Windows Embedded Standard.
- **Database Credential Manager** — This utility enables you to view the details of the WDM database and also create new credentials to access the database.
- **DNS_DHCP_Lookup** — This utility enables you to find out the method that has been configured in the network to discover WDM by the client.
- **Management Console Extractor** — This utility is also known as the Remote GUI Extractor and provides a quick and easy method of deploying the WDM Management Console to remote computers. You can run multiple instances of the WDM Console on different systems at any given point.
- **Script Builder** — This utility enables you to create your own software packages using the WDM Scripting Language.
- **High Availability Configuration Utility** — This 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.
- **WDM Imaging Tool** — This is a mass imaging tool. You can deploy an image to multiple devices in the same platform by using this tool. You can create a schedule to deploy the image to the discovered devices.

For more information, see Utilities.

**Enhanced End-user Notification of Updates**

- The WDM GUI preferences now have an additional option that enables the administrator to set a custom message for a Query User. The options are:
  - 1=Now only
– 2=Delay 5 Minutes only
– 3=Now and Delay 5 Minutes (2 buttons will be displayed)
– 4=Update on Log in only
– 5=Now and Update on Log in
– 6=Delay 5 minutes and Update on Log in
– 7=Now, Delay 5 minutes and Update on Log in (3 buttons will be displayed)
– 8=Custom message with configurable notification and postpone reminder

• **Enhanced Default Device Configuration (DDC)** — This feature prevents the re-imaging of clients if we deploy only BIOS or CMOS.
  
  Now, DDC will consider imaging of BIOS and non-PXE components as packages and not as OS images.

• **Service Logs** —
  
  – **GUI Logs**: Details the activity on the WDM GUI.
  – **Web Services Log** - Details the activity of the WDM Web Services for device management.
    * **TFTP Log** - Details the Trivial File Transfer Protocol activity for distributing software packages to devices.
    * **Standard Services Log** - Details the activity of the WDM Standard Services.
    * **DHCP Log** - Details the activity of the WDM Dynamic Host Configuration Protocol as it assigns IP addresses to devices.

• **File-based Logging for all Services** —

  WDM now supports file-based logging for all WDM Services. These files are located in the WDM Installation folder. For example, C:\ProgramFiles\Wyse\WDM. The files are:
  
  – HServer (main logs for WDM Server)
  – Recurring Scheduler
  – ThreadX (for P-class devices)

• **Enhanced Diagnostic Report** — The Diagnostic Report launched from the WDM Console → Configuration Manager node, now displays the Actual and the Expected versions of the WDM components.

• **Enhanced XML Validation for Merlin Images**
  
  – WDM now supports enhanced validation for correctly constructed XML files that accompany the Merlin images.

### Support Information

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

<table>
<thead>
<tr>
<th>Supported Operating Systems for WDM Server</th>
<th>Windows 2008 R2 SP1 Enterprise Edition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Winodws 2008 SP2 32–bit</td>
</tr>
<tr>
<td></td>
<td>Windows 2012 Enterprise</td>
</tr>
</tbody>
</table>
| Supported Operating Systems for to Upgrade all WDM Components | Windows 2003 R2 SP2 (only for upgrades from WDM 4.9.1)  
Windows 2008 SP2 32-bit (only for upgrades from WDM 4.9.1)  
Windows 2008 R2 SP1 Enterprise |
| Supported Operating Systems for WDM GUI | Windows 2008 R2 SP1 Enterprise  
Windows 2012 Enterprise SP1  
Windows 2012 Enterprise R2  
Windows 7 32-bit SP1 Enterprise  
Windows 7 64-bit SP1 Enterprise |
| Supported Databases | Microsoft SQL Server 2005  
Microsoft SQL Server 2008 Express - English  
Microsoft SQL Server 2008 R2 – English  
Microsoft SQL Server 2008 Enterprise (32 bit)  
Microsoft SQL Server 2012 |
| Supported Thin Client Devices | Wyse Enhanced Microsoft Windows XP Embedded build 587 or later:  
C90LE  
R90L  
R90LE  
V90LE  
Wyse Enhanced Microsoft Windows Embedded Standard 2009 (WES2009) build 641 or later:  
C90LEW  
D90DW  
R90LW  
R90LEW  
V90LEW  
X90CW  
X90MW  
Z90DW  
Z90SW  
Wyse Enhanced Microsoft Windows Embedded Standard 7 (WES7) build 818 or later:  
C90LE7  
D90D7  
D90Q7 |
Wyse Enhanced Microsoft Windows Embedded Standard 7p (WES7p) build 850 or later:
- X90M7p
- Z90D7p
- Z90DE7p
- Z90S7p

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

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

Wyse Enhanced SUSE Linux Enterprise:
- C50LE
- D50D
- R50L
- R50LE
- X50c
- X50m
- Z50D
- Z50S

Wyse Enhanced Ubuntu Linux:
- T50
Dell Wyse Technical Support

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

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

Related Documentation and Services

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

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

Dell Wyse Online Community

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

This section provides information on the core components of Wyse Device Manager software.

Wyse Device Manager software consists of the following components:

- WDM Console
- WDM Database
- WDM Repositories
- WDM Services
- WDM Agents

WDM Console

The WDM Console also referred to as the Administrator Console is the first screen that is displayed when you launch the WDM application. You can view important information on this console and also perform all the device management functions to run and maintain the WDM environment.

**NOTE:** You can install the WDM Console on a separate system if you are installing the WDM Enterprise Edition. For more information, see the Dell Wyse Device Manager Installation Guide.

The WDM Console tree pane contains several functional managers (nodes). Each of these managers performs a specific set of functions that allows you to organize devices, access specific device information, distribute updates to devices, track device update activities, and other configuration functions.

The WDM Console tree pane consists of the following nodes:

- Device Manager
- Package Manager
- Update Manager
- Report Manager
- Configuration Manager

The top pane of the WDM Console contains various task command icons and features, as well as a listing of the items contained in the selected node or folder of the WDM Console tree pane. For example, you can open a folder named Finance in which you have placed a Device View you have created, to display all of the devices in your finance department.

The bottom pane of the WDM Console contains details and task options for the items listed in the top pane of the WDM Console. For example, if you select a device listed in your finance department, the bottom pane provides tabs that contain information on the various details of the device. To view the information you want about the device, click on the appropriate tab. The WDM Console contains the following tabs:
<table>
<thead>
<tr>
<th>Tab Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Info</td>
<td>Displays the name of the device, the operating system installed on it, the MAC Address, the Active IP address of the device, the subnet to which the device belongs, the Write Filter status, and the first check-in and last check-in time.</td>
</tr>
<tr>
<td>Hardware Info</td>
<td>Displays the detailed client hardware information like the CPU speed, RAM size, drivers and BIOS information, and manufacturing date.</td>
</tr>
<tr>
<td>Network Info</td>
<td>Displays the detailed network information for the selected device including the communication details between different components of WDM and the device.</td>
</tr>
<tr>
<td>Application Info</td>
<td>Displays the list of applications installed in the selected device.</td>
</tr>
<tr>
<td>Deployed Package</td>
<td>Displays the details such as Package Name, Description, TimeStamp of Update of all the packages deployed to the device.</td>
</tr>
<tr>
<td>Log History</td>
<td>Displays list of all the logs corresponding to the package deployment in the selected device.</td>
</tr>
<tr>
<td>Custom Info</td>
<td>Displays all the custom information e.g. Location, contact etc. for the selected device.</td>
</tr>
<tr>
<td>Disk Details</td>
<td>Displays list of all the disks including their partition details existing in the selected device.</td>
</tr>
<tr>
<td>Remote Sessions</td>
<td>Displays the details of all the remote sessions such as RDP or Citrix client sessions initiated by the client device.</td>
</tr>
</tbody>
</table>

**NOTE:** The panes also allow you to drag-and-drop items for easy task performance.

## WDM Database

The WDM Database stores all of the information required to manage your devices. This includes information about the devices, packages, distribution schedules, user privileges, and so on.

**NOTE:** Wyse Device Manager Enterprise Edition lets you install the WDM Database separately from the other WDM components.

## Desktop Engine or MS SQL Server

WDM includes a pre-configured SQL 2008 R2 Express so you can begin using the database immediately. However, if you already have an MS-SQL Server instance, you can install (attach) the database to that instance instead of having WDM install SQL 2008 R2 Express.
Connecting to the WDM Database

Connecting to the WDM Database allows WDM to store device information from your network. The Database Server Instance Name dialog box displays the name of the machine where you installed the WDM Database (either SQL Server or SQL Express). If it is not already displayed, enter the computer name and instance name (if any) where the WDM Database is located (do not use a UNC path). For example, Machine_Name\WDMDB is a typical SQL instance name.

Importing Data

With Wyse Device Manager you can import data from comma-delimited and tab-delimited files into the Database. You can use the Import Utility or the Device Import Utility to import data.

Expand the Configuration Manager node in the tree view of the WDM Console and select Utilities → Import to launch the Import Utility. You can use this utility to import:

- IP Range Data. See, Importing IP Range Data from Files.
- Subnet Data. See, Importing Subnet Data from Files.
- Software Repository Data. See, Importing Software Repository Data.

To import device settings from files, expand the Configuration Manager node and select Utilities → Import Device Settings. For more information, see Importing Device Settings from Files.

WDM Repositories

The WDM Repository is a server which supports the FTP, HTTP, HTTPS, and CIFS protocols for communication and contains WDM packages. When you register a package using the Package Manager, WDM copies the related folders and files of the package to the WDM Repository. There are two types of WDM repositories, Master and Remote. By default, each WDM installation has one Master Repository. The Master Repository is the central storage place for all package files.

When you distribute an update, devices connect to the Master Repository through FTP, HTTP, HTTPS, or CIFS (depending on the configuration settings) and download the files that the script file (.rsp file) of the package dictates. Wyse Device Manager and the WDM Agents (formerly known as Rapport Agents) use FTP, HTTP, HTTPS, or CIFS to send and retrieve the appropriate packages from the Master Repository.

In addition, Wyse Device Manager Enterprise Edition allows you to install Remote Repositories on multiple computers on different subnets throughout your network. This scalability reduces network traffic when you need to send updates across subnets. By using their local Remote Repository, devices on a specific subnet do not need to access the Master Repository across a wide-area network (WAN) to retrieve files.

**NOTE:** Wyse Device Manager synchronizes the Master and Remote repositories prior to a package distribution.

If your WDM installation contains Remote Repositories, WDM must establish the relationship between a given set of devices and the Remote Repository that services those devices (thereby ensuring lower network loads). After establishing this relationship, WDM is able to select the appropriate repository when distributing packages to devices. Devices are associated to a Remote Repository by the subnet to which
they belong. After you assign a subnet to a repository, all devices on that subnet will use the assigned repository.

Repository Synchronization

Packages in remote software repositories can be synchronized in two ways:

- **Automatic Synchronization** - occurs when a client device receives an update for a package that is not included in the repository assigned to the client's subnet.
- **Manual Synchronization** - done by the administrator using the WDM Console.

**NOTE:** For details on manual synchronization, see [Software Repository Synchronization](#).

WDM Services

There are two types of WDM services that are used by the WDM server to manage devices, Web and Standard.

The WDM Web Service is both an HTTP and HTTPS command processor and requester. This service relies on push and pull technologies to initiate or respond to requests from devices. Pull technology requires devices that contain the WDM Agent.

A device equipped with the WDM Agent is able to check-in with the Web Service. During check-in, the Web Service can update its database with any new device information and can also distribute updates to the device, if any updates are scheduled.

The ability for devices to initiate communications is especially important for devices that WDM cannot reach through more conventional TCP and UDP mechanisms. Such devices include those that are isolated behind firewalls, proxy servers, or are semi-connected (dial-up and mobile).

**NOTE:** To communicate and manage devices with older versions of WDM Agents (5.0.0.17 and earlier), Web Service routes its requests through the WDM Standard Service component.

The WDM Standard Service allows WDM to provide the following functions:

- **PXE Management** - Executes pre-boot management functions on devices that support the Preboot EXecution Environment (PXE). WDM uses PXE to read and write device images.
- **WDM Agent Upgrades** - Upgrades older versions of WDM Agents to newer versions of the WDM Agent.

WDM Agents

The WDM Agent is a small Web agent that runs within the operating system of the device being managed. It has a very small footprint and is optimized for the thin client environment. The WDM Agent works with the WDM Services on the WDM Server to perform the actions that are needed by you, the administrator. The WDM Agent interprets the commands sent by the WDM Server and makes the necessary changes to the device being managed. In addition, the WDM Agent also provides status updates about the device to the WDM Server.
Device Manager

Device Manager is the first node in the tree view on the WDM Console. When you click the Device Manager node in the tree view, the devices that are discovered or added are displayed on the right-hand pane of the WDM console. When you select a device on the console, the details are displayed in the bottom pane. For more information, see WDM Console.

You can create various device views under the device manager.

You can perform various operations on the Devices from the Device Manager. The operations include:

- Discovering Devices on the network in the same subnet or across subnets. See, Discovering Devices.
- Switching Views. See Switching Device Views.
- Creating device filters. See Creating Device Filter
- Locating a device within a view. See Device Locator - Finding a Device in a View.
- Manually adding devices. See Manually Adding Devices to the Database

You can organize the devices into functional groups and hierarchies. The groups are call the Device Views. If you have created the views, the Device Manager node displays the views when you expand it. When you click on a view you can see the heirarchy for the device. When you select the last node in the hierarchy, the device is displayed on the right-hand pane of the WDM console.

When you select a device on the right-hand pane of the WDM Console, you can perform the following operations:

- Change device information. See Updating Basic Device Information.
- Change network information. See Updating Network Properties.
- Refresh device information.
- Remotely shadow a device. See Remotely Shadowing Devices.
- Get a device image. See Pulling and Configuring Image Packages.
- Execute commands. See Issuing Device Commands.
- Send messages to devices. See Sending Messages to Devices.
- Make the device autogenic capable. See Create Autogenic Device.
- Get logs and view the logs for the device. See Get Logs and View Log.
- Exclude the device from the PAD Repository List. If the device is listed as a Master device in the PAD repository list, clicking this option removes it from the list.
- Include the device in PAD Repository List. If you have excluded the device from the PAD repository list, clicking this option adds it back to the list.
- Shut down the device.
- Reboot the device.
• Use the Wake on LAN feature on devices in the same subnet.
• Use the Relay Wake on LAN feature on devices in different subnets
• Delete a device. See Deleting Devices from the Database.
• Use the package distribution wizard to distribute software packages on the device. See Package Distribution Wizard.
• Use the remote task manager. See Remote Task Manager.
• Export the list of client devices as a .Txt file.

Adding Devices

Adding devices is the process by which WDM becomes aware of the devices in your network, and stores information about them in the WDM Database. After device information is stored in the database, you can use WDM to manage the device.

Devices that have the WDM Agent installed need to be linked to the Web Service so that the devices can check-in regularly. At check-in time, the WDM Agent provides the Web Service with device information such as device name, hardware information (such as platform, flash size, memory, CPU, asset number, serial number), Network Information (such as WINS, DNS, IP address, Domain Name, subnet), Image Number, and so on. There are four ways in which devices can be linked to the server that contains the Web Service:

• Set Up a DHCP Server - (Recommended) Linking is accomplished through DHCP Option Tags 186 and 190 or 192 (for legacy HAgents it is 187) which allow the DHCP server to supply the WDM Agent with the proper WDM Web Server IP address and port.
• Enable DHCP Options for HTTP Discovery - WDM services includes a DHCP Proxy that will respond to DHCP Inform requests from WDM Agents with the Web Server IP address and port.
• Manual Discovery - Initiate discovery from the server to find devices by either Subnet Broadcast or IP Range. WDM Agents will respond to the server discovery by storing the discovering Web Server IP address and port and begin regular check-ins.
• Manual Device Setup - Manually enter the Web Server IP address and port on each device. You can do this through the WDM Control Panel applet on the device (if supported by the device).

You can add devices to WDM either by having WDM discover the devices using Dynamic Discovery or by manually adding devices.

Using Dynamic Discovery, the WDM Agent checks-in periodically with the WDM Web Service. This form of check-in is based on pull communications because the WDM Agent initiates communications.

For more information on using WDM to discover devices, refer to Discovering Devices.

When adding devices manually, you instruct WDM to discover devices on command. This method uses push communications because the WDM Server initiates the operation. When you select this method of adding devices, you can specify whether to add devices through a UDP broadcast or through a TCP connection to every device within a subnet or an IP Range setting.

For more information on manually adding devices to WDM, refer to Manually Adding Devices to the Database.
Discovering Devices

WDM supports Dynamic Discovery, where the devices periodically check-in after you establish the link between the WDM Agent and the WDM Web Service.

To discover devices with the Device Manager:

1. Choose whether to discover all devices in your network or only the new devices.
2. At the dialog box, select whether to discover devices by subnet or IP range.
3. (Optional) To discover devices by IP range, follow these steps:
   - Click the IP Ranges option.
   - From the Network List pane, select either individual IP ranges (use SHIFT or CTRL to select multiple subnets) or all IP ranges by clicking Select All.
     
     **NOTE:** The maximum number of ranges that can be selected at any given time for discovery is 100.

   4. (Optional) To discover devices by subnet, follow these steps:
      - Click the Subnets option.
      - If you enabled the Show Subnet Hierarchy preference (see Subnet Preferences) and you want to select a subnet hierarchy level to find devices, select a subnet hierarchy level from the Network Hierarchy pane. The corresponding broadcast addresses for the subnets in the hierarchy will be displayed on the Network List pane. If you did not enable the Show Subnet Hierarchy preference, continue with the next step.
      - From the Network List pane, select either individual broadcast addresses (use SHIFT or CTRL to select multiple subnets) or all broadcast addresses by clicking Select All.
       
       **NOTE:** The maximum number of subnets that can be selected at any given time for discovery is 100.

5. Click OK

   WDM will begin discovering the devices according to your selections. The results pane will display both the newly discovered devices along with devices that have been discovered previously.

Manually Adding Devices to the Database

You can manually add device to the WDM database if you face technical issues that prevent you from discovery a device in the environment. You can also add devices on which the operating system is corrupt and the device does not operate normally.

To add a device manually:

1. In the WDM Console tree pane, right-click on the the Device node, and select New →Device to open and use the Add a Device dialog box. You can also click on the Manually add a device icon on the WDM Console.

   The Add a Device window is displayed.

2. Enter the following details:
   - **Name** - Machine name of the device that you want to be displayed in the Device Manager.
   - **MAC Address** - Media Access Control (MAC) address of the device, which uniquely identifies the device on the network. Make sure to enter the MAC address accurately to enable communication between the device and WDM.
- **IP Address** - Internet Protocol address of the device. This identifies the device on a TCP/IP network. Network messages are routed to the device based on the IP address.
- **Media Size** - The flash memory size of the device in megabytes. For example, 32, 48, 96, and so on.
- **Operating System** - Operating system installed on the device.
- **Platform** - Hardware platform for the device.
- **Subnet** - The subnet address of the device.
- **Imaging Via PXE** - Select this if the device supports the Preboot Execute Environment (PXE) and can be imaged by WDM.

3. Click **OK** to add the device to the console.

The device is displayed on the right-hand pane of the WDM Console. If you have created a Device View corresponding to any of the device group type characteristics, the device is automatically added into the appropriate Device View.

## Creating Device Filters

To Create a Device Filter:

1. In the WDM Console, select **Device Manager**, select a device on the right hand pane, and right click.
2. Select **Create Device Filter** to launch the **Filter Devices** window. You can also launch this window by clicking **Filter** icon on the tool-bar.
3. The following window is displayed:
Select the column Name from the available Column Name List.

Select the Relation from the Relation List.

Enter the Value for the selected criteria, if applicable.

Click Add button to Add the Filter in the Filter List.

To remove the filter from the Filter List, select the filter and click Undo button.

After adding all the filter criteria, click OK button.

NOTE: You can add maximum up to 5 filter criteria. To make case sensitive filter criteria, check on "Case Sensitive Filter" check box.

All the devices that match the criteria defined in the filter are displayed in the WDM Console against Device Manager.

4. If the Device Manager View is already being filtered, you can edit or remove the filter.

To Edit the Device Filter:

• In the WDM Console, select Device Manager, select a device on the right hand pane, and right click.
• Select Edit Device Filter from the available options or click on the Edit icon on the tool-bar.
• Modify the filter criteria.
• Click Add button to Add the Filter in the Filter List.
• After adding/modifying all the filter criteria, click OK.
• All the devices that match the criteria defined in the filter are displayed in the Device Manager.

5. To Remove the Device Filter -
   • In the WDM Console, select Device Manager, select a device on the right hand pane, and right click.
   • Select Remove Device Filter from the available options or click on the Delete icon to delete the Device Filter.
   • When the Remove Device Filter is selected, the device manager view immediately refreshes to display the unfiltered view.

   NOTE: Switching to a new view in the device manager removes the existing filter.

Device Locator- Find a Device in a View

The purpose of this feature is to provide the user a means of finding as devices correct path in the displayed device manager view. A filter is also provided to limit the listing of the devices.

To find a Device in a view:

1. In the WDM Console tree pane, switch the Device Manager view from All Devices to user created view.
2. In the Device Manager view, right click and select Find Device in View or click on the main toolbar Find Device in View Button.
3. The Find Device in View window will open with all the devices in the view listed and the view path listed next to each device.
4. The list of devices may filtered by entering text into the Search filter textbox.
5. The list of devices may be filtered by any of the device properties listed in the Search Property drop down.

Deleting Devices from the Database

To delete a device from the WDM Database:

1. In the WDM Console tree pane, expand the tree, right-click Device Manager, and select Switch View.
2. Select the Device View that allows you to view the device you want to delete.
3. Right-click the device and select Delete Device.
   The following prompt is displayed:

   ![Confirm WESDX0Q Delete](image)

   Are you sure you want to delete WESDX0Q ?
   Note: Force delete command should only be used to delete a device that is no longer checking-in.

   Yes  No  Force Delete

4. Click Yes to confirm and delete the device. If the device is not checking-in any more to WDM server, click on Force Delete.
NOTE: You can select multiple devices to delete by using CTRL+click or SHIFT+click, right-clicking the selected devices, and selecting Delete Device. If you select multiple devices, you can delete all of them by clicking Yes to All or Force Delete All.

Updating Device Properties

Device Properties consist of basic properties and network properties. You can update the basic properties by using the procedures in Updating Basic Device Information and you can update the network properties by using the procedures in Updating Network Properties.

Updating Basic Device Information

To update basic device information:

1. Switch to the Device View for the device or devices whose information you wish to update.
2. Select the device or devices whose information you want to update, right-click the selection, and then select Change Device Information to open the Change Client Information dialog box.

3. Specify the following details:
   
   - **Computer Name** - Enter a descriptive name for the computer (or range of computers, if you selected multiple devices).
   
   - **Range Starting Value** - If you selected multiple devices, an incremental number will be appended to the name of each device. Enter the starting number for the range of devices.
   
   - **Location** - Enter a descriptive location where the device or devices reside. For example, San Jose headquarters, 2nd floor.
   
   - **Contact** - Enter the name of the person who can serve as a contact for the device or devices in the range.
- **Custom1, Custom2, Custom3** - Enter any additional information that you want to maintain along with the device or group of devices (asset tracking data, a service date, a date of acquisition, or any other information that is useful to you).

4. Depending on whether or not you want to reboot the device or devices automatically after updating the information (devices are updated only after a reboot) select or clear **Reboot Device Immediately** (be aware that if you select to reboot immediately, users will not be notified that the device will be rebooted).

   ☢️ **NOTE:** Write Filter devices ignore this option and will reboot immediately.

5. Click **OK** to open the results pane displaying the newly updated device information after the devices have rebooted and checked-in.

### Updating Network Properties

To update network properties:

1. Switch to the Device View for the device whose network information you wish to update. You can update the network properties for only one device at a time.

2. Select the device or devices whose information you want to update, right-click the selection, and then select **Change Network Information** to open the **Change Device Network Settings** dialog box.

3. Depending on whether or not you want to assign a static IP Address for the selected devices, complete one of the following:
   - If no, select **Obtain an IP Address automatically** and continue with the next step.
   - If yes, select **Use the following IP Address** and complete the boxes in the IP Address section.

   ☢️ **NOTE:** For IP Address section - If you selected multiple devices in step 2, the IP Address you enter will be the starting address for the range of addresses that will include all of the devices you selected. All ranges must fall within a Class C subnet. If a group of devices are assigned a range of IP Addresses that would cross a Class C, WDM issues an error message blocking the operation.

4. Depending on whether or not you want to assign a static DNS Server Address for the selected devices, complete one of the following:
   - If no, select **Obtain DNS Server Address Automatically** and continue with the next step.
   - If yes, select **Use the following DNS Server Addresses** and complete the boxes in the DNS Server Address section.

   ☢️ **NOTE:** CE devices cannot have static DNS Server Addresses if their IP Address is assigned by DHCP.

5. If you want to add a Domain Name as a suffix to the device names for the selected devices, enter the Domain Name in the Domain box (for example, if you were to add as a suffix the Domain Name **DFW1.WyseTechnology.com** to a device named Device1, the result would be: **Device1.DFW1.WyseTechnology.com**).

6. Depending on whether or not you want to assign a static WINS Server Address for the selected devices, complete one of the following:
   - If no, select **Obtain WINS Server Address Automatically** and continue with the next step.
   - If yes, select **Use the following WINS Server Addresses** and complete the boxes in the WINS Server Address section.

   ☢️ **NOTE:** CE devices cannot have static WINS Server Addresses if their IP Address is assigned by DHCP.

7. Depending on whether or not you want to reboot the device or devices automatically after updating the information (devices are updated only after a reboot) select or clear **Reboot Device Immediately** (be aware that if you select to reboot immediately, users will not be notified that the device will be rebooted).
NOTE: Write Filter devices ignore Reboot Device Immediately and will reboot.

8. Click OK.
   The results pane will display the newly updated network information after the devices have rebooted and checked-in.

Viewing Device Properties

Before you can view device properties, you should have discovered devices on your network and have created functional device views.

Use these procedures to view all the information that the Wyse Device Manager Database maintains on any given device, including:

- General information
- Hardware information
- Network information
- Application information
- Deployed software
- Log history
- Custom information
- Disc details
- Remote sessions

For more information, see WDM Console.

To view device properties:

1. Select the Device Manager node in the tree view of the WDM Console.
2. On the right-hand pane, select the device for which you want to view properties, right-click and select Properties to open the Device Properties window.
3. Click the desired tab for the device properties you want to view.

Remotely Shadowing Devices

Viewing and controlling a device remotely (shadowing a device) is useful to help a user with a particular application and to troubleshoot device problems.

NOTE: To enable shadowing, a device must have VNC version 3.3.3.7 or later and the VNC service must be running. If a device does not meet these conditions, you can create an image or package with the necessary files and distribute it to the devices you want to view and control remotely. For more information, see Using the Software Package Wizard to Create and Register Software Packages.

To view and control a device remotely:

1. Switch to the Device View that contains the device that you want to shadow.
2. At the Device Manager results pane, right-click the device you want to shadow and select Remote Shadow.
3. In the results pane, Authentication prompts you for a password.
4. Enter the password you set up earlier for VNC authentication and click OK.
NOTE: Some manufacturers hard-code passwords into their devices, requiring you to contact the manufacturer to get the device password.

The results pane displays the device screen and allows you to run applications and control the device from the WDM Console.

5. To end the shadowing, close the viewer.

Pulling and Configuring Image Packages

PXE is a pre-boot imaging system. It functions within devices that use Intel-enabled PXE BIOS (PXE) for pre-boot environments. To create and register an image that will be deployed as a Default Device Configuration (DDC), you must ensure that the name of the image package is the same as the image version (this version number can be found in the General Info tab of the WDM Administrators Console for the image). This is important because a device uses this image version information to compare the version numbers of the image on the DDC and the device image.

NOTE: When performing a mass distribution of a device image, certain devices will require unique preparation prior to distribution. If required, contact the device manufacturer for detailed information.

To create and register an image package:

1. Expand the Device Manager and select a device.
2. Right-click on the selected device and select Get Device Image to open the Package Wizard.
3. Enter a Name (required) and Description (optional) for the new image package and click Next (the wizard informs you that it is ready to create and register the new package containing the image from the selected device).
   
   NOTE: The new package will remain inactive until WDM successfully retrieves the image from the selected device.

4. If Merlin is selected in Imaging Option of Preferences->Scheduling, the below options will be available to pull the image from the device.
Merlin Image Pulling Options: This option is available only in case of Merlin Imaging.
- **All**: This option provides the flexibility to pull **BIOS**, **CMOS**, **OS** and **Data Partition** (if exists).
- **CMOS and BIOS**: This option provides the flexibility to pull **BIOS** and **CMOS only**.
- **OS (includes Non PXE Partition if present)**: This option provides the flexibility to pull **OS** and **Non-PXE Partition** (if exists) only.
- **Compress Image**: This option when checked, enables the image compression for the pulled image. The whole operation will take much time to compress the image as compare to normal pull operation but the pulled image size will be less than the size of uncompressed pulled image.

Imaging Option: This option is available only in case of WES devices. For rest of the OS this option is not available.
- **PXE**: If PXE is selected then the Non-PXE Partition of the device will not be made active partition.
- **Non-PXE**: If Non-PXE is selected then the Non-PXE Partition of the device will be made as active partition.

5. After the package has been created and registered, click **Finish**. The package is copied to the Master Repository and is displayed under the appropriate category.

**NOTE**: Once this package has been registered WDM starts the image pull operation from the device. The device will go through a PXE boot and the imaging method (either Merlin or WISard, depending on the preferences settings) will create the image and make it available in the Master Repository.

### Imaging Devices

Wyse Device Manager can perform work on devices before the operating system loads on the device. To do this, the device is booted into an environment where it can communicate with the WDM Server to
perform imaging tasks. In order to perform image capture and deployment, scripted installs, registry backups, or execute certain scripts, you must implement a way to boot devices into this environment. There are two ways to image devices:

- **PXE-Based Imaging**
- **Non-PXE-Based Imaging**
- **Autogenic (Melin_ Non-PXE-Based) Imaging**

**PXE-Based Imaging**

Pre-boot Execution Environment (PXE) is an industry standard developed to boot Devices using the network. PXE can boot devices regardless of the disk configuration or operating system installed, and does not require any files or configuration settings on a device. After PXE boot is turned on in the BIOS, a device can communicate with your network PXE Server to receive imaging jobs. PXE provides a number of advantages, and enables you to remotely deploy an image to a device.

**NOTE:** Wyse thin clients come with PXE enabled by default. Nothing must be done on the device for it to perform a network boot.

- **PXE Request Routing**
  
PXE clients use broadcast packets to find DHCP and PXE services on a network to transfer files. These packet types can present challenges when planning a PXE deployment because most default router configurations do not forward broadcast traffic. To resolve this, you must either configure your routers to forward these broadcast packets to the correct server(s), or install a PXE Server on each subnet. Routers generally forward broadcast traffic to specific machines. The source subnet experiences the broadcast, but any forwarded broadcast traffic targets specific machines. Enabling a router to support DHCP is common. If both PXE and DHCP services are located on the same machine, and DHCP packet forwarding is enabled, you should have no problem transferring broadcast packets. If these services are located on different machines, additional configuration might be required. If you are going to forward packets, be sure your router configuration allows DHCP traffic to access the proper ports and IP addresses for both DHCP and PXE servers.

- **Installing and configuring DHCP**
  
DHCP is an integral part of the PXE process, and must be installed and configured in order to use PXE. You must obtain, install, and configure a DHCP Server component separately (a DHCP Server is not provided with WDM). After DHCP is set up and your PXE Servers are installed, you must configure how your PXE Servers will interact with the DHCP Server.

**Deploying an Image Package**

Prior to deploying an image package, complete the following:

1. Register the image package within WDM. The image package can be either a custom image that is provided by Wyse Technology, or an image which has been registered from an existing Reference Device. See **Package Manager**.
2. Enable the image package so that it can be deployed.
3. Ensure that the device to be imaged is part of the WDM system (the device must either be previously discovered or manually added using the WDM Console as described in **Adding Devices**).
4. To register an image in Merlin, see **Register an Image Using Merlin**.

**NOTE:** Merlin supports HTTP and HTTPS protocols for imaging and WISard supports only FTP protocol for imaging.

To image a device you can:
1. **Image a Group of Devices** by using the following guidelines:

   - In the WDM Console tree pane, expand the tree, expand the **Package Manager** until you find the image you need to deploy, and select the image.
   - Drag and drop the image to the group in the Default Device View of the Device Manager on the WDM Console for which this image needs to be deployed (for example, you can open a folder in the Device Manager named *Finance* in which you have placed the Default Device View you have created, to display all of the devices in your finance department). Note that the list of devices will automatically be filtered to include only the devices which have the same operating system as that of the image being deployed.
   - The **Package Distribution Wizard** will appear. Select the devices to which image package needs to be scheduled. If data partition needs to be preserved then check the **Preserve Data Partition(s)** check box.

   ![Package Distribution Wizard](image.png)

   - Click **Next** and Schedule the package for deployment.

2. **Image from the Update Manager** by using the following guidelines:

   - In the WDM Console tree pane, right-click **Update Manager** and select **New | Update** to open the Software Package Wizard.
   - Select the folder that contains the image you want to distribute and click **Next**.
   - Select the image you want to be deployed and click **Next**. Note that the list of devices will automatically be filtered to include only the devices which have the same operating system as that of the image being deployed.
   - Schedule the package for deployment.
About the Imaging process

After you schedule the package for deployment and the device checks in with the WDM Server, the following imaging process occurs:

1. The WDM Server checks if there is an update for the device.
2. If an imaging job is scheduled then the device is notified.
3. The device will then re-boot and go through a network boot process.
4. The WDM Agent will be downloaded to the device and will then contact the WDM Server and get the appropriate image that has been specified from the WDM Repository.
5. The WDM Agent will then apply the image to the flash file system of the device.
6. The device will then re-boot to the new image.

Registering an Image Using Merlin

To register a new Merlin image:

1. Expand the Configuration Manager node in the tree view of the WDM Console.
2. Select Software Repositories and on the right-hand pane select Master.
3. Right click Master and select Properties.
4. Click the HTTP tab for the master repository and specify the details. For more information, see Registering Remote Repositories.
5. Select Preferences under Configuration Manager.
6. On the right-hand pane, double-click Service Preferences.
7. In the Repository Preferences area, select only the HTTP check box. For more information, see Service Preferences.
8. In the left pane of the window, choose Scheduling.
9. In the Imaging Option area at the bottom of the window, select Merlin.
10. In the Imaging Option area at the bottom of the window, select Network Card Speed as per the network speed of the subnet in which the device exists. For more information, see Scheduling Preferences.
11. In the left pane of the window, select DHCP/TFTP.
12. In the TFTP Server Preferences area, click the Start TFTP check box. For more information, see DHCP/TFTP Preferences.
13. In the WDM Console window, navigate to the Package Manager, right click and select New → Package.
   The Package Wizard window appears.
14. Select **Register a Package from a script file (RSP)** and click **Next**.
15. Browse to the location of the image .rsp file (for example, push_9V92_S550_512.rsp) and select **Next**.
16. In the next windows that appear, click **Next** and **Finish**.

The package is now registered and the image is ready to push to the device.

**Recovering Dead Devices**

You can re-image a dead device to recover it.

Use the following guidelines:

- Prepare an image to use by doing one of the following:
  - Obtain the image firmware provided by Wyse Technology and register this image in WDM as described in *Using the Software Package Wizard to Create and Register Software Packages*.
  - Use an existing image which has already be registered from a device in your installation.
- Add a new Device (as described in *Adding Devices*) or select an existing device, and then assign the image you prepared to the device using the Package Manager as described in *Using the Software Package Wizard to Create and Register Software Packages*.
- Schedule the package deployment for the **Next Time Device Boots** (this requires PXE).
- Expand **Update Manager** in the WDM Console tree to find the scheduled device.
- Right-click the scheduled package entry and select **Roll to boot**.
- Power on the dead device to allow the device to be re-imaged.
Non-PXE-Based Imaging

Non-PXE based imaging relies on a Boot Agent that resides in the client device flash memory. The Boot Agent currently supports downloading of Merlin boot floppy only. The Boot Agent communicates with the WDM server to determine whether the target device needs imaging. Since the Boot Agent does not boot via the PXE protocol, it does not receive the WDM server IP address and port number from the WDM proxy DHCP service. In this release, the Boot Agent can discover the WDM server IP address and port number from any one of the following sources (listed in priority order):

- DHCP option tag values received from the standard DHCP server
- WDM server URLs configured from the Boot Agent desktop
- DHCP option tag values received from standard or WDM proxy DHCP service for vendor class “RTIAgent”
- DNS service location record
- DNS host name lookup

Configuring the DHCP Server

Configure the following option tag values on your DHCP server:

- **Option tag 186** - IP address of your WDM server (for example, 192.168.1.10). The value should be in 4 bytes IP address format.
- **Option tag 190** - Secure port number to which WDM server listens (for example, port 443). This value should be in word (value = 0x01bb) or 2-bytes array format (value = 0x01 0xbb).
- **Option tag 192** - Non-secure port number to which WDM server listens (for example, 80). This value should be in byte (value = 0x50), or word (value = 0x0050), or 2-bytes array format (value = 0x00 0x50).

**NOTE:** Some old agents have used option tag 187 for WDM non-secure port number. The value of this option tag, when embedded within vendor class specific information (option 43), was interpreted the same way as option tag 192. i.e. value of 0x0050 was interpreted as 0x0050. New Boot Agent still accepts this option tag value if option tag 192 is not supplied. Option tag 187 is maintained for legacy reason only. It is recommended that DHCP server should use option tag 192 instead of 187.

**NOTE:** Some old agents have used option tag 187 for WDM non-secure port number. The value of this option tag, when embedded within vendor class specific information (option 43), was interpreted the same way as option tag 192. i.e. value of 0x0050 was interpreted as 0x0050. New Boot Agent still accepts this option tag value if option tag 192 is not supplied. Option tag 187 is maintained for legacy reason only. It is recommended that DHCP server should use option tag 192 instead of 187.

**NOTE:** Some old agents have used option tag 187 for WDM non-secure port number. The value of this option tag, when embedded within vendor class specific information (option 43), was interpreted the same way as option tag 192. i.e. value of 0x0050 was interpreted as 0x0050. New Boot Agent still accepts this option tag value if option tag 192 is not supplied. Option tag 187 is maintained for legacy reason only. It is recommended that DHCP server should use option tag 192 instead of 187.

**NOTE:** The WDM server and the DHCP server should not be running on the same machine.

**NOTE:** The WDM server and the DHCP server should not be running on the same machine.

Please consult your DHCP server manual for DHCP option value configuration details.

Follow these steps to configure the WDM server IP address and port option values on a Windows DHCP server:

1. Open the DHCP management wizard, select the DHCP server to be configured, right click he server name, and select **Set Predefined Options**.
2. The **Select Predefined Options and Values** window appears.
3. On the Predefined Options and Values screen, click the Add button. The Option Type window appears.

4. In the Option Type window, enter the required information:
   - Name = WDM Server
   - Code = 186
   - Data Type = IP Address
   - Description (optional) - Enter desired information, or nothing
5. Click OK.
6. Repeat Steps 3 and 4 for the WDM Server port, with these changes:
   • Name = **WDM Server Secure Port**
   • Code = 190
   • Data Type = **Word**
7. Repeat Steps 3 and 4 for the WDM Server port, with these changes:
   • Name = **WDM Server Port**
   • Code = 192
   • Data Type = **Byte** or **Word**
8. Click **OK**.

9. From the DHCP management wizard, select **Scope Options** (from the target DHCP Server Scope, as shown in Figure 54), right click, and select **Configure Options**.
10. In the list of Available Options, check option number 186, and enter the IP address of the WDM server.

11. In the list of Available Options, check option number 190, and enter the port number at which your WDM server listens for secure communication.

12. In the list of Available Options, check option number 192, and enter the port number at which your WDM server listens.

13. Click **OK**.
14. Confirm that options 186, 190 and 192 are listed with proper values under the target DHCP server and scope.

**Configuring Service Location Records in the DNS Server**

On the DNS server, configure a service location record (SRV) with the name `_WDMServer._tcp.`*domain name*`. You can provide one or more WDM server names/ports and corresponding port numbers for this record. If you configure multiple WDM server names, the Boot Agent will access them in order, according to the weight and priority you assign to each entry.

**NOTE:** The DHCP server must provide the proper DNS server and domain name in its offer before the Boot Agent can query the DNS server.

**NOTE:** Please consult your DNS server manual for SRV configuration details.

Follow these steps to configure a WDM server SRV on a Windows DNS server:

1. Open the DNS management window.
2. Select the domain to which the WDM server belongs, right click that domain name, and select **Other New Records** from the context menu.
3. From the **Select a resource record type** list, select **Service Location (SRV)** and click the **Create Record** button.

4. In the **New Resource Record** window, enter the information in the following fields:
   - **Service** = `_WDMService`
   - **Protocol** = `_tcp`
   - **Port Number** = **80** (if HTTPS is used, enter the secure port number, for example, **443**)
   - **Host offering this service** = **FQDN of WDM server**.

5. If desired, you can enter priority and weight values for this WDM server entry. For the priority value, a lower number represents higher priority. To rank entries within the same priority class, you can specify a weight value. For the weight value, a higher number indicates higher priority.

6. Click **OK** when you are finished.
7. Confirm that the WDM server SRV is displayed with proper values under the appropriate domain on the DNS management screen.

**Configuring a WDM Server Host Name in the DNS Server**

On the DNS server, configure a host name record using the name `WDMServer` and including the IP address of the WDM server. Since no port number is provided, the Boot Agent uses HTTP and the default port number 80.

**NOTE:** The DHCP server must provide a proper DNS server and domain name in its offer before the Boot Agent can query the DNS server.

**NOTE:** Please consult your DNS server manual for host name configuration details.

Follow these steps to configure a WDM server host name on a Windows DNS server:

1. Open the DNS management window.
2. Select the domain to which the WDM server belongs, right click that domain, and select **New Host**.
3. In the **New Host** window, enter the required information:

- **Name** = WDMServer
- **Protocol** = WDM Server IP address

4. Click **Add Host**.
5. Confirm that the WDM Server host name is displayed with the proper IP address under the appropriate domain on the DNS management screen.

Deploying an Image Using Merlin

To deploy a new Merlin Image complete the following steps:

1. In the WDM Console window, expand Device Manager to display the list of devices. Drag and drop the Merlin image (for example, `push_9V92_S550_512`) onto the desired device.

2. To verify the Merlin imaging process, check to see that the Boot Agent boots first on the device and then boots the guest OS after contacting the WDM server.

   **NOTE:** If the Boot Agent is not pre-programmed on the device, then the first imaging process will be through PXE using Merlin. After the imaging process is completed on the device, you can pull the image (which has both the Boot Agent and the XPe image) from that device and push it to another device that is pre-programmed with the Boot Agent. To do this, make sure the boot order in the BIOS of the target device is Hard disk.

3. Pull or push the image of the devices which you have already programmed with the Boot Agent image, using Merlin.

   To verify image deployment, observe the following sequence of events:

   1. The device boots up through the Boot Agent.
   2. The device contacts the WDM and downloads Merlin through HTTP.
3. Merlin boots up.
4. Merlin contacts the WDM server and starts the imaging process.

For more information, see [Register an Image Using Merlin](#).

**Autogenic Imaging**

The purpose of Autogenic imaging is to image the device with the image residing on flash or hard drive of the device. This process/scheme requires performing few steps, prior to the actual imaging as mentioned below:

1. Prepare an image to create an Autogenic Capable image. See [Preparing an Image to make an Autogenic Capable Image](#).
2. Register the prepared image in WDM. See [Register an Image Using Merlin](#).
3. Make the image Autogenic Capable. See [Making an Autogenic Capable Image](#).
4. Make an Autogenic Capable device. See [Creating an Autogenic Device](#).
5. Schedule an Autogenic Capable Image to an Autogenic Capable Device. See [Using Advanced View Configuration Options for Delegated Administration](#).

**Preparing an Image to make an Autogenic Capable Image**

To make an image an autogenic capable image-

1. Determine if the image can be converted. Images that are not Merlin or do not support Non-PXE imaging will need to be converted.
2. Start the Merlin Image Converter Utility by clicking on the executable file `ConverterUtility.exe`. This file is found in `{Install Drive}\Program Files\Wyse\WDM\Utilities`. Make sure the files `vmlinuz` and `initrd.pxe` are also present in this directory.
3. Type in, or, using the **Browse** button, navigate to the full path and name of the ".rsp" file for the image and enter it into the "Input .rsp Path" textbox.
   
   **NOTE**: Only non-PXE Merlin image can be made as Autogenic Capable image. So before registering an image in WDM to perform Autogenic Imaging, make sure that you have registered a non-PXE Merlin image (the package should not contain i2d file).
4. When the converted image is registered in the WDM, the status of the image displays **Yes** in the Autogenic column on the WDM console.

**Register the prepared Image in WDM**

To register the prepared image in WDM, perform the same steps as to register a normal package in WDM. After registering the image in WDM, make sure that image type is "Merlin" in Package Manager View.

**Making an Autogenic Capable Image**

To make an Autogenic Capable Image:

1. In the Images Folder of the Package Manager, select the image you wish to make autogenic, and right click to display the context menu.
2. From all the available options, select **Autogenic Capable** if that menu option is visible.

   **NOTE**: The Autogenic Capable menu item will only be displayed if the selected image is a Merlin image, running the XPe, or Windows Embedded Standard, or Windows 7 operating systems and is not already an autogenic image. The WDM edition must also be Enterprise.

3. The image will be Made Autogenic Capable. To confirm this click the **Refresh Button** on the toolbar or press **F5**.
4. To confirm that the image is Autogenic, make sure that the value of **Autogenic** column is **Yes** corresponding to the specific image.

**Creating an Autogenic Device**

To launch a wizard for changing a non autogenic device into one that supports autogenic imaging:

1. Select one or more devices in the right pane of the **Device Manager** and right click to display the context menu.
2. From all the available options, select **Autogenic Capable** option if that menu option is visible.
   
   **NOTE**: The Autogenic Capable menu item will only be displayed when all selected devices are Windows XP or WES, NON-PXE Capable, and have the same flash size.

3. The following window is displayed:

   ![Autogenic Device Creation](image)

   **Figure 1. Autogenic Device Creation**

   - The **Autogenic Device Creation Form** will display containing all autogenic images appropriate for the selected device(s).
   - The **Search Criteria** textbox and **Field(s)** listbox can be used to create a filter that may be used to narrow down the selection of available images. Only images that have a name and/or description that contains the text entered into the criteria box will be displayed. If no text is entered in the Search Criteria textbox, then all appropriate images will appear in the list.
   - The four **Disk Layout** values are prepopulated with the following values whenever an image is selected.
     - **Total Flash Size** - This is simply the total size in MB of the Flash on the selected devices(s).
     - **Non - PXE Size** - This is always 16 MB.
     - **OS Partition Size** - This is dependant on the Backup Partition Size. This is set to be ("total flash size" - "Non - PXE size" - "Backup Partition Size") for devices with flash size of 4096 or less, and to ("4096" - "Non - PXE size" - "Backup Partition Size") for devices with flash greater than 4096 MB.
     - **Backup Partition Size** - Initially this is set to be 100 MB plus that of the selected image. If the total flash size for the device(s) is greater than 4096 MB, this value can not be changed.
However, if the total flash size is not greater than 4096 MB, it may be increased by the user up to any value that still provides room for the OS partition.

4. After choosing the Backup Partition size (if possible or desired), click the Next button. This will bring up additional package distribution wizard forms that are used for scheduling options.

5. For more details on package distribution wizard, see Package Distribution Wizard.

**NOTE:** The Autogenic Imaging is only available with WDM Enterprise Edition.

**Scheduling an Autogenic Capable Image to Autogenic Capable Device**

To schedule an Autogenic Capable Image to an Autogenic Capable Device-

1. Drag and drop the Autogenic Image to the Device Manager. It will list out all the devices that are fulfilling the criteria for the scheduled autogenic image.

2. Select the device from the list of devices to which autogenic image needs to be scheduled.

3. **Case 1:**
   - Check the check box "Download image to backup partition" to download the image to the backup partition of the Autogenic Device and then click "Next" button.
   - The "Package Distribution Wizard" window will appear. Click on "Next" button with default values.
   - Select "PXE" or "Non-PXE" option based on the device configuration and then select "Next".
   - Click on "Finish" button to schedule the image package to the device.

**Package Distribution Wizard**

Please select the device(s) to which you want to distribute the selected package. Click the 'Select All' button to choose all devices in the list.

- [ ] Download image to backup partition
- [ ] Image device from backup partition

Search Criteria

<table>
<thead>
<tr>
<th>Field(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Columns</td>
</tr>
</tbody>
</table>

Selected Devices

<table>
<thead>
<tr>
<th>Name</th>
<th>Active IP Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>PXE00806485...</td>
<td>00806485EBD4</td>
<td>192.168.1</td>
</tr>
</tbody>
</table>

Select All

< Back   Next >   Cancel
• The image download in the backup partition will be scheduled to the device.
• The scheduled image package will appear on Update Manager view.
• After finishing the imaging task, the backup image will reside on the backup partition of the device.

NOTE: The image download will happen in background at the device end. The device will only receive the QU to schedule the imaging task and then rest of the process will be in background.

• After finishing the imaging task, the backup image will reside on the backup partition of the device.
• After that update the HAgent to version 5.1.1.32 on the device to support autogenic imaging.
• After updating the HAgent, on the Device Manager View-> Network Info tab, the details of backup partition will appear.
• After downloading the image to backup partition of the device, schedule an imaging task (with autogenic image) to the device having image in backup partition.

• Check the check box "Image device from backup partition" to image the device from the backup partition of the autogenic device and then click "Next" button.
• The "Package Distribution Wizard" window will appear. Click on "Next" button with default values.
• Select "Non-PXE" option based on the device configuration and then select "Next".
• Click on "Finish" button to schedule the image package to the device.
• The scheduled image package will appear on Update Manager view.
 NOTE: Before scheduling the image task, change the device boot order settings to boot from disk first instead of boot from network.

- The Merlin Imaging Agent will come up to start imaging from the backup partition.
- After imaging is done, again update the HAgent to version 5.1.1.32 on the device to verify the image version on the device and the backup partition details.

4. Case 2:

- Check both the check boxes “Download image to backup partition” and “Image device from backup partition” to download the image to the backup partition of the autogenic device and then to image the device from the backup partition. Click the “Next” button.

   ![Package Distribution Wizard](image)

   - The “Package Distribution Wizard” window will appear. Click on “Next” button with default values.
   - Select “PXE” or “Non-PXE” option based on the device configuration and then select “Next”.
   - Click on “Finish” button to schedule the image package to the device.
   - The image will be downloaded to the backup partition of the device and then the device will get imaged from the backup image residing on the backup partition.
   - After imaging is done, again update the HAgent to version 5.1.1.32 on the device to verify the image version on the device and the backup partition details.
Using Advanced View Configuration Options for Delegated Administration

WDM allows you to delegate administration across multiple administrators. The Advanced Configuration option allows you to filter the devices based on authorization. Thus each administrator controls only the devices that they are authorized to manage.

For example, a company that has multiple offices in two states can delegate the control of the devices in each state to the local administrators responsible for managing the devices in those offices.

To delegate administration across multiple administrators use the following guidelines:

1. Create a Device View as described in Creating Device Views.
2. Assign the Device View to the different administrators you want.
3. Add filters on the Device View to allow each administrator access to their authorized devices only.

Issuing Device Commands

To issue Device Commands:

1. Switch to the Device View that contains the device where you want to issue commands.
2. At the Device Manager results pane, right-click the desired device to open the menu.
3. Select the command you want to issue (the type of device, manufacturer, and OS determines what commands are available; Copy, Delete, and Refresh are part of the MMC and are not a part of WDM Quick Device Commands).

   - **Change Device Information** - Lets you change basic device information (name, location, contact, and three custom boxes) for a given device or group of devices (see Updating Basic Device Information).
   - **Change Network Information** - Lets you change basic network information (IP Address, subnet, and so on) for a given device or group of devices (see Updating Network Properties).
   - **Device Configuration** - This command is applicable only to CE and Linux devices. It allows you to pull the reference configuration from a device so that it can be cloned across the installation. This command will launch the creation process of a configuration package (see Register a Configuration from a Device).
   - **Refresh Device Information** - Causes the WDM Agent on a device, or group of devices, to check-in with WDM Web Service to report on its basic information.
   - **Remote Shadow** - Lets you remotely view and control a device using VNC (see Remotely Shadowing Devices).
   - **Get Device Image** - Reads an entire image. For more information on Get Device Image, refer to Using the Software Package Wizard to Create and Register Software Packages.
   - **Execute Command** - Invokes a command line where you can type executable commands for a given device (if the executable is not in the path of the device, you must provide a fully qualified path).
   - **Create Device Filter** - Creates a device filter to filter out the devices in Device Manager View based on the criteria specified (see Creating Device Filter).
   - **Find Device in View** - Allows you to find out in which View a particular device is located (see Device Locator - Finding a Device in a View).
   - **Autogenic Capable** - Makes a device to get imaged from image on backup partition residing in the device (see Create Autogenic Device).
   - **Get and View Device Logs** - Allows you to create a device logs (e.g. OS, Agent and VNC logs) and view them according to the selection criteria (see Get Logs and View Log).
• **Send Message** - Allows you to send messages to a device. See [Sending Messages to Devices](#).
• **ShutDown** - Lets you shut down a device or group of devices.
• **Reboot** - Reboots the device or group of devices.
• **Wake On LAN** - Enables you to wake a device, or group of devices within the same subnet.
• **Relay Wake on LAN** — Enables you to send a Wake on LAN message to devices across subnets.
• **Delete** - Lets you delete the selected device, or group of selected devices (see [Deleting Devices from the Database](#)).
• **Package Distribution** - Lets you to schedule a package to a device, or group of selected devices (an easy way to invoke the package distribution wizard).
• **Remote Task Manager** - Launches the task manager of the selected device (see [Remote Task Manager](#)).

4. To track real time commands, go to **Update Manager** -> **Real Time Commands**. On the right pane all the scheduled real time commands will be displayed.

## Sending Messages to Devices

As an Administrator, you can send messages to devices. The messages could be specific instructions or informational that you want to broadcast over the network. You can select multiple devices and send messages to them.

To send messages to devices:

1. Select the **Device Manager** node in the tree view of the WDM Console. The devices are displayed on the right-hand pane.
2. Select one or more devices, right-click and select the **Send Message**. The **Send Message** window is displayed.

![Send Message Window](default_image_url)

3. Select the message type from the drop-down. Choose from one of the following options:
   - Information — if it is an information that you want to broadcast.
   - Critical — if it is a critical message related to the device.
   - Warning — if it is a warning related to the device.
4. Enter a message title.
5. Type the message in the **Message** space provided.
6. Click OK.
The message is broadcast to the device or devices and is displayed on the device screen.

Enter an example that illustrates the current task (optional).
Enter the tasks the user should do after finishing this task (optional).

Getting and Viewing Logs

To Get and View OS, HAgent and VNC logs for any selected device:

1. In the WDM Console tree pane, select any device in the Device Manager.
2. Right click to bring up the context menu and select Get Logs.
3. The following window will appear:

   ![Create Log File window]

   - In Create Log File window provide the name of the log file or pick the default file name.
   - Select OS, HAgent and/or VNC as per requirement.
   - Now click on OK button to generate the log file.
   - Depending on the selection, it will generate the log file containing the appropriated logs from the selected device.

4. To view the logs, right click to bring up the context menu and select View Log.
5. The View Logs window is displayed:
In View Logs window, select the log type to see the specific log for OS, HAgent or VNC.

Now click on View Log button to view the logs in the bottom of the window.

To delete any specific log file, select the log file and then click on Delete Log button.

It will delete the selected log file.

Package Distribution Wizard

To launch the Package Distribution Wizard from the Device Manager:

1. Select one or more devices in the right pane of the Device Manager and right click to display the context menu.
2. From all the available options, select “Package Distribution Wizard...” if that menu option is visible.

   NOTE: The package Distribution Wizard menu item is only displayed when all the selected devices share the same operating system.

3. The following window is displayed:

   ![Package Distribution Wizard](image)

   This Wizard will guide you through the process of distributing a package to one or more devices. To begin, please select the category containing the package you wish to distribute.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Update</td>
<td>Agent Update</td>
</tr>
<tr>
<td>Device Configuration</td>
<td>Device Configuration</td>
</tr>
<tr>
<td>Images</td>
<td>Images</td>
</tr>
<tr>
<td>Other Packages</td>
<td>Other Packages</td>
</tr>
<tr>
<td>PColP Device config.</td>
<td>PColP Device configuration</td>
</tr>
</tbody>
</table>

Select a Package Category and click the Next button.

4. Follow the steps given in Distributing Device Updates.

**Remote Task Manager**

To View Applications, Processes, and Performance in a task manager window for any selected device:

1. In the WDM Console tree pane, select any single device in the Device Manager.
2. Right click to bring up the context menu and select Remote Task Manager menu. The following window is displayed:
The window displays the Applications tab by default and displays the list of applications on the selected device.

- The name of the device is displayed in the title bar of the Remote Task Manger.
- The MAC Address and IP Address are displayed in the window’s Status Bar.
- Selecting the Processes Tab displays the running processes for the selected device.
Selecting the **Performance Tab** displays memory, page file, virtual memory, and CPU usage information for the selected device.
Add/Remove Columns in Device Manager

On the right pane of the Device Manager view, the user can configure the list of columns he/she would like to display. Using this you can customize the Device Manager view as per your requirements.

To customize the Device Manager View:

1. At the Device Manager results pane, right-click and navigate to View then select Add/Remove Columns....
2. The Add/Remove Columns window is displayed.
3. It will display the list of Available Columns on the left and list of Displayed columns on the right.
4. You can move the fields from **Available columns** to **Displayed columns** depending on the requirements.
5. Click **OK** to confirm the changes you have made.
6. Verify the changes you have made in right pane of the Device Manager View.

**PCoIP Device Configuration**

You can configure PCoIP devices in your environment through the PCoIP Device Configuration.

To change the PCoIP device settings:

1. Switch to the Device View for the device or devices whose information you wish to update.
2. Select the PCoIP device or devices whose information you want to update, right-click the selection, and then select **PCoIP Device Settings** to open the **PCoIP Device Configuration** dialog box.
3. The **Basic** tab is displayed. Configure the following details:

**Label (Device Information)**

- **Label**: Provide the device name, description, and generic tag and click **Apply**.

  **NOTE**: If you select multiple devices, the Label settings are disabled.

**Time Zone Configuration**

- **Identify NTP Host by**:
  - **IP Address**
  - **FQDN**

- **NTP Server**:
  - **Port**: Enter the port number, default is 0.
  - **Query Interval**: Enter the query interval in minutes, default is 0.
  - **Enable Daylight Saving Time**: Select if needed.

- **Time Zone**:
  - Select the time zone.

- **VMware Horizon View - Connection Server Settings**

  - **Identify Server by**:
    - **IP Address**
    - **FQDN**

- **Connection Server**:
  - **Port**: Enter the port number, default is 80.
  - **Use secure connection (SSL)**
  - **Always connect to this server at startup**
  - **Auto launch if only one desktop**
Time, if it is applicable to the time zone you are selecting.

• Select the time zone from the drop-down list.

**Video**

Provide the minimum and maximum image quality details and click **Apply**.

**RDP**

Provide the RDP connection details and click **Apply**.

**Language for the Local GUI**

Provide the local language and keyboard details for the localized GUI and click **Apply**.

**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.

4. **Click the Advanced tab to configure the following details:**

**Enable Advanced Configuration**

Select the options if you want to enable the web interface of the device, the Wake-on-LAN feature, Power on after Power Loss feature, and User Name Caching feature.

**Device Administrator Password**

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

**USB Permissions**

Provide the USB permission details for the device.

5. You can choose to apply a single configuration set or apply the entire configuration at a time by clicking **Apply All Settings**.

6. You can also apply these configuration settings to multiple devices at a time.
Package Manager

Package Manager is the second node in the tree view of the WDM Console.

The Package Manager allows you to:

- Register packages to the WDM Master Repository. The packages can come from:
  - Package files
  - Images and/or configurations that you create (get) from devices in your network (to distribute it to other devices)
  - Pre-registered WDM Agent upgrades that are installed
- Organize the packages into functional categories
- Distribute packages to selected devices (immediately or on a scheduled basis)

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

- **Agent Update**
  - **SUSELXHAgentUpgrade** - This package can be scheduled only to the devices running SUSE Linux OS and are running HAgent Version less than the HAgent Version available in WDM.
  - **UbuntuHAgent Upgrade** - This package can be scheduled only to the devices running the Wyse Enhanced Ubuntu Linux OS and are running HAgent less than the HAgent Version available in WDM.
  - **WE8SHAgentUpgrade** - This package can be scheduled only to the devices running the Windows Embedded 8 Standard 64 bit OS and are running HAgent less than the HAgent Version available in WDM.
  - **WE8SxHAgentUpgrade** - This package can be scheduled only to the devices running the Windows Embedded 8 Standard 32 bit OS and are running HAgent less than the HAgent Version available in WDM.
  - **WES7HAgentUpgrade** - This package can be scheduled only to the devices running WES7 OS and are running HAgent Version less than the HAgent Version available in WDM.
  - **WES7PHAgentUpgrade** - This package can be scheduled only to the devices running WES7P OS and are running HAgent Version less than the HAgent Version available in WDM.
  - **WESHAgentUpgrade** - This package can be scheduled only to the devices running WES OS and are running HAgent Version less than the HAgent Version available in WDM.
  - **XPHAgentW** - This package can be scheduled only to the devices running XPe OS and are running HAgent Version less than the HAgent Version available in WDM.

When these updates are scheduled to a device, they upgrade the HAgent of the device.

- **Device Configuration** — You can create packages using the Dell Wyse Configuration Manager (WCM).
  a. To launch WCM, right click **Device Configuration** and select **New → Configuration**.
b. Create the device configurations using the WCM Application GUI 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.

You can then deploy these packages to the devices using the Device Configuration Manager, the Package Distribution Wizard, or just by dragging and dropping the package on the device listed under Device Manager.

For more information, see Distributing Device Updates, and Device Configuration Manager.

• Images
  – BootAgentUpgradeWES - This package can be scheduled only to the devices that are having Boot Agent embed with the image and the Boot Agent Version is less than the Boot Agent Version available in WDM. When scheduled to a device, it upgrades the Boot Agent of the device.
  – BootAgentUpgradeXPe - This package can be scheduled only to the devices that are having Boot Agent embed with the image and the Boot Agent Version is less than the Boot Agent Version available in WDM. When scheduled to a device, it upgrades the Boot Agent of the device.

• Other Packages
  – BootAgentUpgradeLinux- To upgrade the boot agent for a device running the SUSE Linux Enterprise 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.
  – 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.

• 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.

**NOTE:** You can also edit the script part of the .rsp file corresponding to a custom package. With this option you can change the rsp file of a registered package without deleting and re-registering the package in Package Manager.

**Using the Package Wizard**

You can use the package wizard to create and register software packages. To create and register packages:

1. On the WDM Console, select the **Package Manager** node, right-click on it and select **New → Package**.
   The **Package Wizard** is displayed.

2. Select the option for the task you want to accomplish.
3. Click **Next** and complete the wizard using the procedures from one of the following options (that you selected):
   - Register a Package from a Script File (.RSP)
   - Register an Image from a Device (Requires PXE)
   - Register a Configuration from a Device
   - Build and register a CE image plus add-ons ("CE bundled image")

   ![Package Wizard](image.png)
Registering a Package from a Script File (.RSP)

To register an existing software package:

1. In the File Path box, enter (or browse to select) the path to the WDM script file (.rsp) file for the package you want to register and click Next to open the Software Package Information dialog box.

2. Use the following guidelines:
   For Non-imaging, General-purpose Applications, Settings, CE Bundled Images, and so on:
   - If necessary, change the package Name, Description, and Category.
   - Depending on whether or not you want to have the package distributed, select or clear Active.
   - Click Next.
   - The wizard notifies you that it is ready to register the package.
   - Click Next to start creating the package.
   - After the package has been created and registered, click Finished. The package is copied to the Master Repository and is displayed under the appropriate category.

Registering an Image from a Device (Requires PXE)

This function requires that an Imaging Scripting Template must exist for the Device Type. If no Imaging Scripting Template is available, a Warning message will display (contact the manufacturer of the device to obtain an Imaging Scripting Template).

To register an image from a device:
1. Enter a Name and Description for the Read Image package, which will read the image from a desired device, and click **Next** (when you create the Read Image package, ensure that the .rsp file contains values for the imagesize parameter and for the image number of the device upon which the image is based; proper .rsp files will have a well-formed header).

2. The wizard prompts you to select the group from which to read the image. Select the group where the source device is found and click **Next**.

3. The wizard prompts you to select the desired device (be sure to select a device that supports the Pre-boot EXecute Environment (PXE)). Select the device whose image you want to read with the Get package and click **Next**.

4. The wizard prompts you for the Name and Description of the Write Image package, which you will use to distribute the image you obtain with the Read Image package. Enter a Name and Description for the Write Image package which will write the image to the desired devices, and click **Next**.

5. The wizard informs you that it is ready to create and register the Get/Set packages.

6. Click **Next** to start creating the package.

7. After the package has been created and registered, click **Finish**. The package is copied to the Master Repository and is displayed under the appropriate category.

### Registering a Configuration from a Device

Pulling a configuration from a device is an important function which can be used to clone a Reference Device configuration across the installation.

**NOTE:** This function is only applicable to Wyse® Winterm™ 3 series Thin Clients using the Windows CE operating system and Wyse 5 series Thin Clients using the Wyse Linux embedded operating system.

1. Prior to registering a configuration you must:
   - Identify a Reference Device.
   - Configure the Reference Device to fulfill your specifications.
   - Test the Reference Device and resolve any issues you may find.
   - Ensure that the Reference Device supports the Pre-boot EXecute Environment (PXE).

2. Once you have completed these steps you must then complete the following steps which will pull and register the configuration from the device:
   - Right click on the Reference Device and select **Get Device Configuration**.
   - Enter a Name and Description for the Configuration package (the new package will remain inactive until WDM successfully retrieves the configuration from the selected device).
   - Click **Next**.
   - Click **Next**.
   - After the package has been created and registered, click **Finish**. The package is now ready for deployment (see **Distributing Device Updates**).

3. **Registering a CE Device Configuration**

   With a CE device, you have high granular control over the configuration information that can be pulled from the device. To register a CE device configuration:
   - Right click on the Reference Device and select **Get Device Configuration**.
   - Enter a Name and Description for the Configuration package (the new package will remain inactive until WDM successfully retrieves the configuration from the selected device).
   - Click **Next**.
4. The entire configuration can either be replaced or appended to an existing device configuration when this package is distributed. Use the following guidelines:

- **Replace** - Replacing the Registry resets the Registry to factory defaults and then applies the Registry Settings contained in the configuration (settings.reg) file of the configuration package. These Registry Settings were configured when you set up the test CE device in Step 1.

- **Append** - Appending the Registry applies Registry Settings from the configuration (settings.reg) file on both of the existing Registry Settings. Duplicate Registry Settings are not affected.

- You can also exclude a specific configuration setting to pull by selecting it in the list (by selecting the check box next to the configuration setting you are excluding that configuration setting). Each of the configuration settings is grouped in logical order.

5. Click **Next**.

6. Click **Next**.

7. After the package has been created and registered, click **Finish**. The package is now ready for deployment (see Distributing Device Updates).

**Building and Registering a CE Image Plus Add-ons (CE Bundled Image)**

To build and register a CE image plus Add-ons package:

1. Enter a Name and Description for the CE bundled image and click **Next**.
   
2. Depending on whether or not you want to have the package distributed, select or clear **Active**.
   
3. Click **Next**.

4. The wizard prompts you for the CE version number and base image for the CE bundled image. Enter the CE version number and base image for the CE bundled image.
5. Browse and select the location of the Base CE Image and, optionally, for the location of the Registry Image in the CE Base box, and click **Next**.

   **NOTE:** The CE Base image (or Primer) is generally a binary or executable file, most often the CE operating system.

   The CE bundled image creation process requires a params.ini file. This file should reside in the same directory from which you obtain the CE base image. The wizard gets the build version information from the params.ini file. If the file is not available, the CE bundled image creation process will stop.

6. The wizard prompts you to select Add-ons for the CE bundled image. Click **Select File** to navigate and select the location where known Add-ons reside and select the Add-on (or Add-ons) you want.

   **NOTE:** The Add-on is generally a binary, executable, or registry file.

   The CE bundled image creation process requires a params.ini file for each Add-on that you select. This file should reside in the same directory from which you obtain the Add-on. The wizard gets the Add-on’s build version information from the params.ini file. If the file is not available, the CE bundled image creation process will stop.

   The Add-on and Build boxes display the name and build, respectively, for each Add-on (or Add-ons) you want.

   The Add-On selection dialog will display your chosen Add-ons and allow you to continue making additional Add-on selections.

7. When you have finished selecting the Add-ons you want, click **Next**.

   **NOTE:** To delete Add-ons, simply select them (use SHIFT or CTRL for multiple selections) and click **Remove** (click **Remove All** to delete all Add-ons).

   A window displays the steps related to bundling the Add-ons to the CE image. The wizard informs you that it is ready to create the package for your CE Bundled image.

8. Click **Next** to start creating the package.

9. After the package has been created and registered, click **Finish**. The package is copied to the Master Repository and is displayed under the appropriate category.

### Deploying an Image Using Merlin

To deploy a new Merlin Image complete the following steps:

1. In the WDM Console window, expand Device Manager to display the list of devices. Drag and drop the Merlin image (for example, push_9V92_S550_512) onto the desired device.

2. To verify the Merlin imaging process, check to see that the Boot Agent boots first on the device and then boots the guest OS after contacting the WDM server.

   **NOTE:** If the Boot Agent is not pre-programmed on the device, then the first imaging process will be through PXE using Merlin. After the imaging process is completed on the device, you can pull the image (which has both the Boot Agent and the XPe image) from that device and push it to another device that is pre-programmed with the Boot Agent. To do this, make sure the boot order in the BIOS of the target device is Hard disk.

3. Pull or push the image of the devices which you have already programmed with the Boot Agent image, using Merlin.

To verify image deployment, observe the following sequence of events:

1. The device boots up through the Boot Agent.

2. The device contacts the WDM and downloads Merlin through HTTP.
3. Merlin boots up.
4. Merlin contacts the WDM server and starts the imaging process.

For more information, see Register an Image Using Merlin.

Deploying a Package Using PAD

To deploy a package with PAD:

1. On the WDM Console, select Images under Package Manager.
   The registered images are displayed on the right-hand pane.
2. Select an image, right-click and select Deploy via Peers in Subnet.
   The Peer Assisted Deployment window is displayed.

3. Select the deployment date range and time range within which you want to execute the schedule.
4. If you want to override the settings for the number of devices that support PAD, then select one of the options under Override Preferences.
5. Select the subnets to which you want to deploy the package.
   You can filter the subnets that are displayed on the grid by specifying the filter criteria under Filter Subnets.
6. Click OK to save the settings and begin deployment at the scheduled time.

**Viewing the Properties of a Registered Package**

To view the property of a software package:

1. Expand the Package Manager and select the folder that contains the software package for which you want to view the properties.
2. Right-click the software package and select Properties.
3. The Edit Package window is displayed.

   ![Edit Package Window]

   - **Name** - Name of the registered package.
   - **Description** - Description of the Package.
   - **Active** - The package will be Active and you can deploy this to a device if checked otherwise it will be inactive and user can not deploy the package to a device.
   - **Operating System** - The name of the Operating System for which this package is compatible.
   - **Size** - Size of the package in Kilo Bytes.
   - **Date Created** - Package creation date and time.

**Viewing and Editing the Package Script of a Registered Package**

To view the property of a software package:

1. Expand the Package Manager and select the folder that contains the software package you want to view the property.
2. Right-click the software package and select View Package Script.
3. The Package Script window is displayed.
4. In Package Script window check the box “Edit and Save Script to Database ONLY”. The following screen is displayed.

```
[Version]
Number=Checkin1
Description=This script will have devices checkin
OS=XP
Category=Other Packages

[Script]
CD "XP"
```

5. You can modify the script part of the rsp file and press OK to save it.

**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. Expand the Package Manager node and select the folder that contains the software package you want to export.
2. Right-click the software package and select Export Package Script.
3. The following window is displayed.
4. Browse through the path where you want to save the script and click on OK button to save.
5. The confirmation window will appear, click on OK button to save the script at specified location.

**Deleting Packages from the WDM Database**

Before deleting software packages from the WDM Database, you should understand the update distribution process and the content of packages, and ensure that the package that you want to delete has already been registered in the WDM Database.

**NOTE:** You can only delete software packages that are not scheduled for distribution. If you delete a software package that has already been distributed, you can recover it from the Backup folder of the WDM Repository and re-register it. When archived, a package receives a date-stamped name, therefore, before re-registering an archived package, you must rename it to its original name.

**CAUTION:** When you delete a software package that has never been distributed, WDM also deletes it from the WDM Repository. The package is recoverable only if you have a copy of it outside of WDM. In such a case, you can re-register the package.

To delete a software package:
1. Expand the **Package Manager** and select the folder that contains the software package you want to delete.
2. Right-click the software package you want to delete and select **Delete**.
3. Click **Yes** to confirm and delete the software package.

### Using the WDM Scripting Language

The WDM Scripting Language is a simplified scripting language that you can use to build your own software and image packages. You can also use the WDM Scripting Language to perform basic tasks such as copying files and modifying the registry of the devices that WDM manages. The Scripting Language is not a programming language because it does not support looping, branching, and the use of subroutines. However, it does contain a small command set to allow it to perform a variety of routine functions such as checking the operating system version on a given device.

**NOTE:** To generate the script for any custom package, use "**Script Builder**" utility packaged with WDM in the utilities folder.

For information on using the WDM Scripting Language, refer to [Advanced Administration](#).
Update Manager

Update Manager is the third node in the tree view of the WDM console. It appears as follows:

The Update Manager allows you to:

- Distribute packages to selected devices (immediately or on a scheduled basis). See, Distributing Device Updates.
- Perform Peer Assisted Deployment. See, Peer Assisted Deployment.
- Track device updates that are scheduled for distribution.
- Track synchronization of Remote Repositories.
- Reschedule pending updates.
- Track scheduled real time commands.
- Delete pending updates.
- Modify multiple errored out/scheduled updates.
• Perform recurring updates to devices. See, Distributing Device Updates using Recurring Scheduler.

Tracking Software Repository Synchronization Jobs

1. In the WDM Console tree pane, click Update Manager and then click Software Repository Synchronization.

   The results pane displays any scheduled, error and in-progress repository job synchronization packages.

2. If you want to delete a any repository job, select the row for the scheduled job you want to delete or edit (use SHIFT+CTRL to select multiple rows) and click the Delete icon from the menu bar to delete the selected job.

3. Click Yes to confirm the deletion.

4. To edit the selected job(s), right-click the selection and choose Properties. The Edit Update window is displayed.

5. Modify the desired fields and click OK to confirm your changes.

Tracking Scheduled Packages

1. In the WDM Console tree pane, click Update Manager and then click on Scheduled Packages.

   The results pane displays any scheduled, error and in-progress packages or updates scheduled to the devices.

2. Select the row for the scheduled package you want to delete or edit (use SHIFT+CTRL to select multiple rows) and click the Delete icon from the menu bar to delete the selected job.

3. Click Yes to confirm the deletion.

4. To edit or delete the selected update(s), right-click the selection and choose Properties. The Edit Update window is displayed.

5. Modify the desired fields and click OK to confirm your changes.

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. 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:

• Windows Embedded
• SUSE Linux — SLETC 11 SP2

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.

To make a Windows device PAD capable:

1. Make sure that the device has the latest released version of Windows Embedded Standard 7 image.
2. Make sure you have Z/D class devices with a minimum of 8GB flash drive and 4GB RAM.
3. Deploy the latest available version of **WES7 HAgent** on the device.
4. Deploy the latest available version of **BootAgentUpgradeWES7** on the device.
5. Deploy **PADService_SysprepScript_WES7** on the device.
6. Delete the **HagentSettings.ini** file from \Program Files\WDM and run the following command in the command prompt:
   ```
   Hagent.exe —Install
   ```
7. Prepare the device to pull the image by executing the batch file **WES7_CustomSysprep4man.bat -r** present in the \windows\setup folder .
8. Set the device check-in interval to at least 1 hour.
9. Pull the image using WDM.
10. Deploy the pulled image using the Peers in Subnet option.

   For more information, see Deploying a Package Using PAD.

To confirm whether a device is PAD capable or not:

1. Select Device Manager on the tree pane of the WDM Console, and from the right-hand pane select any device.
2. Click the Hardware Info tab on the bottom pane to view the details of the selected device.

   If the device is not PAD capable the PAD Capable flag is set to False as shown below:
3. After you configure the device to be PAD capable, the PAD Capable flag is set to **True** as shown below:

**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.
To configure PAD on WDM:

1. On the WDM Console, select **Configuration Manager → Preferences**.
2. On the right-hand pane, double click on **Subnet Preferences**.
   The Preferences window is displayed.

   ![Preferences Window](image)

3. Specify the minimum number of required peer capable repositories as One or Two.
4. Change the maximum number of simultaneous connections to the master device if required. The default is 7.
5. Click the button next to **Configure Repository Details**. The **Configure Peer Assisted Deployment** screen is displayed.
6. Specify the Repository Details for the following options:
   - **SUSE Linux** — specify the User Name, Password, and the relative path of the WDM server.
   - **Windows Embedded Standard 7** — specify the User Name, Password, and the HTTP Port Number for the peer device to download image from the PAD master repository device.

7. Click **Update Changes** to save the configuration and **Close** to close the window.

**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 Deployment** node under **Update Manager**. The node displays the **Repositories**, **Schedules**, and **Summary**.

2. To view the list of clients that serve as Master repositories, select **Repositories** under **Peer Assisted Deployment**. The list of clients are displayed on the right-hand pane.

3. To view the PAD schedules, select **Schedules** under **Peer Assisted Deployment**. The list of package deployment schedules are displayed on the right-hand pane.
4. To view the PAD Image update process, select **Summary** under **Peer Assisted Deployment**. The progress is displayed on the right-hand pane.
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 Deployment under Update Manager and select Schedules.
      The schedules are displayed on the right-hand pane.
   b. Select a schedule, right click and select Edit PAD Schedules.
      The Edit Schedules window is displayed.
   c. Change the date and time ranges as required and click Update Times.
      The schedule displays the new date and time.

2. To delete a PAD schedule:
   a. On the WDM console, expand Peer Assisted Deployment under Update Manager and select Summary.
      The schedule summaries are displayed on the right-hand pane.
   b. Select a summary, right-click and click Delete.
      The schedule is deleted.
Updating Devices

The device update process includes distributing single or multiple software packages to one device or to a group of devices on your network. The type of software packages you send to your devices depends on the needs of your organization.

**NOTE:** Before you can distribute any package, you must first register it. For more information, see Using the Package Wizard.

1. Examples of device updates include:
   - **Application updates** - A package that either sends or retrieves an application to or from a device.
   - **Image updates** - A package that either sends or retrieves a base image (an OS, system settings, and any other packages) to or from a device.
   - **Settings updates** - A package that either sends or retrieves Independent Computer Architecture (ICA) settings, Remote Desktop Protocol (RDP) settings, or registry entries to or from a device.

2. In addition to the packages offered by your device vendor, the WDM Script Language allows you to create your own software packages. For example, you could create custom packages for device-management tasks such as:
   - Manipulating a device registry
   - Sending a file to the device
   - Retrieving a file from the device
   - Executing a file on a device
   - Changing an application configuration

3. WDM distributes software packages either manually (by using either the Software Distribution Wizard or the drag-and-drop method) or automatically (by assigning a Default Device Configuration).

   **NOTE:** You can obtain packages from your device vendor or create your own package with WDM Script Language (information to create a package can be obtained by reading the image or configuration of the device).

4. The manual distribution process includes (in the order shown):

   **NOTE:** Before you begin to distribute packages, you must create your Device Views as described in Creating Device Views.
   - **Registering the package into the WDM Database** - By using the Package Manager (the package must exist in your network).
   - **Switching to the Device View where you want to distribute the package** - By using the Device Manager (you must first create this Device View for the package distribution).
   - **Dragging and dropping the package you want onto the group you want in the Device View** - By using the Package Manager (this process can be automated by using the Software Distribution Wizard).
   - **Selecting the devices that will receive the package in your current device group** - This process can be automated by using the Software Distribution Wizard.
   - **Scheduling the package distribution** - By using the Scheduling Preferences (this process can be automated by using the Software Distribution Wizard).

5. The automatic distribution process includes (in the order shown):

   **NOTE:** The Default Device Configuration (DDC) method of package distribution is automatic because, once set, WDM automatically sends the packages in the DDC to the devices whenever it is necessary and without your intervention. Assigning DDCs to groups of devices ensures conformity, and allows you to target functional areas of your enterprise with tailored imaging and configuration.
• **Determine the target devices** - Identify the devices to which you want to assign a DDC, and create a suitable Device View to isolate the target devices (a DDC can only be applied to a group of devices that have the same OS and media size).

• **Determine the make-up of the DDC** - Identify the images and/or packages that you want to include in the DDC (be sure you have created the images and that all packages are registered in the WDM Database).

• **Assign the DDC** - Use the procedures in Creating Default Device Configurations to isolate the target devices by OS within any branch or entire Device View and media size; also be sure to assemble the DDC by selecting its own OS and the packages you want to deploy with the DDC (you can also determine the sequence in which the packages are executed on the devices).

### Distributing Device Updates through the Package Distribution Wizard

Before using the **Package Distribution Wizard** to distribute updates to devices, you must register the appropriate software packages that contain the settings, applications, or image updates you want to distribute.

You can distribute the following types of updates to devices:

- Settings that include registry modifications, `.ini` file modifications, addition or deletion of individual files.
- New applications.
- Complete images.

> **NOTE:** Updates are custom scripts and can serve other functions such as collecting certain inventory files from a device or a group of devices.

To distribute the device updates:

1. On the WDM Console, right-click on the **Update Manager** node and select **New → Update**.

   The Package Distribution Wizard is displayed.
NOTE: You can also launch the wizard by selecting the device in the right-hand pane of Device Manager, right-clicking on it and selecting Package Distribution Wizard from the menu.

2. Select the folder that contains the software package you want to distribute and click Next.

The packages to be distributed are displayed.
3. Select the package that you want to distribute and click Next.

The device views that you created under Device Manager are displayed.
4. Select the view to which you want to distribute the package.

The devices that belong to the selected group are displayed.
5. Select the devices one by one or click **Select All** on the right-hand pane and click the > button to add the device under the **Selected Devices** pane.

6. Check the **Recurring Update** check box to schedule a recurring update. For more information, see **Distributing Device Updates using Recurring Scheduler** and **Edit/Modify Recurring Updates**.

7. Select the devices under the **Selected Devices** pane and click **Next**.

8. Select the date and time when you want the distribution to start under **Distribution Will Occur** section. Select **Retry Failed Updates** if you want WDM to retry pushing update packages if they have failed.

   If your devices are serviced by a remote repository and you have set the preference to synchronize the remote repositories, then you will be prompted to enter the synchronization information.

9. Click **Next** to create the updates.

10. After the wizard notifies you that updates are created, click **Finish**.

**Distributing Device Updates using Recurring Scheduler**

Before using the Software Distribution Wizard to distribute updates to devices, you must register the appropriate software packages that contain the settings, or applications you want to distribute.

1. Use the procedures in this section to distribute the following types of updates to devices:
   - **Settings**, including:
2. Recurring update scheduling is made available through the Package Distribution Wizard. This wizard may be launched using one of the following methods:
   a. Run Wizard...
   b. New Update

3. **Run Wizard...** method:
   a. Switch to the Update Manager view.
   b. Right-click on Update Manager and select **New** → **Update** to launch the Package Distribution Wizard.

   **NOTE:** The package distribution can also be performed by selecting the package the needs to be scheduled from Package Manager and then Drag and Drop it to the Device Manager View.
   c. Select the folder that contains the software you want to distribute and click **Next**.
   d. Select the software package to distribute and click **Next** (the device groups you see in the Update Manager view depend on the Device View you selected in step 1).
   e. Select the group of devices to receive the update (to select all of the groups in the hierarchy, select **Device Manager** at the top of the hierarchy) and click **Next**.
   f. Check the **Recurring Update** check box and click **Next**.
   g. Create Recurring Update window is displayed.
h. Enter a description for the recurring update, select the time of day that the recurring update will be sent to the device(s) and the recurrence pattern - either daily or weekly.

\[\text{NOTE: If Weekly, select the recurrence interval and the day(s) of the week. If Daily scheduling, select every day, every weekday, or the day of the week.}\]

i. Select the start and end dates and click **Next** and **Finish** to create the recurring update.

4. **New Update** method:

a. On the left panel tree view, navigate to **Update Manager**->**Recurring Schedules**. Launch the Wizard with either:
   - On the main toolbar, click the **Schedule a Software Update** button. Or
   - Right click in either main panel and select **New** -> **Update**.

b. Now follow the above mentioned steps (Run Wizard method) to create a recurring update.

**Editing Recurring Updates**

To edit or modify the Recurring Updates:

1. Expand the **Update Manager** node in the tree view of the WDM Console.
2. Select the **Recurring Updates** node.
3. Select the update to be edited. **Right** click and select **Properties** from the context menu.
4. The Edit Recurring Updates window is displayed with the update details.

5. Change any of the update settings and click **OK** to save the update settings.

6. To view a list of the devices scheduled for the selected update, check the **View Clients** checkbox.
### Editing Scheduled Device Updates

**NOTE:** You cannot edit in-progress device updates. If a device has been removed from a network before deleting a scheduled update for that device, the scheduled update may remain in a status of in-progress indefinitely.

To edit scheduled updates:

1. In the tree view of the WDM Console, expand **Update Manager** and click **Scheduled Packages**. The right-hand pane displays the scheduled and in-progress device updates.
2. Select the scheduled update you want to edit, right-click and select **Properties**. The **Edit Update** window is displayed.
3. Make the desired changes in the **Edit Update** window.
   - If you want to select the **Next Time the Device Boots** option, make sure that the device supports PXE and that you set the preference to allow updates to occur at PXE.
**NOTE:** If the device updates are linked to a Remote Repository, you may see two update records. The first record is for an update to synchronize the Remote Repository with the Master Repository. The second record is for the actual update to the devices that are serviced by the Remote Repository. You can edit either or both of these updates. However, you cannot reschedule the synchronization update to occur after the update for the corresponding devices.

4. After making the desired changes, click **OK**. The changes are displayed on the WDM console.

5. If the schedules display an **Error** status, select the schedule, right-click and select **Error Details** from the menu.

   The details are displayed in the **Error Details** window.

### Deleting Scheduled Device Updates

Use these procedures to delete device updates that you have previously scheduled.

**NOTE:** You cannot delete in-progress device updates. If a device has been removed from a network before deleting a scheduled update for that device, the scheduled update may remain in a status of *in-progress* indefinitely.

To delete scheduled updates:

1. In the WDM Console tree pane, click **Update Manager** (the results pane displays any scheduled and in-progress device updates).
2. Select the row for the scheduled update you want to delete (use **SHIFT+CTRL** to select multiple rows).
3. Click the **Delete** icon from the menu bar.
4. Click **Yes** to confirm the deletion.

### Software Repository Synchronization

To synchronize remote repositories:

1. Expand the **Update Manager** node in the tree view of the WDM Console.
2. Select **Software Repository Synchronization**, right-click and select **New → Remote SW Repository Sync...**

   The Remote Software Repository Synchronization Wizard is displayed.
3. Select the folder that contain the updates to be synchronized and click **Next**.

   The packages to be synchronized are displayed.
4. Select a package and click **Next**. The remote repositories are displayed.
5. Select a repository and click **Next**.
6. Specify the date and time for the synchronization.
7. Select **Retry Failed Updates** if you want the synchronization to be retried if it fails.
8. Click **Next**, and in the window that is displayed , click **Finish** to complete the repository synchronization.

   The synchronization record is displayed on the WDM Console against **Update Manager → Software Repository Synchronization**.
NOTE: When you are synchronizing the repositories, make sure that there is at least one common protocol is configured between the Master and the Remote repositories. For example, if you have configured the Master repository for HTTPS protocol, you must configure the Remote repository also for the HTTPS protocol.
Report Manager

Report Manager is the fourth node in the tree view of the WDM Console.

You do not need to create the same report once you have created it. Every time you view the report, it displays latest information from your devices according to the criteria you set up in the report.

To create, view, and save a report:

2. Enter a Name and Description for your report.
3. Select any group of devices and any available sub-selections that you want to include in the report, and then add them to the report. You can also use the AND and OR options to qualify your selections further.

   In case of Log Report select the Start date and End date for the data you want to generate in report.
4. After selecting the devices and sub-selections you want, you can generate the report and view the results.

5. To save a report as a .txt file (which you can print), click the **Save Report** icon in the tool bar and assign the report a name.

6. To use the report in the future, simply select the report from the **Report Manager** and view the latest device information that fits the criteria of the report.

You can use the report manager to create, save, and print the following:

- Device Listing Reports. See [Creating a Device Listing Report](#).
- Log Reports. See [Creating a Log Report](#).
- Package Distribution Reports. See [Creating a Package Distribution Report](#).
- Client Package Reports. See [Creating a Client Package Report](#).
- Installed Software Reports. See [Creating an Installed Software Report](#).
- Client Down Time Reports. See [Creating a Client Down Time Report](#).
- Package Synchronization Reports. See [Package Synchronization Reports](#).
- Installation Details. See [View the Installation Details](#).
- Component Details. See [Viewing the Component Details](#).

## Creating a Device Listing Report

Device Listing Reports provide important information about the devices in your WDM environment. 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 Report Manager node (in the WDM tree of the Administrator Console) 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 very 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 device listing report:

2. Enter a Name and Description for your report (be sure to name and describe the report in a way that will allow you to easily recognize it later) and click Next.

3. Make the desired device selections by OS, Image, Subnet, Platform, or Vendor ID... and click OK to generate the report.

- The lower panes let you select a group and individual choices within a group. For instance, to include devices with the OSes Linux, CE, and WES, first you select OS. Then you use the Ctrl key to select the desired OSes from the Choose Group Selection panel. For example:
Finally, you select Add/OR to move your choices to the selection panes. For example:

- Individual items within a group always use the OR condition. In the example above, the device listing would include any devices whose OS is either WES, CE, or Linux.
- Across groups, you can use either selection condition, AND and OR, but not both. For instance, you can add Subnet to your selection criteria and use the AND radio button to ensure that your device listing includes only the devices that meet your OS selection in addition to residing in a specific
subnet. Conversely, if you used the OR radio button, then the device listing would include devices from your selected OSes or devices from a given subnet regardless of OS.

- The conditions AND and OR are global. After you have selected either AND or OR between the first and second selection groups, all other selections across groups will also be ANDed or ORred with the result of your previous selections.
- To remove a selection criterion, select the criterion (for instance, OS Windows XP) from the selection pane and click Remove.
- To remove all selection criteria, click Clear All.

The results pane displays the Device Listing.

**NOTE:** To save a report as a .txt file (which you can print), click the Save Report icon in the toolbar and assign the report a name (you can compare reports that you save as .txt files). To use the report in the future, simply select the report from the Report Manager.

### 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 Report Manager node (in the WDM tree of the Administrator Console) 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 very 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:

2. Enter a Name and Description for your report (be sure to name and describe the report in a way that will allow you to easily recognize it later) and click Next.

The wizard prompts you for the start and end ranges for your log report:
3. Select the desired ranges and click Next.

The wizard prompts you to choose a single user or all users whose activity your log report will include:
Creating a Package Distribution Report

Package Distribution Reports provide important information about Packages deployed into the devices in WDM. 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 Report Manager node (in the WDM tree of the Administrator Console) 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 very 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 device listing report:

The Report Wizard dialog box is displayed.

2. Enter a Name and Description for your report (be sure to name and describe the report in a way that will allow you to easily recognize it later).

3. Make the desired Group selections by Agent Update, Device Configuration, Images, or Other Packages and click OK to generate the report.

The results pane displays the Package Distribution Report.

NOTE: To save a report as a .txt file (which you can print), click the Save Report icon in the toolbar and assign the report a name (you can compare reports that you save as .txt files). To use the report in the future, simply select the report from the Report Manager.

Creating a Client Package Report

Client Package Reports provide important information about Packages deployed into the specific devices in WDM. 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 Report Manager node (in the WDM tree of the Administrator Console) 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 very 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 device listing report:

   The Report Wizard dialog box is displayed.

2. Enter a Name and Description for your report (be sure to name and describe the report in a way that will allow you to easily recognize it later).
3. Make the desired View, Subgroup as well as client(s) selections by different available Views, different subgroups and the client(s) and click OK to generate the report.

The results pane displays the Client Package Report.

NOTE: To save a report as a .txt file (which you can print), click the Save Report icon in the toolbar and assign the report a name (you can compare reports that you save as .txt files). To use the report in the future, simply select the report from the Report Manager.

Creating an Installed Software Report

This enables the user to create a report - listing the devices that have the specific software installed (or not installed) and version selected by the user.

Use the following guidelines to create and view installed software report:

1. Expand Report Manager, right-click Installed Software Reports and select New | Report....
   The Installed Software Report dialog box will be displayed.
2. Or right-click on **Report Manager**, and select **All Tasks | Run Wizard**...

The Select Wizard dialog box will be displayed.
3. In the Select Wizard, select the node for Report Manager | Report Wizard. The Report Wizard dialog box will be displayed.

4. In the Report Wizard, select the radio button for Installed Software Report Manager and then press Next.
The Installed Software Report dialog box will be displayed as in Figure 9.9.

5. Enter a Name and optional Description for your report (be sure to name and describe the report in a way that will allow you to easily recognize it later).

6. Select the installed software from a list of all installed software on all registered devices.

7. Select the version of the selected software (or the list item ALL VERSIONS) from the Select Version list box.

8. Select whether the report shows devices that have the selected software installed or those that do not have the selected software installed (using the Software Installed radio buttons).

9. Select all devices from the Select a Group list box - or create a device filter using existing specified grouping values and the search criteria control buttons. (A Platform and OS filter has been created as an example and is displayed in the Selected Items list view in the above figure)

10. Click OK to generate the report.

The results pane displays the Installed Software Report.

NOTE: To save a report as a .txt file (which you can print), click the Export List icon in the toolbar and assign the report a name (you can compare reports that you save as .txt files). To use the report in the future, simply select the report from the Report Manager.

Creating a Client Down Time Report

Client Down Time Reports provide important information about the down time period for the specific devices in WDM. It allows you to easily see what you want, when you want it. Based on the selected criteria, WDM automatically saves the report in the Report Manager node (in the WDM tree of the Administrator Console) so you can use it again whenever you want. There is no need to create the report. Every time you select the node, you get the very 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 view client down time report:
1. Expand **Report Manager**, select **Client Down Time Reports** and click on the **Create a new Report** icon in the Tool Bar Menu.

2. The wizard prompts you for the view, subgroup as well as client selection criteria:

   ![Client Down Time Report]

3. Make the desired View, Subgroup as well as client(s) selections by different available Views, different subgroups and the client(s) and click **Generate**.

   The results pane displays the Client Down Time Report.

   ![Client Down Time Report]

   **NOTE:** To save a report as a .txt file (which you can print), click the **Save Report** icon in the toolbar and assign the report a name (you can compare reports that you save as .txt files). To use the report in the future, simply select the report from the Report Manager.

**Package Synchronization Reports**

Package Synchronization Reports provide the important information about the synchronization of packages between the master and remote repositories. There are three types of Package Synchronization Reports:

- **Package Synchronization History**
- **Unsynchronized Package Report**
- **Orphaned Package Report**
**Package Synchronization History Report**

This report displays the details of package synchronization for each package in master repository with a remote repository. A record is displayed each time a package is synchronized with a remote repository. For example, a package synchronized with 5 remote repositories displays 5 rows each time that package is synchronized.

To view and export package synchronization history, on the WDM console expand **Report Manager → Package Synchronization Report** and select **Package Synchronization History**.

The right-hand pane displays the detailed report. The following details are displayed:

- **Repository** - Name of the remote repository for which the package was synchronized with the master repository.
- **Package Name** - Name of the software package.
- **Synchronization Time** - Time the package was synchronized with the remote repository. Packages scheduled for synchronization but not yet synchronized are not displayed here.
- **Version** - This is only valid for the most recent synchronization of that package with the remote repository.
- **Master Version** - This is the current version of the package in the master repository.
- **Status** - This represents the comparison of the version of the package in the master repository and the version in the remote repository at the current time. If the versions are the same in the most recent record - then the package is synchronized with that remote repository. If the versions are not the same, then the status is not synchronized. If the package in the master repository has been deleted, it will show up as deleted status. If packages remain in the remote repositories, these will show up in the Orphaned Package report.

**Unsynchronized Package Report**

This report displays a row for each package that has different current versions in the remote repository as compared to the master repository.

To view and export package synchronization history, on the WDM console expand **Report Manager → Package Synchronization Report** and select **Unsynchronized Package Report**.

The right-hand pane displays the detailed report. The following details are displayed:

- **Repository** - Name of the remote repository for which the package is not synchronized with the master repository.
- **Package Name** - Name of the software package.
- **Last Synchronized** - The time of the most recent synchronization record displayed in the Package Synchronization History Report.
- **Version** - This is the current version of the package in the remote repository.
- **Master Version** - This is the current version of the package in the master repository.

**Orphaned Package Report**

This report displays the list of packages in each remote repository for which the corresponding package has been deleted in the master repository.

To view and export orphaned package report, on the WDM console expand **Report Manager → Package Synchronization Report** and select **Orphaned Package Report**.
The right-hand displays the detailed report. The following details are displayed:

- **Repository** - Name of the remote repository that contains a package which is not in the master repository.
- **Package Name** - Name of the software package.
- **Last Synchronized** - The time of the most recent synchronization record displayed in the Package Synchronization History Report.
- **Version** - This is the current version of the package in the remote repository.

**Viewing the Installation Details**

Installation Details provide the important information about the installed components of WDM.

To view the installation details:

1. Expand **Report Manager** and select **Installation Details**.
2. The results pane displays the detailed information about the different installed components of WDM:
   - **Component** - Name of WDM Component.
   - **Server Name** - Name of the Server in which WDM Component is installed.
   - **User Name** - Login ID of the User.
   - **Installed On** - The date and time on which the specific component has been installed.
   - **Repository** - Name of the main repository of WDM.
   - **Latest Hot Fix ID** - Latest hot fix ID of WDM installed on the server.
View the Component Details

Component Details provide the important information about all the running components of WDM.

Use the following guidelines to view the Component Details:

1. Expand Report Manager and select Component Details.
2. The results pane displays the detailed information about different running components of WDM:
   - **Server Type** - Name of WDM Component.
   - **Server Name** - Name of the Server in which WDM Component is installed.
   - **IP Address** - IP Address of the Server in which WDM Component is installed.
   - **Listening Port** - Port number on which the specific Component is communicating.
   - **SSL Port** - SSL Port Number.
   - **TZ Offset** - The value of Time Zone offset related to GMT.
   - **Check In** - The date and time at which the specific component has checked in.
   - **Check Out** - The date and time at which the specific component has checked out.
Remote Sessions History 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 easily 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 console. You can export this report and use it later. After the view is changed the report is no longer available, and you have to regenerate the report.

To generate the Remote Sessions History Report:

1. Expand **Report Manager** in the tree view of the WDM Console and select **Remote Sessions History Report**.
2. Right-click on right pane of Report Manager and select **New → Report**.
3. The **Remote Session History Report** window is displayed.
Provide the following information:

- **Search Criteria** - Provide Device Name, Connection Type, Connection Name etc., based on the requirement
- **Relation** - Select the relation for the Search Criteria.
- **Value** - Specify the value for the selected Search Criteria.
- **Case Sensitive Filter** - Check the box if the Search Criteria value is case sensitive.
- **Report Duration** - Select the duration for the report. By default it is past 45 days from the current date (this is defined in the preferences). User can also give the date range for the report

4. Click **Add** to add your selection criteria in the **Final Selection for Report** pane.
5. After defining the required report creation criteria, click **OK** to display the report on the right pane of the console.

**Remote Sessions Summary Report**

The Remote Sessions Summary Report provides a summary of the remote session connections by all the devices in WDM during a specified time period.

To generate the Remote Sessions Summary Report:
1. Expand **Report Manager** in the tree view of the WDM Console and select **Remote Sessions Summary Report**.

2. Right-click on right pane of Report Manager and select **New **→**Report**.

3. The **Remote Session Summary Report** window is displayed.

![Remote Sessions Summary Report](image)

Provide the following information:

- **Report Duration** - Select the duration for the report. By default it is past 45 days from the current date. You can change this in the Device Manager Preferences screen. For more information, see **Device Manager Preferences**. You can also give the date range for the report.
- Click **OK** to display the report on the right pane of the console.
Configuration Manager

Configuration Manager is the last node in the tree view of the WDM Console. As the name suggests, you can perform various operations pertaining to configuration and management of WDM.

You can perform the following operations in Configuration Manager:

- Create and edit group types. See Group Types.
- Create new and edit existing Device Views. See Device Views.
- Setup Default Device Configurations. See Creating Default Device Configurations.
- Create configuration packages using the Profile Manager. See Profile Manager.
- Manage WDM licenses. See Activating WDM Sales Keys.
- Configure WDM system preferences. See Configuring Preferences.
- Define Remote Repositories and assign them to subnets (WDM Enterprise Edition only). See Registering Remote Repositories.
• Create and edit subnets and IP ranges. See Setting Subnets Manually and Setting IP Ranges Manually.
• Set up WDM users and maintain their permissions. See User Management.
• Import IP ranges, subnets, and software repositories. See Importing Data into the Database.
• Generate Diagnostic Reports. See Viewing the Diagnostic Report.
• Track Certificate Expiration. See Certificate Authority Expiration Tracker

Group Types

Groups can be defined as a Group Type (predefined or custom), a Group Instance (within a Group Type), or any combination of these items. WDM allows you to use predefined Group Types that includes:

• Operating System
• Platform
• Image/Firmware Image Number
• Subnet
• Location
• Contact

You can also create any number of custom group types and group instances to facilitate the organization of your devices into functional hierarchies. You can then use these groups to create custom device views for your devices. For more information, see Creating Custom Group Types.

Creating Custom Group Types

To create a custom Group Type:

1. In the WDM Console tree pane, expand the Configuration Manager, right-click the Group Types node, and select New | Group to open the Create New Group Type dialog box.
2. Enter the Name and Description for the Group Type.

3. In the space provided, enter the names of the device groups that you want to manage under this group type.

4. Click OK to add the Group Type to the list of available WDM Group Types that you can use when assigning devices to groups (see Assigning Devices to Groups).

**Editing Custom Group Types**

You can add groups to the group type, delete groups, or change the name of the group type by editing the group type. To edit a group type:

1. In the WDM Console tree pane, expand the Configuration Manager, select the Group Types node. The Edit Group Type dialog box is displayed.

2. If you want to change the name or the description of the group type, enter the new name or description or both in the Name and Description fields.

3. If you want to add a group name, click Add and in the Group Name dialog box, enter the name of the group you want to add. Click OK.

4. If you want to delete a group, click Delete. The application prompts you to confirm the deletion. Click OK if you want to proceed with the deletion.

5. If you want to change the name of a group, click Change. In the Group Name dialog box, enter the new name of the group. Click OK.

6. Click OK in the Edit Group Type dialog box to save the changes.
Device Views

Device Views offer a way to visually organize your devices functionally so that you can better manage them. Wyse Device Manager uses an organizational system based on group types and groups so that you can assign a hierarchical structure to your devices.

Since Wyse Device Manager lets you create your own user-defined group types and groups, you can organize your devices in any way that best suits your organization’s needs. Wyse Device Manager also provides predefined group types for your convenience.

Views are built on Group Types arranged in a user-assigned hierarchy. You can build views based on the ten built-in group types (predefined group types), or on user-created Custom Group Types (user-defined Custom Group types), or on any combination of built-in and user-created Groups.

The process to create Device Views can be broken down into three stages:

Stage I: Determine Logical Groups and a Hierarchy for your Device View

1. Analyze your organizational structure along functional lines and ask yourself, How can I logically group my devices to better manage them? Then conceive the necessary categories (or group types) that you can use to organize your devices. Wyse Device Manager allows you to use these group types to build hierarchies of device groups (or Device Views) with any level of granularity. When your devices are grouped into hierarchies of Device Views, it is much easier to manage and control them.

   • To come up with group types, consider the ways in which your organization distributes software or updates, provides technical support, is functionally organized (along the lines of departments, office branches, region), and distinguishes its applications (point-of-sale, back-office).

   • Wyse Device Manager provides six predefined group types that you can use immediately. By considering your organization’s functional environment, you can add any number of user-defined group types. The more group types you come up with, the more granular and varied your Device Views can be.

2. Determine ways of organizing the group types you conceived into functional hierarchies of devices (Device Views) for your organization. For example, if your group types include Building and Department, you could have one Device View that groups devices by building within each department. Conversely you could use the same group types and create a Device View that groups devices by department within each building.

   • Just as Wyse Device Manager lets you have unlimited group types, Wyse Device Manager also allows you to have any number of Device Views. You can create as many Device Views as is necessary to manage your devices.

3. Use the Wyse Device Manager Configuration Manager to create the necessary group types to accommodate the organizational hierarchy you developed in the previous step.

   To create a group type, use the Group Type node under the Wyse Device Manager Configuration Manager.

Stage II: Create a Device Manager View and Select Its View Levels
1. A Device View name can be any text you want. However, it makes sense to assign device names that correspond to the levels in your view so that you can identify your views immediately.
   - By using arrows (=>) between each level, you can clearly establish the hierarchy of your view with the Device View name.
   - You create a Device View Name by using the Views node under the Configuration Manager.

2. Every Device View requires you to select at least one view level. The number of view levels dictates the granularity of your device hierarchy. View levels equate to group types that you might have created earlier, in Stage I.
   - In our example, we assume that you have created group types for Building and Departments. Because our example Device View uses a two-level hierarchy of Building => Departments, you would select the group type Building as the first view level. Similarly, you would select Departments as the view level-2.
   - This hierarchical arrangement would allow you to group your devices by building, and within each building, by the department to which the devices belong.

Stage III: Create Group Instances and Assign Devices to Each Group Instance

1. Create group instances (or simply groups) for each group type created in Stage I, and which you assigned to a level view in Stage II.
   - In our example, we created the Exodus I Building and Exodus II Building as group instances (groups) for the group type Building. Similarly, we created the groups Engineering Dept., Sales Dept., and Marketing Dept. as groups of the group type Departments.
   - You create groups from the Device Manager node at each view's level.

2. Drag and drop devices from the Unassigned folder into the appropriate folder for your Device View.
   - The Unassigned folder serves as a container to hold devices until they are assigned to a group.
   - After you have assigned devices among your groups to create your Device View, you can move devices from one custom group to another. If this becomes necessary, be sure to review the Rules for Moving Devices in a Device View.

**NOTE:** To create your own Device Views, see [Creating Device Views from the Configuration Manager](#).

### Creating Device Views

To create a Device View:

1. In the WDM Console tree pane, expand the **Configuration Manager**, right-click the **View** node, and select **New | View** to open the Create New View dialog box.
2. Use the following guidelines:

- Enter the View Name and select the Group Type from the list of "Available Group Types".
- To select the Group Type from the list of "Available Group Types" -
  - Select the Group Type from the list of "Available Group Types" and double click on it.
  - or, Select the Group Type from the list of "Available Group Types" and click on "Add" button.
- To delete the Group Type from the list of "Group Type Hierarchy" -
  - Select the Group Type from the list of "Group Type Hierarchy" and double click on it.
  - or, Select the Group Type from the list of "Available Group Types" and click on "Remove" button.

  **NOTE:** You can add up to 30 View Levels (Group Types).

- **Private View** - By selecting the current view as private, the grouping structure is only available to you, the current user. By clearing the check box (the default) this view will be available to all administrators who are authorized to use WDM.

- **Use as Current Device Manager View** - By selecting this check box the current view is automatically displayed by default when you click on Device Manager in the Administrator Console tree. Any previous selections for the Device Manager view will be replaced by this current view. You can switch views at any time (for details on switching views, refer to **Switching Device Views**).
• **Use as Current Update Manager View** - By selecting this check box the current view is automatically selected during the update creation process. This is also the view which is created by default while viewing the scheduled packages.

### Create New View

<table>
<thead>
<tr>
<th>Create New Group Type</th>
<th>Edit Group Type</th>
<th>Delete Group Type</th>
<th>Advanced Configuration</th>
</tr>
</thead>
</table>

**View Description**

- **Name**: Geographic location

**Hierarchy (Maximum of 30 View Levels Allowed)**

- **Group Type Hierarchy**
  - Country
  - -> State
  - -> City
  - -> Department

**Settings**

- Use as Current Device Manager View
- Private View
- Use as Current Update Manager View

### Notes:

For details on Deleting Views, refer to [Deleting Device Views](#).

For details on Editing Views, Create New Group Type and Advanced Configuration refer to [Editing Device Views](#).

3. After you have finished configuring all View Levels in the View Hierarchy, click **OK** to add the Device View to the available Device Views that you can use.

### Editing a View

**To Edit a View:**

1. In the WDM Console tree pane, expand the **Configuration Manager**, click the **View** node, and right click on an existing view.

2. Select **Properties**; to launch the **Edit View** window. The Group Type Hierarchy is shown on the left side of the window with each level of hierarchy designated by an increasingly indented “->” symbol.
3. To add an additional Group Type to the hierarchy of the Group Type Hierarchy of the selected view:
   - select a Group Type in the Available Group Types list and double click on it.
   - or, select a Group Type in the Available Group Types list and click Add button.
   - or, select a Group Type in the Available Group Types list and drag and drop it to the appropriate position in the Group Type Hierarchy.
   - The new Group Type will appear directly below the selected Group Type in the Group Type Hierarchy display.

4. To delete a Group Type to the hierarchy of the Group Type Hierarchy of the selected view:
   - select a Group Type in the Group Type Hierarchy and double click on it.
   - or, select a Group Type in the Group Type Hierarchy and click Remove button.
   - The selected group type will returned to the Available Group Types and the Group Type Hierarchy display will be updated.

5. To move a Group Type from one position to another in the Group Type Hierarchy:
   - select a Group Type in the Group Type Hierarchy and use "Move up" and "Move Down" buttons.

6. Use as Current Device Manager View - By selecting this check box the current view is automatically displayed by default when you click on Device Manager in the Administrator Console tree. Any previous selections for the Device Manager view will be replaced by this current view. You can switch views at any time (for details on switching views, refer to Switching Device Views).

7. Use as Current Update Manager View - By selecting this check box the current view is automatically selected during the update creation process. This is also the view which is created by default while viewing the scheduled packages.

8. To create a New Group Type:
   - Click on "Create New Group Type" button or "Create New Group Type" tab.
   - "Create New Group Type" is displayed.
• Fill in the "Name" and "Description" fields and click on OK button.
• The newly created group will appear on Available Groups list.

9. To go to "Advanced View Configuration"-
• Click on "Advanced View Configuration" tab.
• "Advanced View Configuration" window will appear.
• For more details on "Advanced View Configuration", follow step "12".

10. By selecting the Set Current Device Manager View, the current view will be set as the selected view.

11. By selecting the Advanced Filter, the following window Advanced View Configuration is displayed.

12. To give permissions to access the selected view to different users, use "Advanced View Configuration"-
• Individual user can be selected from the available list of users.
Select a user from the Available list and click "->" button.
or, Select a user from the Available list and double click on it.
or, Click "All" button to assign permission to all the users to access the selected view.
All the selected users will appear directly below the Selected list.

13. To remove permissions to access the selected view to different users, use "Advanced View Configuration"-
   - Individual user can be selected from Selected list.
   - Select a user from the Selected list and click < button.
or, Select a user from the Selected list and double click on it.
   - All the removed users will appear directly below the Available list.

14. To assign the filter criteria for each or any of the Groups Types in the view’s Group Type Hierarchy-
   - Select a Group type from Group Type Hierarchy.
   - Select the corresponding Group Name from “Group Names” list.
   - Click on Add button or, double click on selected “Group Name”.
   - The added Group Name will appear directly below the Filter Criteria with Type and Name.

15. To clear the filter criteria for each or any of the Groups Types in the view’s Group Type Hierarchy-
   - Select a Group type from Filter Criteria.
   - Click on Clear button to clear the selected “Filter Criteria”.
or, Click on Clear All button to clear all the "Filter Criteria".

16. By clicking the Delete option, it will delete the selected view.

NOTE: For details on deleting views, refer to Deleting Device Views.

Deleting Device Views

To delete a Device View:

1. Expand Configuration Manager and select Views to display your existing Device Views.
2. Right-click the Device View you want to delete and select Delete.
3. Click Yes to confirm and delete the Device View.

NOTE: You cannot delete a Device View that is currently in use with either the Device Manager or Update Manager (you must first switch to a different Device View before you can delete it).

Switching Device Views

To switch Device Views:

1. Right-click Device Manager and select Switch View to open the Select Current Manager View dialog box.
2. Use the lists to select the Device View that you want to use with the Device Manager and the Update Manager.
3. Click OK.

The results pane will display the view to which you switched.
Implications on Device Views

The implications of the preference Show Empty Custom Group Folders on your Device Views depends on whether the view contains folders for custom groups, predefined groups, or for combinations of the two groups.

1. **For Device Views with Folders of Custom Groups Only**
   
   If you have a Device View that uses only custom group types and groups, and the preference Show Empty Custom Group Folders is enabled, your Device View will show all of the group folders, regardless of whether devices have been assigned to every folder.

   For example, in a single-level Device View there is only one group type, Building. The group instances for this group type include the Exodus I and Exodus II buildings. Because the preference Show Empty Custom Group Folders is enabled, the Device View shows the folder for the Exodus I building even though there are no devices in it. In a Device View such as this, you can move devices from the Exodus II Building to the Exodus I Building by dragging and dropping. If the preference were disabled, however, the Device View would show only the Exodus II building.

2. **For Device Views with Folders of Predefined Groups Only**

   As mentioned earlier, the preference Show Empty Custom Group Folders has no effect on folders for predefined groups. Folders for predefined group types will not show on a Device View unless there are devices that meet the characteristics of the predefined group types. For example, if all of the devices in your network are either CE or Linux and you have a single-level Device View with the predefined group type OS, the Device View would contain only groups for CE and Linux, but not groups for any of the other possible operating systems (CE.net, Windows 2000, Solaris, etc.).

   In a Device View that contains predefined group types, Wyse Device Manager prevents you from moving devices across predefined group types. It would be illogical to move a device that has the CE OS to a folder of devices that have the Linux OS.

3. **For Device Views with Folders of Custom and Predefined Groups**

   When you have a Device View with both custom and predefined groups, the same rules as before still apply. However, because a folder for a predefined group can be the parent to children folders of custom group types, some special circumstances arise.

   Even with Show Empty Custom Group Folders enabled, folders for custom groups that are children of a predefined group type will not be shown as long as all of the custom group folders are empty. However, if a single children folder has a device assigned, all of the other sibling folders will be shown.

About Default Device Configurations

The Default Device Configuration functionality 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 will revert 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.
Creating Default Device Configurations

Before assigning Default Device Configurations (DDC) to update devices automatically, you must register the appropriate software packages that contain the settings, applications, or image updates you want to assign as a Default Device Configuration. You must also select the Enable Default Device Configuration option in the Default Device Configuration dialog box, as discussed in Device Manager Preferences.

To assign a DDC to devices:

1. In the WDM Console tree pane, expand Configuration Manager, right-click Default Device Configuration, and select New | Default Device Configuration to open the Default Device Configuration Wizard.

2. Use the following guidelines:
   - **Select A View For Adding A DDC** - Select the Device View that includes the groups of the devices to which you intend to assign the DDC. After you select a view, the View Hierarchy pane shows the various groups and levels of that view (you can use Expand All Items to view all levels in your view). In the View Hierarchy pane, select the group folder that contains the devices to which you want to assign the Default Device Configuration.
   - **Operating System** - Select the operating system of the devices to which you intend to assign the DDC.
   - **Media Size** - Enter the media size (in MBs) of the devices to which you intend to assign the DDC. The WDM script package file for any packages to be used in a DDC must specify the media size value of the intended target devices in the imagesize parameter under the [Version] section of
script (for example, Imagesize=32). For more information on scripts, refer to **Understanding the Script File Structure**.

- **Qualifying OS Image** - Select the image associated with the OS you want to form the basis for the DDC that you intend to assign. The image package must be named to correspond with the image number displayed by the Device Manager.

  NOTE: You can assign different images and packages to different view folders.

  NOTE: After selecting Operating System and Media Size, No Image option will be available in the Qualifying OS Image drop down list. By selecting this option the DDC packages can be deployed without any image in it.

- **Enforce Sequence** - 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.

3. After configuring your settings, click **Next** to open the Software Packages tab.

4. Select the packages in the Available For Selection list that you want to include in the DDC and click **Add** to move the packages to the Selected list.

  NOTE: You can use Add and Remove to move as many packages as you want to (and from) the Selected list. You can use Select/De-Select All to select or clear all package check boxes in the Available For Selection list or the Selected list. You can use Move UP and Move Down to change the order of the packages in the Selected list.
5. After configuring your settings, click **Next** to open the Execution Time tab.

6. Select either the **Whenever a device checks in** option or the **Each day at the time specified** option for DDC reconciliation (if you select the **Each day at the time specified** option, be sure to enter or select the time you want).

7. Select **Preserve Data Partition** option and **Non-PXE** option if imaging using Non-PXE and data partition needs to be preserved for DDC.

8. After configuring your settings, click **Next** to open the Summary tab.
9. View the Summary tab to ensure that you have configured the DDC the way you want (if not, use Back and make your changes), and then click Finish to open the results pane displaying the newly assigned DDC.

**NOTE:** The DDC is identified by its Operating System and Media Size. The next time a device from the Device View you specified checks-in or is discovered, and meets the Operating System and Media Size criteria, it will automatically be assigned the DDC.

**Managing the Default Device Configuration**

To manage or view the Summary of Default Device Configuration:

1. In the WDM Console tree pane, expand Configuration Manager and select Default Device Configuration, to display your existing DDCs.
2. Right-click the DDC for which you want to see the summary and select Manage DDC.
3. The Manage DDC window for the specific DDC is displayed.
4. The window is split into three parts:
   - **Primary Definition** (Not Editable)
     - This will list the View, OS and Media size which are assigned to the DDC.
     - **View Hierarchy Path** displays the group values which have been assigned to this particular DDC.
   - **DDC Image**
     - When a particular group is selected from the **View Hierarchy Path** list it displays the image which is assigned to that particular group. This image can be changed to any other image displayed in the ‘DDC Image’ drop down.
   - **Software Packages**
     - When a particular group value is selected from the **View Hierarchy Path** list it displays the corresponding software packages which are assigned to that group. The packages can be added, removed and the order can be shuffled.
     - To Add/Remove the packages the user has to click on ‘Edit Packages’ button. Once the changes are done the ‘Save Packages’ button needs to be clicked for the changes to be reflected.

**Deleting Default Device Configurations**

To delete a Default Device Configuration:
1. In the WDM Console tree pane, expand **Configuration Manager** and right-click **Default Device Configuration**, to display your existing DDCs (if you moved the DDC you want to delete to a different folder, go to the folder that contains the DDC).

2. Right-click the DDC you want to delete and select **Delete**.

3. Click **Yes** to confirm and delete the DDC.

**Profile Manager**

Profile Manager (PM) is a new feature that is added to Dell Wyse Device Manager (WDM) version 5.0. 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. A repository is a system where you save the configurations that you create. 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. DCM configurations are unique for an Operating System and you can apply only one configuration on a single group of devices at any given time.

PM is available under the **Configuration Manager** node on the WDM console.

For more information on the WDM console, see the *Dell Wyse Device Manager Online Help* or the *Dell Wyse Device Manager Administrator’s Guide*.

For more information on the PM functionality, see:

- **Identifying DCM Supported Devices**.
- **Creating a WCM Configuration Package**.
- **Enabling DCM**.
- **Creating a Configuration Package Using DCM**.

**Identifying PM Supported Devices**

Devices that are running WCM Client version 1.3.1.1 and above support the DCM feature. 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.

You can see the WCM support information in the **Hardware Info** tab on the WDM console.

If the client device supports PM, then **WCM Support** displays as **True** on the **Hardware Info** tab. This indicates that you can deploy a WCM configuration package to the device using PM.
Creating a WCM Configuration Package

To create a WCM configuration package from the WDM console:

1. On the WDM Console, expand the Package Manager node.
2. Right-click Device Configuration and select New → Configuration. The WCM Application GUI is displayed.
3. Create the WCM Configuration file by selecting and updating the required configurations. For more information on creating WCM Configurations, see the Dell Wyse Configuration Manager Administrator’s Guide available on the Dell Wyse Support Site.
4. Save the configuration.

Enabling PM in Preferences

To deploy WCM configuration packages using PM on the client devices, you need to enable PM in Preferences. If you do not enable this option, then you can only create configuration packages using WCM and same package cannot be deployed to the client devices using PM. However, you can deploy the packages using the package distribution wizard. For more information on the package distribution wizard, see the Dell Wyse Device Manager online help or the Dell Wyse Device Manager Administrator’s Guide.
To enable PM in preferences:

1. On the WDM Console, click the **Configuration Manager** node.
2. Select **Preferences** and on the right-hand pane double-click on **Device Manager Preferences**. The **Preferences** window is displayed.
3. Select **Profile Manager** under **Device Manager**.
4. Select **Enable Profile Manager** in the **Profile Manager Preferences** pane.
5. Click **OK** to save your settings.

**Deploying a Configuration Package Using Profile Manager**

To create a configuration package using DCM:

1. On the WDM console, expand the **Configuration Manager** node.
2. Right-click on **Profile** and select **New → Profile Manager**. The PM window is displayed.
3. Select the operating system from the drop-down box. The drop-down box displays only those operating systems for which you have not created configuration packages. You can create only one configuration package per operating system.
4. Select a view from the **Select a View for Adding a Profile Manager** drop-down. The drop-down displays all the views that you have created in WDM.
5. Select a node in the selected view.
6. Select a WCM configuration under **Available Configurations for Selection**. This list displays all the configuration packages that you have created for the selected operating system using the WCM application.
7. Click **Apply**. The PM Summary pane displays the complete path of the selected node and the selected configurations for the device.

⚠️ **NOTE:** You can apply only one configuration to one group. However, you can select multiple configurations and assign them to multiple groups, that is one configuration per group.

8. Click **OK**. The WCM Application GUI is launched in **Merge** mode and displays the progress of the merging of the WCM packages.
9. Click **OK** to view the PM configuration package on the WDM console.

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.

**Deleting a PM Configuration Package**

To delete a configuration package:

1. On the WDM console, expand the **Configuration Manager** node.
2. Click **Profile Manager**. The configuration packages are displayed on the right-hand pane.
3. Select any configuration package, right-click and select **Delete**. You will be prompted to proceed with the delete operation or cancel it.

4. Click **Yes** to delete the configuration package.

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

### Activating WDM Sales Keys

To activate a WDM Sales Key (license):

**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

1. In the WDM Console tree pane, expand the **Configuration Manager** and select **Licensing** to open the results pane showing your Non-activated Sales Key(s).

2. Right-click a Non-activated Sales Key from the list and select **Activate** to open the Licensing Wizard.

**NOTE**: Make a note of your Sales Key and Non-activated Key numbers to use on the online WDM licensing form. You can copy-and-paste the Sales Key and Non-activated Key from the Key Information area into the online WDM licensing form.

3. Complete the online WDM licensing form at:

https://www.rapportlicensing.com/clientframe/rapport.aspx

You will 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. After completing the form, click **Submit** to display the Activation Code (you will also receive an e-mail with your Activation Code).

5. Enter or copy-and-paste the Activation Code into the Activation Code box of the Licensing Wizard and click **Next** to open the results pane showing your Sales Key as Activated.

### Adding and Using Multiple WDM Sales Keys

You can have multiple WDM Sales Keys (licenses) as long as they are all of the same edition (WDM Workgroup Edition or WDM Enterprise Edition). By adding new Sales Keys you can add more devices to your WDM installation.

**NOTE**: You cannot have Evaluation Keys and Sales Keys of the same vendor within the same WDM installation.
To add a WDM Sales Key:

1. In the WDM Console tree pane, expand the Configuration Manager, right-click the Licensing node, and select New | License to open the License Wizard.

2. Enter (or copy and paste) the Sale Key for the license you want to add and click Next. to open the success page.

3. Click Finish to open the results pane showing your added Non-activated Sales Key.

4. Activate this added Sales Key by completing the procedures in Activating WDM Sales Keys.

Upgrading a WDM Workgroup Sales Key to an Enterprise Sales Key

Once you have an Activated or Non-activated Workgroup Sales Key added to your WDM installation, you can upgrade to an Enterprise Sales Key.

**NOTE:** During the upgrade to an Enterprise Sales Key, all Workgroup Sales Keys will be deleted.
To upgrade a WDM Workgroup Sales Key to an Enterprise Sales Key:

1. In the WDM Console tree pane, expand the Configuration Manager, right-click the Licensing node, and select New | License to open the License Wizard.

2. Enter (or copy and paste) the new Enterprise Sale Key you obtained from Wyse and click Next.

3. Click Yes to confirm and start the license upgrade. After the upgrade is complete, the results pane displays your new Non-activated Enterprise Edition Sales Key information.

4. Activate this Enterprise Edition Sales Key by completing the procedures in Activating WDM Sales Keys.

Deleting WDM Sales Keys

You can delete Activated or Non-activated WDM Sales Keys, however, only an Activated Sales Keys can be re-entered into your WDM installation after the Sales Key is deleted.


⚠️ **CAUTION:** If you delete an Non-activated Sales Key, it cannot be used again. Only an Activated Sales Key can be deleted and then re-entered into your WDM installation.

To delete a WDM Sales Key:

1. In the WDM Console tree pane, expand the **Configuration Manager** and select **Licensing** to open the results pane showing your Sales Keys.
2. Right-click the row for the Sales Key you want to delete and select **Delete**.
3. Click **Yes** to confirm the deletion. After the deletion is completed, the results pane no longer displays the Sales Key.

⚠️ **NOTE:** Since you must have at least one WDM Sales Key to operate WDM, you can delete all but the last WDM Sales Key.

## Configuring Preferences

To configure WDM preferences:

1. In the WDM Console tree pane, expand **Configuration Manager** and click **Preferences** to display the list of preferences available.
2. Double-click the name of the preference you want to configure.
3. Configure that preference as described in one of the following sections:

   - **Device Manager Preferences**
   - **Logging Preferences**
   - **Service Preferences**
   - **DHCP/TFTP Preferences**
   - **Scheduling Preferences**
   - **Subnet Preferences**
   - **WTOS Preferences**

### Device Manager Preferences

When you double-click **Device Manager Preferences** in the preference list, the **Preferences** dialog box is displayed.

1. Enter the following details:

   - **Web Service Check-In Preferences** area:
     - **Perform a partial check-in every** - Set the partial check-in frequency of 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.
     - **Missed Check-ins for Yellow Icon** - Select the number of missed check-ins before the icon for the device turns yellow to indicate there might be a problem with the device.
     - **Missed Check-ins for Red Icon** - Select the number of missed check-ins before the icon for the device turns red to indicate there might be a more serious problem with the device.
   - **Full Check-In After Update** - Select to cause a device to check-in with the Web Service after the device receives and executes the files in a package.
• **Show Empty 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. For more information, see **Understanding the Show Empty Custom Group Folders Option**.

• **Collect Data for Remote Sessions** - This option is applicable to Wyse 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 of the WDM Console. For more information, see **WDM Console**. This data is useful in charging the end users for the remote sessions.

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

• **GUI Discovery Preferences** area:
  – **Maximum number of ranges to discover** - Enter the number you want to discover.

• **Socket Family Preferences** area:
  – **Select from IPv4, Dual Stack, and IPv6** - Supports setup of WDM components in IPv4, dual-stack and IPv6 mode, i.e. all components of WDM (server, database, GUI and remote repositories) can run/connect over the selected option.
    
    At present none of the WDM platform management agents (hagent) support management over IPv6. Support for running WDM in IPv6 is experimental, and not fully supported. You need to reboot the device to make this change take effect.

2. Click **DDC (Default Device Configuration)** in the Device Manager tree to launch the Default Device Configuration window:

3. Specify the following details:
• **Enable Default Device Configuration** - (WDM Enterprise Edition only) Select this option if you want to allow devices to use DDCs for automatic upgrades (see Creating Default Device Configurations).

• **Time to Schedule DDC Reconciliation** area - Select the appropriate option:
  - **Upon Check-in**
    - if you want the DDC to occur when a device checks-in with the Web Service
  - **Custom Time**
    - to specify the time of the day after which you would like DDC to occur. The actual time however, depends on the frequency of check-ins you set in the Device Manager preferences.

4. Click **Discovery** in the Device Manager tree to launch **Post Discovery Settings for agents** window.

5. Specify the following details:

• **Enable automatic discovery methods** - Select if you want to allow devices to use all discovery options mentioned in the list. You can select one or more options from the list.
  - **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 optipon tags** - Select if you want to allow devices to use DHCP option tags to discover WDM Server.
  - **Manual discovery from Device Manager (using Find Devices)** - Select if you want to discover devices from WDM Server **Find Devices**.
• **Enable autodiscovery after missed check-ins** - Select the number of missed check-ins to enable autodiscovery options.

6. Click **Profile Manager** in the Device Manager tree to launch Profile Manager Preferences window.

7. Specify the following details:
   - Select **Enable Profile Manager** in the Profile Manager Preferences pane.
   - Click **OK** to save your settings.

**Logging Preferences**

Select **Logging Preferences** in the preference list and double-click to launch the Preferences window.
1. Specify the following details:

- **Logging Services** area - Select the logging level for each of the communication protocols. Options include:
  - **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.

- **Write Preferences changes to system log** - This check box needs to be checked if you want to keep logging level changes in the system log table.

- **Auto Archiving Log Services** area - Configure the size of the system log table and warning message frequency:
  - **Maximum Line Count** - Set the number of records allowed before archiving occurs; valid values are from 500000 to 10000000, the default value is 10000000).
  - **Number of Log Entries to Truncate** - Define the number of records to be archived; valid values depend upon the maximum line count configured; if the maximum line count value is 5000, valid values for log entries to truncate are from 500 to 4999. If the maximum line count is set to 10000000, the valid values for log entries to truncate are from 500 - 999999).
NOTE: Auto Archiving is the process by which the System Log Table in the WDM Database is automatically archived to prevent performance degradation due to an extremely large number of records. Auto Archive checks the database in two minute intervals, using the criteria provided in Logging Preferences, to determine whether or not an archive is needed. Archives are stored as syslogtable-DD-MM-YYYY.txt in the root directory of WDM. It is your responsibility to manage these files. It is recommended that you delete or move the syslogtable-DD-MM-YYYY.txt files to preserve drive space.

NOTE: The value for the Number of Log Entries to Truncate is always less than the value for the Maximum Line Count in SystemLog Table.

- Log Archive Warning message on every - Edit the time interval for displaying the circular logging warning message. The default interval is every 5 hours. When the value you set for the Maximum Line Count in SystemLog Table is exceeded, the "Archive Logs" warning message appears. The first time the line count exceeds the configured limit, a warning message appears immediately. If you select OK, the Archive Record window appears. If you select Cancel, you will see the warning again at the next configured warning message interval. (See Figures 86 and 88.)

- Click OK to display the System Log Archive window.

- Use the radio buttons and drop-down menus to select the logs to be archived and the output file format and destination.

2. Click Logging Details in the Logging Levels tree to launch the Logging Details Preferences window.
3. Select the details you want to log.

**NOTE:** Category Status Changes refers to whether a package changed from one category to another. For example, if you edit the script file for a package and change it from Image to Client Configuration, while Package Status Changes refers to whether a package changes from active to inactive or inactive to active.

### Service Preferences

Select **Service Preferences** in the preference list and double-click to launch the **Service Preferences** window where you can select global preferences for repository communication. The service preference settings determine the protocol that is used to communicate with a repository during Package Registration, Package Deletion, Remote Repository Synchronization, and Package Updates for client devices.
1. Specify the following details:

- **Time Out Preferences** area - Set the **Connect (Millisecs)** (number of milliseconds in which WDM attempts to connect to a device, whether through the Web Service or the Standard Service, before timing out) and the **Discovery (Secs)** (maximum time allotment for WDM to discover all of the devices in your network).

- **Wake On LAN Preferences** area - 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 on.

- **Repository Preferences** - You can select any or FTP, HTTP, and CIFS transfer type in repository preferences depending on your requirement.

2. Select **Enable ThreadX Service Polling** to poll the Thread X services if you are managing PCoIP devices.

3. Select **Enable WDM Service Logs** to log and view the WDM Service details.

4. Click **Serv/Port Settings** in the Service tree to open the **Service Preferences** dialog box.
5. Specify the following details:

- **Port Preferences**
  - **GUI Listening Port** - The port through which the Web Service listens for incoming WDM Agent requests.
  - **Alternate GUI Listening Port Range** —
  - **Standard Service Listening Port** - The port through which the Standard Services listens for device check-in activity.
  - **Web Service HTTP Port** - The port WDM uses to issue real-time commands (such as Quick Device Commands or device updates at a specific time). Normally this is port 80. Note that you can change this port only through your Web Server.
  - **Web Service HTTPS Port** - (Wyse Device Manager Enterprise Edition only) The port WDM uses to issue real-time commands (such as Quick Device Commands or device updates at a specific time). Normally this is port 443. Note that you can change this port only through your Web Server.
  - **ThreadX Service Port** -

6. **Use Alias Name**: When checked, the WDM Management Agent uses the Host Name to connect to the server.

- **Alias Server Host Name** - Server Host name will have a default value of the Host machine. You can change this value to a different host name. In case of load balancing where you configure a Proxy Server to route the requests from managed devices to multiple Management Servers, you can enter the host name of the Proxy Server. For more information, see the *Dell Wyse Device Manager Installation Guide*.
DHCP/TFTP Preferences

Select **DHCP/TFTP Preferences** in the preference list to launch the **DHCP/TFTP Preferences** dialog box.

**Specify the following details:**

- **DHCP Proxy Preferences** area:
  - **Start DHCP Proxy** - Select to allow WDM to serve as a Dynamic Host Configuration Protocol (DHCP) proxy.
  - **Enable DHCP Options for HTTP Discovery** - Select to allow the Web Service to use DHCP when discovering devices.

- **TFTP Server Preferences** area:
  - **Start TFTP** - Select to allow WDM to use Trivial File Transfer Protocol (TFTP) when updating devices.
  - **TFTP Master 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 (Secs.)** - Specify the length of time (in seconds) that WDM waits for a connection to the TFTP service before attempting to reconnect.
  - **TFTP Retries** - Specify the number of times that WDM will attempt to connect to the TFTP service before failing.
Scheduling Preferences

Select Scheduling Preferences in the preference list to launch the Scheduling Preferences window.

Specify the following details:

- **General Scheduling Preferences area:**
  - **Max. Web Service Simultaneous Updates** - Specify the number of updates that WDM can perform concurrently to devices with WDM Agents.
  - **Schedule(s) / Page** - Select the number of scheduled packages to display on the Scheduled Packages page.
  - **Time Zone for Scheduled Updates** - 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** —
  - **Default Query User Time Out (Secs.)** - The length of time that the user options will be displayed before the script proceeds without user input.
PM, then the update starts at the following local times at each location: 1:00 PM at the Console, 2:00 PM at the Database, and 3:00 PM at the device.

- **Time bound rollout** - This is the check box to enable and disable the garbage collector feature for scheduled updates. If this field is checked then depending on the below two fields settings the scheduled updates will go into error, otherwise they will remain in scheduled state and will never go into error state.

  - *Global Schedule Time-out (Minutes)* - The time period after which all the outstanding scheduled updates will be moved to error state.
  - *Client Response Time-out (Minutes)* - The time period for which WDM server will wait for the client to check in after WDM has successfully sent the notification to the client.

- **Auto-sync Remote Repositories** - (WDM Enterprise Edition only) Select to enable WDM to determine if Remote Repositories should be synchronized before performing an update to devices served by a Remote Repository.

- **Enable Next Boot** - Select to allow WDM to update devices after their next reboot.

- **Rescheduling Failed Packages** area:
  - *Max. Retry Count* - Specify the number of retries you want if package deployment fails.

- **Delayed Updates (Linux only)**

- **Imaging Option** - There are two ways to image a device:
  - **Wisard** - This is the legacy method for imaging devices which requires PXE for imaging.
  - **Merlin** - This option enables HTTP and HTTPS-based imaging for the devices.
  - **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 (100 MBPS Full duplex), 100M-H (100 MBPS Half duplex).

### Subnet Preferences

Select **Subnet Preferences** in the preference list and double-click to launch the **Subnet Preferences** window.
Use the following guidelines:

**Subnet Hierarchy Section**

- **Show Subnet Hierarchy** - (WDM Enterprise Edition only) Select to allow any subnet views to include the hierarchical view of the subnet.
- **Show Subnet Description in Hierarchy** - (WDM Enterprise Edition only) Select to display hierarchical subnet views by the descriptions of the subnets rather than by their address. Note that the default description is always the subnet IP.
- **Subnet Hierarchy Start Level** - Specify the starting level for displaying subnet hierarchies. A level refers to one of the four octets in the subnet address.
- **Subnet Hierarchy End Level** - Specify the ending level for displaying subnet hierarchies. A level refers to one of the four octets in the subnet address.

**Peer Assisted Deployment Section**

- **Required minimum number of devices that can support peer capable repository** - Select either One or Two to indicate the number of peer capable repositories.
- **Maximum number of simultaneous connections: (1-7)** - This indicates the total number of devices that can be updated using peer repository or maximum number of simultaneous connections to master device. The default value for simultaneous connection is seven.
- **Configure Repository Details**: - Click the button next to Configure Repository Details. The **Configure Peer Assisted Deployment** screen is displayed.
Specify the Repository Details for the following options:

- **SUSE Linux** — specify the User Name, Password, and the relative path of the WDM server.
- **Windows Embedded Standard 7** — specify the User Name, Password, and the HTTP Port Number for the peer device to download image from the PAD master repository device.

### WTOS Preferences

Select **WTOS Preferences** in the preference list to launch the **WTOS Preferences** window.

#### WTOS Preferences

- **WTOS INI path upon checkin (FTP/HTTP/HTTPS/CIFS)**
- **WTOS Root Path**: WTOS\CONFIG

Specify the following details:

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

### Secure Communication (HTTPS)

Beginning with WDM Release 4.7, there is support for secure HTTPS communication between components of WDM.
The secure communication can be initiated in two ways:

- HTTPS Communication Initiated by HAgent.
- HTTPS Communication Initiated by WDM GUI.

**HTTPS Communication Initiated by HAgent**

The HAgent can initiate communication with the HServer during client device startup. When the HAgent on a client boots up, it requests the following information from the DHCP server or proxy server:

- Server IP address.
- HTTPS port number used for communication.

If the HAgent cannot retrieve the HTTPS Port number from the DHCP option tags, it follows the sequence below:

- The HAgent tries to communicate via HTTPS using ports 443 and 8443.
- If the HAgent cannot communicate via HTTPS, it tries to connect via HTTP using ports 80 and 280.
- If the HAgent successfully initiates communication with the HServer, it caches the communication mechanism, IP address, and port number used and uses that information for any subsequent requests.
- If HTTPS communication fails during startup, the HAgent will not try the HTTPS protocol again.

**NOTE:** For devices using WDM releases earlier than WDM 4.7, the HAgents can initiate communications with the HServer via HTTP, if that protocol is enabled on IIS. If you disable HTTP communications via the IIS settings to enhance security, the HAgents cannot communicate with the HServer.

**HTTPS Communication Initiated by WDM GUI**

You can configure your network to allow the GUI to determine the port number and protocol to use for communication with the HServer.

**Determining the Port Number** - To allow the GUI to determine the port number for communication, follow these steps:

- Configure the IIS that hosts the HServer with the desired port number.
- Stop the IIS and WWW service.
- Start the HServerInit service.

When the WDM GUI starts up, it queries the database to retrieve the port number and IP address to use for communication with the HServer.

**Determining the Protocol** - To allow the GUI to determine the protocol for communication, follow these steps:

- Bind the IIS that hosts the HServer with a TCP, SSL, or TCP and SSL port.
  
  **NOTE:** For an SSL port, you must install a certificate.

- Stop the IIS and WWW service.
- Start the HServerInit service.

The port number and IP address are stored in the WDM Database. If the request came via SSL, the entire WDM configuration is set to secure.
No configuration is required in the WDM GUI, but the Secure Communications check box is displayed in the Port Settings preferences dialog box for information purposes.

If an SSL port is configured on IIS, the Secure Communications check box will be checked, otherwise it will be unchecked.

Before starting secure communication, make sure all the settings are configured for secured communication.

**NOTE:** The secure communications flag applies to both remote and master repositories.

### Upgrading Older WDM Agents Selectively

Before upgrading selectively, you should have configured WDM with subnet and/or IP range information (see [Configuring WDM Preferences and Settings](#)), understand the WDM architecture, have discovered the devices you wish to upgrade (see [Discovering Devices](#)), ensure that the Auto-Agent Upgrade feature is turned off in the Device Manager Preferences (see [Using the Auto-Agent Upgrade Feature to Automatically Upgrade WDM Agents](#)).

Use the following guidelines to selectively upgrade older WDM Agents (formally Rapport Agents) to the new HTTP-based WDM Agent:

1. Switch to an Update Manager view that identifies the device or devices whose WDM Agents you want to upgrade to the new WDM Agent.
   
   **NOTE:** You can distribute the WDM Agent package to multiple devices simultaneously by isolating the devices into one group. To isolate a group of devices, you can discover devices using a specific subnet or an IP range (see [Discovering Devices](#)). You can also create a Device View of devices by subnet, OS, or any other functional group (see [Creating Device Views](#)).

2. Expand **Package Manager**, and select the **Agent Updates** folder to view the results pane showing all the packages contained in the Agent Updates folder.

3. Drag the WDM Agent package and drop it onto the Device Manager icon in the WDM Console tree pane (or onto a device group in the Device Manager) to open the Software Distribution Wizard.

4. Select the devices with the WDM Agents you want to upgrade and click **Next**.

   **NOTE:** Selected devices must match the OS of the WDM Agent software update package. Scroll to the right to determine the device OS (under the OS column) and use SHIFT or CTRL to select multiple devices. If you dropped the software package onto a device group, only the devices in that group are displayed.

5. Select and configure the distribution option you want for the WDM Agent upgrade and click **Next**.

6. After the wizard informs you that it is ready to create the update, click **Create**.

7. When the wizard finishes creating the update, click **Finish**.

   **NOTE:** For information on editing or deleting a scheduled update, refer to [Editing Scheduled Device Updates](#) or [Deleting Scheduled Device Updates](#).

### Using WDM Device Security

WDM allows you to set a Device Manager preference that prevents unauthorized WDM installations from managing your devices. When the **Enable Device Security** option is set, the WDM Agent and the WDM Web Service enter into a one-to-one relationship. In this relationship, both the device and the Web Service share a unique security certificate in common. Before processing any WDM requests, the WDM
Agent on the device verifies the certificate. If the Web Service certificate matches its own, the WDM Agent allows the device to perform the requested functions or instructions. If the certificates do not match, the WDM Agent prevents the device from complying with any of the requests.

**NOTE:** Device security can only be enabled only with an WDM Enterprise Edition Sales Key.

**CAUTION:**

**When Enabling Device Security** - If you decide to enable device security, be sure to write down your certificate number and keep it in a safe place. If your WDM installation becomes corrupt for any reason, and you must reinstall WDM, you will get a new certificate number. Without the original certificate number, however, you will not be able to manage your devices. WDM gives you the option of either changing a security certificate to a new one, or restoring an older certificate.

**When Disabling Device Security** - If you decide to disable device security, existing devices will not release their security certificate until their next check-in. They cannot be refreshed or rediscovered because the server no longer presents a certificate. They must check-in on their interval (that is, pull not push).

To enable device security:

1. In the WDM Console tree pane, expand the Configuration Manager and select Preferences to view the results pane showing the categories for the WDM Preferences.
2. Double-click Device Manager Preferences to open the Device Manager Preferences dialog box.
3. Select Enable Device Security and click OK.
4. Click Yes to confirm.

From this point forward, if a device does not already possess a security certificate, then the next time the device is discovered or checks-in, WDM will establish the one-to-one relationship between the WDM Agent of the device and the WDM installation. This relationship prevents unauthorized WDM installations from managing the devices.

**NOTE:** When you enforce device security, WDM automatically encrypts all communications between the Web Service and the WDM Agents. However, encryption can be turned on independently of device security (see Service Preferences).

### 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.

Note 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. The user IDs and passwords for all repositories can be the same.
- 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:
• 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 tree pane, expand Configuration Manager, right-click Repositories and select New →Repository.

2. Complete the configurations using the following guidelines:

   • **Repository Information area:**
     - **Name** - Provide the name to identify the Software Repository.
     - **Location** - Use the IP address to identify the Software Repository.
     - **Relative Path** - Displays the home account information of the user specified in the repository.

   • **FTP area:**
     - **User/Group Name** - User or group name for FTP repository access.
     - **Password** - Password for FTP repository access.
     - **Verification** - Confirm the password for FTP repository access.
     - **Bandwidth** - How much bandwidth in Kbps to utilize for data transfer to and from the Software Repository.

Note: Specifying a repository using this dialog does not actually install a new Software Repository. You must install new repositories with the WDM CD.
- **Session Timeout** - Time in seconds that the connection for each session should remain open.
- **Port Number** - Displays the port number for FTP communication. The default port number for FTP is 21.

Click the **HTTP** tab and fill the following details:

### Repository Information

| Name:       | Location: 10.150.116.25 | Relative Path: /rapport |

*Note: Specifying a repository using this dialog does not actually install a new Software Repository. You must install new repositories with the WDM CD.*

### HTTP tab

- **User/Group Name** - Not required for HTTP-based communication.
- **Context** - Displays the virtual directory path for HTTP communication. This field is disabled if the selected transfer type is FTP only.
- **Password** - Not required for HTTP-based communication.
- **Timeout** - Time in seconds that the connection for each session should remain open.
- **Port Number** - Displays the port number for HTTP communication. The default port number for HTTP is 80, and for HTTPS is 443.
- **Verification** - Not required for HTTP-based communication.
- **Secure (HTTPS)** - If checked, the HTTP communication for the repository is secure.
- **Validate Certificate with CA** - If checked, the Certificate validation for HTTPS communication is enabled.

- **HTTP area:**
  - **User/Group Name** - Not required for HTTP-based communication.
  - **Context** - Displays the virtual directory path for HTTP communication. This field is disabled if the selected transfer type is FTP only.
  - **Password** - Not required for HTTP-based communication.
  - **Timeout** - Time in seconds that the connection for each session should remain open.
  - **Port Number** - Displays the port number for HTTP communication. The default port number for HTTP is 80, and for HTTPS is 443.
  - **Verification** - Not required for HTTP-based communication.
  - **Secure (HTTPS)** - If checked, the HTTP communication for the repository is secure.
  - **Validate Certificate with CA** - If checked, the Certificate validation for HTTPS communication is enabled.
– **Read Only** - If checked, the repository will be read only.

Click the CIFS tab and fill the following details:

![Software Repository dialog box](image)

- **CIFS area:**
  - **Domain/Host Name** - Give the domain or host name of the repository server.
  - **User Name** - Give the user name that has access to the shared folder.
  - **Share Name** - Give the name of the shared folder from where package needs to be deployed.
  - **Password** - Password for CIFS user that has access to the shared folder.
  - **Verification** - Confirm the password for CIFS user that has access to the shared folder.

3. Click **OK**.

**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 right-clicking the Remote Repository name and selecting **Test 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.
Software Repositories List

To edit or modify an existing repository, follow these steps:

1. Display the list of repositories. In the left pane of the WDM Administrator Console, navigate to WyseDeviceManager → Configuration Manager → Software Repositories.
2. Double click any repository in the list, software repository window is displayed. In the Software Repository Window you can make any desired changes.

- To change to FTP protocol, specify the following details:
  - **User/Group Name** - User or group name for FTP repository access.
  - **Password** - Password for FTP repository access.
  - **Verification** - Confirm the password for FTP repository access.
  - **Bandwidth** - How much bandwidth in Kbps to utilize for data transfer to and from the Software Repository.
  - **Session Timeout** - Time in seconds that the connection for each session should remain open.
  - **Port Number** - Displays the port number for FTP communication. The default port number for FTP is 21

- To change to HTTP/HTTPs protocol, specify the following details:
  - **User/Group Name** - Not required for HTTP-based communication.
  - **Context** - Displays the virtual directory path for HTTP communication. This field is disabled if the selected transfer type is FTP only.
  - **Password** - Not required for HTTP-based communication.
  - **Timeout** - Time in seconds that the connection for each session should remain open.
  - **Port Number** - Displays the port number for HTTP communication. The default port number for HTTP is 80, and for HTTPS is 443.
  - **Verification** - Not required for HTTP-based communication.
  - **Secure (HTTPS)** - If checked, the HTTP communication for the repository is secure.
  - **Validate Certificate with CA** - If checked, the Certificate validation for HTTPS communication is enabled.
  - **Read Only** - If checked, the the repository will be read only.

- To change to CIFS protocol, specify the following details:
  - **Domain/Host Name** - Give the domain or host name of the repository server.
  - **User Name** - Give the user name that has access to the shared folder.
  - **Share Name** - Give the name of the shared folder from where package needs to be deployed.
  - **Password** - Password for CIFS user that has access to the shared folder.
  - **Verification** - Confirm the password for CIFS user that has access to the shared folder.

Assigning Software Repositories to a Subnet

To assign software repositories with any supported protocol to a subnet, follow these steps:
In the WDM Administrator Console, navigate to **WyseDeviceManager → Configuration Manager → Networks → Subnets**.

Double click a subnet in the list to modify an existing subnet. To create a new subnet, click **New** in the context menu. The Subnet window is displayed.

Software Repository Service Preferences

From the Service Preferences dialog box you can choose FTP, HTTP, HTTPS, CIFS for repository preferences. The selected repository preference indicates the protocol a repository uses to deploy a package. These preferences can be set globally, following these steps:

- Double-click **Service Preferences** in the preference list to open the Service Preferences dialog box where you can select global preferences for repository communication. The service preference settings will determine the protocol that is used to communicate with a repository during Package Registration, Package Deletion, Remote Repository Synchronization and Package Updates for Client Devices. For more information, see **Service Preferences**.
Network Configuration

You can configure network settings in the Configuration Manager to enable you to manage devices across subnets and across IP ranges.

WDM uses the subnet information to discover and communicate with the devices on the subnet. You can add and configure subnets manually, or you can import subnet data from comma-delimited and tab-delimited files into the Database. For more information, see Setting Subnets Manually and Importing Subnet Data from Files.

IP Ranges allow WDM to discover devices with all supported versions of WDM agents through a Transmission Control Protocol (TCP) connection to each device in an IP range rather than through a User Datagram Protocol (UDP) broadcast to an entire subnet level. You can add and configure IP ranges manually or you can import IP range data from comma-delimited and tab-delimited files into the Database. For more information, see Setting IP Ranges Manually and Importing IP Range Data from Files.

Setting Subnets Manually

With WDM, you can add and configure subnets manually.

To add and configure a subnet:

1. In the WDM Console tree pane, expand Configuration Manager and Networks.
2. Right-click Subnets and select New | Subnet.
3. Complete one of the following:
   
   - 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 **# of Contiguous Bits** (if your network uses Classless Inter-Domain Routing or supernetting, type the number of contiguous bits to configure your subnet mask).

4. If your WDM configuration includes multiple Remote Repositories and you want to associate the subnet with one of them, select the **Subnet Repository**.

   **NOTE**: When distributing packages to a group of devices, WDM uses the subnet/repository association to determine the appropriate Remote Repository for the devices.

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

6. (Optional) If you want to associate newly discovered devices on this subnet with a user-defined Group Type and Group (WDM always assigns devices to the predefined group types according to the values found on the devices), select the row for the Group Type you want from the Default Groups pane, select the **Default Value** in the Default Group Value dialog box and click **OK** to return to the Subnet dialog box. Be aware that to associate devices in a subnet with a group type and group, you must have previously created the desired group types and groups.

7. Complete one of the following:
   
   - 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.
  – **Wake On LAN Retries** - The number of times WDM attempts to wake a device in the subnet before stopping.
  – **TFTP Time Out (Secs.)** - The length of time WDM attempts to use the Trivial File Transfer Protocol to communicate with devices during PXE operations.
  – **TFTP Retries** - The number of times WDM attempts to use TFTP 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.

**Setting IP Ranges Manually**

With WDM, you can add and configure IP ranges manually.

To add and configure an IP range:

• In the WDM Console tree pane, expand **Configuration Manager** and **Networks**.
• Right-click **IP Ranges** and select **New | IP Range**.
• Complete the configurations using the following guidelines:
  
  – **Start IP Address** - The starting IP address for the IP Range.
  – **End IP Address** - The ending IP address for the IP Range.
  – **Exclude From** - The beginning IP address for the range of addresses to exclude from the range you are setting up (for example if you wanted to exclude device between .30 and .35 then you would enter 192.168.1.30).
  – **Exclude To** - The ending IP address for the range of addresses to exclude from the range you are setting up (for example if you wanted to exclude device between .30 and .35 then you would enter 192.168.1.35).
  – **Description** - Type a brief description to identify the IP Range.

• Click **Add** to store information about the IP Range in the WDM Database. WDM can now selectively discover devices in a subnet through a TCP connection to each device.

### User Management

As an administrator you can add, edit and delete WDM users. WDM allows you to manage users from local computer accounts or from Active Directory. You can also use advanced Device View Configuration options (User Security and Filter Criteria) for distributed user and device administration.
Expand the **Configuration Manager** node in the tree view of the WDM Console. Select **User Permissions** to view the list of users created.

You can perform the following operations under user management:

- Add users from Local Computer Accounts. See Adding Users from Local Computer Accounts.
- Add users and groups from Active Directory. See Adding Users and Groups from Active Directory.
- Edit user permissions. See Editing User Permissions.
- Delete users. See Deleting Users.

### Adding Users from Local Computer Accounts

As an administrator you can add WDM users from local computer 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 tree pane, expand **Configuration Manager**, right-click **User Permissions**, and select New | User to open the Pick a user dialog box.
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 as described in Editing 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 tree pane, expand **Configuration Manager**, click **User Permissions**, and then click the Active Directory Search tab.
2. Select the **Global Catalog** option if you want to add a user from the global address book. 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 Find A Specific User, 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:** You cannot edit your own user permissions.
To edit user permissions:

1. In the WDM Console tree pane, expand **Configuration Manager**, and click **User Permissions** to view the list of WDM users.
2. Double-click the user you want from the list of users to open the User Permissions dialog box.

3. Select the user permissions you want for the user and click **OK**.

   **NOTE:** If you select the **Administrator** check box, all permissions are selected.

**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 tree pane, expand **Configuration Manager** and click **User Permissions** to view the list of WDM users.
2. Right-click the user you want from the list of users, and select **Delete**.
3. Click **Yes** to confirm the deletion.

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

## Utilities

WDM provides many utilities that enable you to perform many additional functions such as importing data, importing device settings, viewing and modifying database credentials, creating a management console self extractor, and perform a bulk deployment of WDM Images.

You can access some of the utilities from **WDM Console → Configuration Manager → Utilities** or from **Start → All Programs → Wyse Device Manager 5.0 → Utilities**.

For more information, see:

- [Importing Data into the Database](#)
- [Importing Device Settings from Files](#)
- [Database Credential Manager](#)
- [Management Console Extractor](#)
- [WDM Imaging Tool](#)
- [High Availability Configuration Utility](#)
- [DNS-DHCP Lookup Utility](#)

## Importing Data

With Wyse Device Manager you can import data from comma-delimited and tab-delimited files into the Database. You can use the Import Utility or the Device Import Utility to import data.

Expand the **Configuration Manager** node in the tree view of the WDM Console and select **Utilities** → **Import** to launch the **Import Utility**. You can use this utility to import:

- IP Range Data. See, [Importing IP Range Data from Files](#).
- Subnet Data. See, [Importing Subnet Data from Files](#).
- Software Repository Data. See, [Importing Software Repository Data](#).

To import device settings from files, expand the Configuration Manager node and select **Utilities** → **Import Device Settings**. For more information, see [Importing Device Settings from Files](#).

## Importing IP Range Data from Files

With WDM, you can import IP range data from comma-delimited and tab-delimited files into the Database.

1. The following example shows the required format for IP range flat files:
   
<table>
<thead>
<tr>
<th>StartIP, EndIP, ExclusionStartIP, ExclusionEndIP, Description</th>
</tr>
</thead>
</table>

   - **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** = Name of IP range that will appear in GUI

**Example:** My IP Range, 10.10.10.10, 10.10.10.200, 10.10.10.20, 10.10.10.30

2. This IP Range definition will be added to the database to allow for IP Range walking discover on and 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 will show up in the WDM GUI as *My IP Range*.

3. To import IP Range data:
   - In the WDM Console tree pane, expand **Configuration Manager** and **Utilities**.
   - Right-click **Imports** and select New | Import.

   ![Import Utility](image)

   - Select the **IP Ranges** option, and enter (or browse for) the location of the data file in the Import Path and Filename box.
   - Click **OK** to import the IP Range data into the WDM Database (you can select the IP Range node under the Configuration Manager node to view the newly imported IP Ranges).

**Importing Subnet Data from Files**

With WDM, you can import subnet data from comma-delimited and tab-delimited files into the Database.

**NOTE:** Your WDM Database must contain information about at least one Master Repository before you can work with subnets.

1. The following example shows the required format for subnet flat files:
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** = Broadcast address; example 10.10.10.255
- **Description** = Name of Subnet that will appear in GUI
- **SW Repository** = Name of a Software Repository. You can not add a Subnet without a Software Repository. The name of the master Repository ID is MASTER.
- **Override Default Parameters** = Override Global Preferences (Enterprise Only)
- **IP Address** = Valid IP address in subnet; example 199.199.10.2
- **Subnet Mask** = Subnet mask; example 255.255.255.0
- **Max. Web Service Simultaneous Updates** = Maximum Simultaneous Updates; example 5
- **Wake On LAN Time Out(Secs.)** = Time Out for Wake On LAN; example 2
- **Wake On LAN Tries** = WOL Retry; example 3
- **TFTP Time Out(Secs.)** = TFTP Timeout; example 10
- **TFTP Retries** = TFTP Retries; example 3
- **Network Card Speed** = Network Card Speed; example 1 (for Auto), 2(for 100M-F), 3(for 100M-H)

Example: 10.10.10.255, Subnet1, MASTER, False, 199.199.10.2, 255.255.255.0, 6, 2, 1, 1, 7, 2

This will add to the database a subnet definition that will discover and manage devices on a class C subnet with IP address assignments from 199.10.0.1 to 199.10.0.254. The column header either doesn’t exist or exists in the above proper order.

2. To import Subnet data:
   - In the WDM Console tree pane, expand **Configuration Manager** and **Utilities**.
   - Right-click **Imports** and select **New → Import**.

 ![Import Utility](image)
• Select the **Subnets** option, and enter (or browse for) the location of the data file in the Import Path and Filename box.

• Click **OK** to import the subnet data into the WDM Database (you can select the Subnets node under the Configuration Manager node to view the newly imported subnets).

**Importing Software Repository Data**

The following example shows the required format for Software Repository Flat Files:

Name of Rep, 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, IsHTTPS Secure, HTTPS Validate With CA, Remote Server Name, CIFS Username, CIFS Password

- **Name** = Name of the Software Repository as it appears in the GUI
- **Location** = IP address of the FTP server
- **Transfer Type** = Type of transfer protocol that is in use. It can be FTP or HTTP or Both.
- **Relative Path** = Path to the Software Repository relative to the root directory. The default value for this is /rapport.
- **Context** = This is valid for HTTP communication and is the name of Virtual Directory. By default HTTP context is MyWDM.
- **FTP Port Number** = Port number for FTP communication. By default it is 21.
- **HTTP Port Number** = Port number for HTTP/HTTPS communication. By default it is 80 for HTTP and 443 for HTTPS communication.
- **FTP User Name** = User name for the FTP account as set up by IIS FTP or the FTP service that you use to connect the repository.
- **FTP Password** = Password for the FTP account as set up by IIS FTP or the FTP service that you use to connect the repository.
- **HTTP User Name** = User name for the HTTP account as set up by IIS HTTP or the HTTP service that you use to connect the repository.
- **HTTP Password** = Password for the HTTP account as set up by IIS HTTP or the HTTP service that you use to connect the repository.
- **Secure(HTTPS)** = It is -1 if Secure is checked(HTTPS supported) and 0 if Secure is unchecked (HTTP is supported not HTTPS).
- **HTTPS Validate With CA** = It is -1 if ‘Validate Certificate with CA’ is checked and 0 if unchecked.

**Example where 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 Transfer Type is HTTP**: RemoteHTTP, 10.10.11.9, HTTP, /rapport, MyWDM,, 80,, HTTPUserName, HTTPPassword, 0, 0

**Example where Transfer Type is FTP**: RemoteFTP, 10.10.11.9, FTP, /rapport, MyWDM,, 21, FTPUserName, FTPPassword, 0, 0

**Example where Transfer Type is CIFS**: RemoteCIFS, 10.150.112.3, SMB, /rapport, MyWDM,, 0, 0, RemoteServerName, CIFSUsername, CIFSPassword
Example where Transfer Type is FTP, HTTP, and CIFS: FTPHTTPandCIFS,10.150.112.3,HTTP and FTP and SMB,/Rapport,MyWDM,21,80,FTAccess,FTPass,HttpAccess,HttpPass,0,0,RemoteServerName,CIFSusername,CIFSpassword

Example where Transfer Type is FTP, HTTPS, and CIFS: FTPHTTPSandCIFS,10.150.112.7,HTTP and FTP and SMB,/Rapport,MYWDM,21,443,FTPAccess,FTPass,HttpAccess,HttpPass,-1,0,RemoteServerName,CIFSUserName,CIFSPassword

This Software Repository definition will be added to the database to define a repository on a server at 10.10.11.9 where the FTP service’s root directory is the default path of /rapport. This repository will be accessed using a username of user. It will use FTP as the transfer protocol and show up in the Wyse Device Manager GUI as Remote.

The column header either doesn’t exist or exists in the above proper order.

To import Software Repository data:

1. In the Wyse Device Manager MMC Snap-in Tree panel, expand **Configuration Manager** and **Utilities**.
2. Right-click **Imports** and select **New | Import**.

   ![Import Utility Image]

3. Select the **Software Repository** option, and enter (or browse for) the location of the data file in the Import Path and Filename box.
4. Click **OK** to import the Software Repository data into the Wyse Device Manager Database (you can select the Software Repository node under the Configuration Manager to view the newly imported remote software repositories).
NOTE: When you register a new Software Repository, Wyse Device Manager establishes a connection to ensure that it can communicate with the remote repository. When you import repository data, Wyse Device Manager tests the connection to the repository automatically. Therefore, after you import one or more remote repositories, you do not need to test connection.

**Importing Device Settings from Files**

With Wyse Device Manager, you can import Device Settings data from comma-delimited and tab-delimited files into the Database. The following example shows the required format for Device Settings Flat Files:

Client Name, Mac address, Platform, Custom field 1, Custom field 2, Custom field 3, Contact, Location

- **Client Name** = Name of the Device; example W1009341019
- **Mac address** = MAC address of the Device; example 0080646A1144
- **Platform** = Platform of the Device; example VX0
- **Custom field 1** = Custom field of the specific Device
- **Custom field 2** = Custom field of the specific Device
- **Custom field 3** = Custom field of the specific Device
- **Contact** = Contact information of the Device
- **Location** = Location of the Device
- **OS** = Operating System of the device. This field is applicable only to devices with the new Dell naming scheme. The list of OS codes are as follows:
  - Wyse Xenith - XEN
  - WTOS - BL
  - WTOS PCoIP - BLP
  - PCoIP (ThreadX) - TDC
  - SUSE Linux - SLX
  - Dell Wyse Enhanced Ubuntu Linux 12.04 - UBN12
  - Red Hat Linux 6.x, 7.x and 8.x - RLX
  - Windows XP - XP
  - Windows Embedded Standard - WES
  - Windows Embedded Standard 7 - WES7
  - WE8Sx Windows Embedded 8 Standard 32 - WE8Sx
  - Windows Embedded 8 Standard 64 - WE8SEmbedded 8 Standard 64 - WE8S

The following example shows the required format for Device Settings Flat Files:

ClientName;MACAddress;Platform;Custom1;Custom2;Custom3;Contact;Location

W1009341019;0080646A1144;V90;ABCD;EFGH;IJKL;Administrator;San Jose Office

To import Device Settings:

1. In the select **Configuration Manager** in the tree pane of the WDM Console, and under **Utilities** select **Import Device Settings**.
2. Right-click and select **New → Device Import**.
   The **Device Import Utility** is launched.

   ![Device Import Utility](image)

   - Click **Browse** to select the file containing the device details OR enter the full path and filename in the field provided. (e.g. C:\Program Files\Wyse\WDM\ImportClients.txt)

3. Enter (or browse for) the location of the data file in the Import Path and Filename box.
4. Click **OK** to import the Device Settings into the Wyse Device Manager Database.

### Database Credential Manager

The **Database Credential Manager** is a utility that enables you to view the details of the WDM database and also create new credentials to access the database.

You can access this utility in two ways. To access and use the tool:

1. Expand the **Configuration Manager** node in the tree panel of the WDM Console and select **Utilities → Database Credential Manager**. You can also access this from **Start → All Programs → Wyse Device Manager 5.0 → Utilities → DatabaseCredentialManager.exe**.

   The utility displays the following information:
   - **Server: Port** — The IP address of the WDM database server and the database server port number.
   - **Name** — The name of the WDM database.
   - **User** — 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 **Save and Close** if you have entered new credentials, or click **Cancel** to close the window if you have not entered any new credentials.

### Management Console Extractor

The Management Console Extractor also known as the Remote GUI Extractor provides a quick and easy method of deploying the WDM Management Console to remote computers. You can run multiple instances of the WDM Console on different systems at any given point.

You can use the Management Console Extractor to create an installer package that contains only the WDM Console component and deploy it on different systems.

To create an installer package:

1. Launch the Management Console Extractor from **Start → All Programs → Wyse Device Manager 5.0 → Utilities → MgmtConsoleExtract.exe**

2. Enter the **Install path on destination** or click the button to browse to the folder location. This is the path where the WDM Console components are installed when you run the extractor on a system.

3. Enter the path where you want to save the extractor in the **Save extractor to:** field.

4. Click **Create**. The extractor **MgmtConsoleZip** is created in the location you specified.

5. Copy the **MgmtConsoleZip** file to the system where you want to install the WDM Console and double click the file to extract the WDM Console components.

### WDM Imaging Tool

The WDM Imaging Tool is a mass imaging tool. You can deploy an image to multiple devices in the same platform by using this tool. You can create a schedule to deploy the image to the discovered devices.

When you launch the tool, it displays the image packages you have registered. For more information on registering images, see [Register an Image from a Device (Requires PXE)](#). You can also register image packages in the tool.

To use the WDM Imaging Tool:

1. Launch the WDM Imaging Tool from **Start → All Programs → Wyse Device Manager 5.0 → Utilities → WDMImaging**.

   The tool displays the image packages that you have registered. If there are no packages, then you can register image packages.

2. To register packages from the tool, click **Register**.

   The Package Registration Wizard is displayed.

3. Browse to the location of the .rsp file, select it and click **Next**.

   The **Image Registration** screen is displayed.

4. Enter the name, description, and category of the package and click **Register**.

5. Click **OK** when registration is complete. The image is displayed on the WDM Imaging Tool.
6. Click **Unregister** to delete a registered package from WDM.
7. Click **Add Schedule** to create a deployment schedule for all the devices to which you want to deploy the image package.
   
   The schedule is displayed on the WDM Console under **Update Manager**.
8. Click **Remove Schedule** to remove the schedule from WDM.
9. Click **Close** to close the tool.

**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.

To configure the cluster information:

1. Launch the High Availability Configuration Utility from **Start** → **All Programs** → **Dell Wyse Device Manager** → **Utilities**.
2. Enter the following details:
   - **Configure Setup As** – select **Cluster** from the drop-down list.
   - **Database Name** – this is displayed by default and cannot be edited.
   - **Database Server** – Specify the hostname of the database cluster.
   - **Database User Name** – Specify **rapport** as the database user.
   - **Database Password** – Specify the password of the rapport user.
3. Click **Configure**.
   
The connection details are displayed on the bottom pane of the utility.

**DNS-DHCP Lookup Utility**

This utility enables you to find out the method that has been configured in the network to discover WDM by the client.

You can run this utility from **Start** → **All Programs** → **Wyse Device Manager** → **Utilities** → **DNS_DHCP_Lookup.exe**

**Viewing the Diagnostic Report**

The Diagnostic Report provides hardware and software summary information as well as a list of running processes. The Diagnostic Report has seven sections:

- **Software Repository Information** = Describes the status of the software repository component of WDM.
- **HServer Information** = Describes the status of the HServer component of WDM.
- **Standard Service Information** = Describes the status of the Standard Service Component of WDM.
- **Basic System Information** = Describes the status of the currently running processes in the system.
- **Install Information** = Describes the Installed Component information of the system.
- **Database Information** = Describes the values of the preference settings in the WDM.
- **Logs** = Describes the WDM log information.

To view the Diagnostic Report:
1. In the Wyse Device Manager MMC Snap-in Tree panel, expand **Configuration Manager** then **Click Diagnostic Report**
2. Right-click **Diagnostic Report** and select **New →Diagnostic...**
3. WDM will generate the Diagnostic Report.

**Certificate Authority 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.

1. To view the certificates that are currently being tracked from WDM:
   - Expand the **Configuration Manager** in the tree view of the WDM Console, and select **Certificate Expiration Tracker**
   - The right-hand pane displays all the certificates that are currently being tracked.
2. To enter or edit the certificates from WDM:
   - Expand the **Configuration Manager** in the tree view of the WDM Console, and select **Certificate Expiration Tracker**, right-click and select **New →Certificate Authority**
   - The Certificate Expiration Tracker window is displayed:
   - Enter the following details:
     - **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:
Event Properties

Date: 9/10/2008  Source: HServerInit
Time: 12:09:56 PM  Category: None
Type: Error  Event ID: 15
User: N/A
Computer: BLR-N-F5SBW61

Description:
The Service produced a warning:
Certificate With Name: CA.Certificate has or is about to expire.
Expiration Date: 10/10/08
Advanced Administration

This section contains information on Wyse Device Manager security and using the WDM scripting language to create WDM Packages.

Changing the WDM Security Certificate

Before changing WDM Security Certificate, ensure you have an activated WDM Sales Key and that you have disabled device security before you can change the WDM security certificate. After changing the certificate number, you can re-enable device security (see Configuring Preferences).

Use this procedure to change the WDM certificate number (you can change the certificate to a new number or restore an older certificate).

To change the WDM Security Certificate:

1. Expand the Configuration Manager, right-click the Licensing node, and select New | Certificate to open the Change Security Certificate dialog box (note that WDM creates a new certificate number in the New Certificate box).

   ![Figure 2. Change Security Certificate](image)

   NOTE: If you have not disabled device security, you will see a warning message.

2. Depending on whether or not you want to accept the new certificate, complete one of the following:
   - If yes, click OK. You are done with this procedure.
   - If no, enter the security certificate to restore (presumably, your devices share this certificate from a previous WDM installation; by restoring the security certificate, you will regain control of the devices), and then click OK.
CAUTION: Before changing the security certificate, wait for a period of one check-in interval to allow all devices to check-in and release the current certificate. If a device that uses the current certificate does not check-in within this time, and you enable security for the new certificate, the device that did not check-in will be unmanageable (as it still has the old certificate).

About the WDM Scripting Language

The WDM scripting language was designed to allow you to create your own software packages. A software package consist of a script (.rsp) file and any required application or image files. You can create a software package, then register and distribute it to one or more devices using WDM.

Distributing software packages to one or more devices on the network saves time but requires caution and planning. It is very important that you test your software package on a separate test device to ensure validity and reliability.

CAUTION: It is imperative that all software packages be thoroughly tested before mass distribution occurs. This is the responsibility of the WDM administrator with package distribution permissions.

WDM Package Structure

A WDM Package structure consists of two components:

- The Package script (.rsp) file (ImgXL24.rsp)
- The Package folder that contains the required application or image files (ImgXL24)

In order for a Package to function properly, these two components must adhere to the following structural rules:

- The Package script file must have an .rsp extension. You can create and edit an .rsp file using ScriptBuilder.
- The Package folder must have the same name as the Package script file.
- The Number= parameter in the [Version] section of the Package script file should match the value reported by the device to the Client Manager. This becomes extremely important when using the Default Device Configuration feature.
- All the files referenced by the Package script file must be within the Package folder or a sub-folder within.
- All command arguments should be enclosed in double-quotes and are separated by spaces ONLY.
- All registry paths are delimited with backslashes (\) and are within quotes.
- Do not use abbreviations for the root registry keys (e.g. use HKEY_LOCAL_MACHINE, not HKLM).
- All filenames are delimited with backslashes (\) and are within quotes.
- Neither path names nor registry branches should ever end with a backslash.
- In general, a script is aborted if a command fails. If you do not want the script to abort if a command fails, then appended the command with an asterisk (*). (Note not all commands support this).
- <REGROOT> (e.g. <regroot>\sourcefile.txt) points to the root directory of the registered package (e.g. c:\inetpub\ftproot\rapport\<packagename>).

NOTE: <regroot> is a pointer that tells the WDM Service to look in a specific location on the WDM server (not the device) for Package application files. <regroot> finds the WDM Master Repository and identifies the folder contained within that is holding the needed Package files.
Optional Arguments and HKEY_CURRENT_USER

Four commands have optional arguments related to operations on the HKEY_CURRENT_USER registry branch.

The WDM service HKEY_CURRENT_USER registry branch is not related to any user’s HKEY_CURRENT_USER branch, so changes made directly to HKEY_CURRENT_USER typically do not have the desired effect. When called with their optional UserName arguments these four commands translate all references to HKEY_CURRENT_USER to HKEY_USERS\<username's SID>.

NOTE: These commands will fail if the given user is not logged-on at the time of distribution.

Version

The Version section contains information required for package registration and distribution purposes.

BootFloppy=

Specifies the boot floppy WDM uses during the imaging process - Rapportitf.0 (WDM Imaging agent).

Category=

Defines the category for the Package. If you type a different category name in Category=, and then register the Package using WDM, a folder is created under the Package Manager with that name.

NOTE: A package can be moved from one category to another by changing Category= and re-registering the package.

Command=

The image operation to be performed.

Example: Command=%ImageWrite%

Possible Values:

• %ImageWrite% (This value writes to the DiskOnChip)
• %ImageRead% (This value reads from the DiskOnChip)

DeployedSW=

This defines whether the package should be added to the WDM deployed package table for the device.

DEPLOYEDSW=Yes or No - Default is Yes if not specified or specified incorrectly. This option is used primarily in conjunction with DDC. If a DDC has Enforce Sequence enabled any package sent to the device will trigger the DDC to re-image the device (thereby removing all packages). Using DeployedSW=No allows the user to send packages to devices without logging their distribution, thereby not triggering a DDC operation.

Description=

Allows the script developer to add a short description about the Package. The description is a comment line and is not parsed by WDM when the script is executed.
**Image=**
This defines the file name to be used when reading or writing an image for PXE operation.

*Image=filename* - The default is the first file found in `<regroot>` excluding CRC.txt.

**ImageSize=**
Identifies for WDM the size of image being sent to a client.

Values: 8, 16, 24, 32, 48, 64, 72, 80, 96, 128, 144, 192, 256, (512)

**Number=**
Identifies for WDM the name of the Package. The name of the Package script (.rsp) file must match the *Number=* parameter. For example, if the Package script name is `ImgXL24.rsp`, you must have *Number=ImgXL24* in the [Version] section of `ImgXL24.rsp`.

Example:

[Version]
*Number*=[Number reported by device in Device Manager under Image]

*Description=Image to Write to Device*

*OS=NT*

*Category=Images*

*USE_PXE=YES*

*USE_REMOTE=NO*

*DEPLOYEDSW=YES*

*IMAGE=[xyz24xl.img]*

*IMAGESIZE=24*

**OS=**
Defines the Operating System the device is running.

Values:
- XPe Windows XPe
- CE Windows CE 3.0
- LX Tuxia Linux
Use_PXE=
WDM utilizes Intel Wired for Management standard Preboot eXecution Environment (PXE) to load images to devices. The default is Yes if Category=Images and No for all other Categories (Categories<>Images) if not specified or specified incorrectly.

If Boot from LAN is enabled in the BIOS, then Use_PXE=.

If you want the Package to be recognized by WDM as a non-imaging package, or you are working with systems that are not PXE enabled, then type No as the value.

Values: Yes and No

Use_Remote=
This defines whether the package (script verbs and PXE) should use a Remote Repository assigned to its subnet or if it should always use the Master.

Use_Remote=Yes or No - Default is Yes, if not specified or specified incorrectly.

Script
The Script section contains the WDM commands that are carried out when the script is distributed. Each command is executed in order as they appear within the [Script] section.

Append File
Verb:
AF

Description:
Adds the specified text as a new line at the end of specified device filename.

Support:
• XPe
• Linux

1. XPe Usage
   • Continue if Script Command Fails: No
   • Arguments:
     1. Path and filename
     2. New text line
   • Examples:
     AF "c:\temp\example.txt" "new line text" (This will add the line "new line text" to the end of example.txt located at c:\temp\)

2. Linux Usage
   • Continue if Script Command Fails: No
   • Arguments:
1. Path and filename
2. New text line
   • Examples:
     AF "/wfs/Append.txt" "new line text" (This will add the line "new line text" to the end of Append.txt located at /wfs)

**General Rules:**
This command will append a new line of text to the end of a text file. If the file does not already exist it will be created. This can be very useful in adding additional commands to batch and script files.

⚠️ **NOTE:** The destination directory must exist for this command to work.

**Confirm Disk Free Space**

**Verb:**
CF

**Description:**
Confirms the free space is greater than the specified amount on the specified device drive.

**Support:**
- XPe
- CE 3.0
- Linux

1. **XPe Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     1. Device drive letter (no colon required)
     2. Kilobytes free
   - Examples: CF "C" "2048" (Confirms there is at least 2MB of free space on the C: \ drive)

2. **CE Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     1. Must be blank
     2. Kilobytes free
   - Examples: CF " " "2048" (Confirms there is at least 2MB of free space on the storage device)

3. **Linux Usage**
   - Continue if Script Command Fails: No
   - Arguments:
1. Must be blank
2. Kilobytes free
   • Examples: CF ”" "512" (Confirms there is at least 2MB of free space on the storage device)

**General Rules:**

• This command should be included on all scripts.
• Do not include a colon with the device drive letter.

**Confirm File Version**

**Verb:**
CV

**Description:**
Confirms the device filename against the operand and value specified.

**Support:**
• XPe
• CE 3.0

1. **XPe Usage**
   • Continue if Script Command Fails: No
   • Arguments:
     1. Device filename (CE Add-on name)
     2. Test (<, =, >, <=, >=, or !=)
     3. Value (decimal #)
   • Examples:
     - CV "c:\Program Files\Rapport\Hagent.exe" ">=" "4.0.0.73" (Verifies hagent.exe is version 4.0.0.73 or higher)
     - CV "c:\windows\system32\mfc42.dll" "!=" "6.0.9586.0" (Verifies mfc42.dll is not version 6.0.9586.0)

2. **CE Usage**
   • Continue if Script Command Fails: No
   • Arguments:
     1. Device filename (CE Add-on name)
     2. Test (<, =, >, <=, >=, or !=)
     3. Value (decimal #)
   • Examples:
     - CV "ICA" ">=" "0019" (Verifies ICA addon is version 019 or higher)
     - CV "ICA" "=" "0023" (Verifies ICA addon is version 0023)
     - CV "ICA" "<" "0031" (Verifies ICA addon is less than version 0031)
**General Rules:**
- For a CE Add-on name, use the Add-on name as reported in the WDM GUI.

**Confirm Image**

**Verb:**
CI

**Description:**
Confirms the device operating image. This command uses the first characters (same number of characters specified in parameter) of the image number in image.ver on the device.

**Support:**
- XPe
- CE 3.0
- Linux

1. **XPe Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     - 1. Image version substring
   - Examples:
     - CI "1.2" (Verifies device Image Number begins with 1.2. Thus 1.21, 1.256, 1.295.45 will all report success)
     - CI "2.00297.192" (Verifies device Image Number begins with 2.00297.192)

2. **CE Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     - 1. Image version substring
   - Examples:
     - CI "441" (Verifies device Image Number begins with 441. Thus 441.6, 441.22 and 441.39.7 will all report success)
     - CI "486.7.1" (Verifies device Image Number begins with 486.7.1)

3. **Linux Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     - 1. Image version substring
   - Examples:
     - CI "3.6.3.00.5" (Verifies the device Image Number)
     - CI "3.6.3." (Verifies the device Image Number)
     - CI "3." (Verifies the device Image Number)
General Rules:

- This command should be included on all scripts.
- The Image version substring behaves as if a wildcard were present at the end of the image number. For example, if command was CI = "441", image numbers 441.22 and 441.23 would pass. Images 440 and 442 would fail.

Confirm Minimum RAM Size

Verb:
CR

Description:
Confirms the device has at least the specified amount of memory.

Support:

- XPe
- CE 3.0
- Linux

1. **XPe Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     1. The minimum amount of RAM in Kilobytes
   - Examples:
     CR "16000" (Verifies that device has a minimum of 16MB of RAM)

2. **CE Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     1. The minimum amount of RAM in Kilobytes
   - Examples:
     CR "16000" (Verifies that device has a minimum of 16MB of RAM)

3. **Linux Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     1. The minimum amount of RAM in Kilobytes
   - Examples:
     CR "32000" (Verifies that device has a minimum of 32000MB of RAM)

General Rules:

- This command should be included on all scripts where software is being deployed that requires a certain amount of memory.
Confirm Operating System

Verb:
CO

Description:
Confirms the device operating system. This command uses a character string representation for OS type (that is, CO "XPe").

Support:

- XPe
- CE 3.0
- Linux

1. XPe Usage
   - Continue if Script Command Fails: No
   - Arguments:
     1. Device operating system
        - XP = Windows XP
        - LX = Tuxia Linux
        - CE = CE 2.12
        - CEN = CE.Net
        - TPC = CE 3.0
     2. Optional CE version Arguments:
        - CO "CE" "2.12"
        - CO "CEN" "4.0"
        - CO "CEN" "4.1"
   - Examples:
     - CO "XP" (Verifies that Operating System is XP)
     - CO "CEN" "4.1" (Verifies that Operating System is CE.Net version 4.1; Returns true if Operating is CE.Net 4.1; Returns false if Operating System is CE.Net version 4.0)

2. CE Usage
   - Continue if Script Command Fails: No
   - Arguments:
     1. Device operating system
        - XP = Windows XP
        - LX = Tuxia Linux
        - CE = CE 2.12
        - CEN = CE.Net
        - TPC = CE 3.0
     2. Optional CE version Arguments:
• Examples:
  – CO “CE” “2.12”
  – CO “CEN” “4.0”
  – CO “CEN” “4.1”

3. Linux Usage

• Continue if Script Command Fails: No

• Arguments:
  1. Device operating system
     – XP = Windows XP
     – LX = Tuxia Linux
     – CE = CE 2.12
     – CEN = CE.Net
     – TPC = CE 3.0
  2. Optional CE version Arguments:
     – CO “CE” “2.12”
     – CO “CEN” “4.0”
     – CO “CEN” “4.1”

  • Examples:
    CO “LX” (Verifies that Operating System is LX)

**General Rules:**

• This command should be included on all scripts.

**Confirm User**

**Verb:**
CU

**Description:**
Confirms that the specified user is logged into the device.

**Support:**

• XPe

1. **XPe Usage**

• Continue if Script Command Fails: No

• Arguments:

  1. Username

• Examples:
General Rules:

- This command should be included on all scripts that have user-specific registry commands.

Delete File

Verb:

DF

Description:

Deletes the specified device filename (analogous to DEL or rm).

Support:

- XPe
- CE 3.0
- Linux

1. XPe Usage
   - Continue if Script Command Fails: Yes
   - Arguments:
     1. Path and Filename
     2. Examples: DF "c:\winnt\filetodelete.txt" (Deletes specific file from device)

2. CE Usage
   - Continue if Script Command Fails: Yes
   - Arguments:
     1. Path and Filename
     2. Examples: DF"\Windows\filetodelete.txt" (Deletes specific file from device)

Wyse devices support limited DF commands:

- DF "Gkeyreset" (Resets device to factory defaults)
- DF "CEAddon" "<addon name>" (Removes Add-on named in 3rd argument)

3. Linux Usage
   - Continue if Script Command Fails: Yes
   - Arguments:
     1. Path and Filename
     2. Examples: DF "/wfs/SendTest/filetodelete.txt" (Deletes specific file from device)
General Rules:

- Device filename should include the path.

Delete Registry Branch

**Verb:**
DB

**Description:**
Deletes the specified registry branch.

**Support:**
- XPe

1. **XPe Usage**
   - Continue if Script Command Fails: Yes
   - Arguments:
     1. Device key string
     2. User profile (not used with CE) [Optional]
   - Examples:
     DB “HKEY_LOCAL_USER\Printers” "user" (Deletes specified registry branch from user profile)

**General Rules:**

⚠️ **CAUTION:** Use care with this command. Once executed, it cannot be undone.

- The name of the registry hive should not be abbreviated.
- The WDM Agent runs in the system security context. Because of this, HKEY_CURRENT_USER for WDM is the system user, not the currently logged in user. To overcome this, a special username argument must exist that tells the agent to apply the changes to the specified user rather than the system user. The specified user must be logged into the box for this command to succeed. Note that the user profile name is used to resolve the hive location. The profile name and username can be different.

Delete Registry Value

**Verb:**
DR

**Description:**
Deletes the specified device registry key. The option username is used to change user specific registry values. The REEDIT file must use HKEY_CURRENT_USER. WDM will change this to HKEY_USERS_USERSID

**Support:**
- XPe

1. **XPe Usage**
• Continue if Script Command Fails: Yes
• Arguments:
  1. Device key string
  2. User profile [Optional]
• Examples:
  DR "HKEY_CURRENT_USER\CONTROL PANEL\COLORS\background" "user" (Deletes specified registry key from 'user's' profile)

General Rules:

⚠️ CAUTION: Use care with this command. Once executed, it cannot be undone.

• The name of the registry hive should not be abbreviated.
• The WDM Agent runs in the system security context. Because of this, HKEY_CURRENT_USER for WDM is the system user, not the currently logged in user. To overcome this, a special username argument must exist that tells the agent to apply the changes to the specified user rather than the system user. The specified user must be logged into the box for this command to succeed. Note that the user’s profile name is used to resolve the hive location. The profile name and username can be different.
• DR must be followed by the Reboot command (RB) for the changes to take effect.

Delete Tree

Verb:
DT

Description:
Deletes the specified device directory and its contents (analogous to DELTREE or rm -R).

Support:
• XPe
• Linux

1. **XPe Usage**
   • Continue if Script Command Fails: Yes
   • Arguments:
     1. Device directory
   • Examples:
     DT "C:\Test" (Deletes the 'Test' folder and all files within it)

2. **Linux Usage**
   • Continue if Script Command Fails: Yes
   • Arguments:
     1. Device directory
   • Examples:
     DT "/wfs/Test" (Deletes the 'Test' folder and all files within it)
General Rules:

⚠️ CAUTION: Use care with this command. Once executed, it cannot be undone.

End Lockout

Verb: EL

Description:
Removes the splash screen displayed by the LU command on the client device.

Support:
- XPe

1. XPe Usage
   - Continue if Script Command Fails: Yes
   - Arguments: None
   - Examples: EL

2. CE Usage
   - Continue if Script Command Fails: Yes
   - Arguments: None
   - Examples: EL

General Rules:
- This command should always be used in conjunction with a LU. It is recommended that all non-image scripts use this command.

Execute on Device

Verb: EX

Description:
Executes the specified client filename (assumes the specified file is executable).

Support:
- XPe

1. XPe Usage
   - Continue if Script Command Fails: Yes
• Arguments:
  1. Path and filename
  2. Synchronous execute [Optional]
• Examples:
  – EX "c:\test.exe" (Launches c:\test.exe on the device and continues to next command in script)
  – EX "c:\test.exe" "+" (Launches c:\test.exe on the device and pauses until the executable is finished before continuing with next command in script)
  – EX "c:\test.exe" "+30" (Launches c:\test.exe on the device and pauses until the executable is finished or 30 seconds have elapsed, whichever occurs first, before continuing with the next command in script)

**General Rules:**
• The command may be issued exactly as it would be from a command prompt on the device.
• In Windows, the path may be omitted if the executable is a registered Windows application
• The optional synchronous argument stops script processing until the executable is finished. This option can be expressed as "+" with no timeout or "+n" where n indicates the maximum time in seconds to wait before continuing script processing.

**NOTE:** Because of differences between process and system speeds, it is HIGHLY recommended that this option be used.

**Get File**

*Verb:*
GF

*Description:*
Copies the specified device filename to the specified master repository filename (analogous to COPY or cp).

*Support:*
• XPe
• CE 3.0
• Linux
1. **XPe Usage**
   • Continue if Script Command Fails: No
   • Arguments:
     1. Device filename (source)
     2. Master repository filename (destination)
   • Examples:
     GF "c:\temp\temp.txt" "<regroot>\temp.txt" (Pulls temp.txt from the device to the Master repository)
2. **CE Usage**
   • Continue if Script Command Fails: No
   • Arguments:
1. Device filename (source)
2. Master repository filename (destination)

- Examples:
  GF `\Windows\temp.txt` "<regroot>\temp.txt" (Pulls temp.txt from the device to the Master repository)

Wyse devices have limited GF support:
- GF "CEConfig" "<regroot>\Settings.reg" (Exports device registry to Settings.reg on the Master repository)

3. **Linux Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     1. Device filename (source)
     2. Master repository filename (destination)
   - Examples:
     GF `/wfs/SendTest/zero1.txt` "<regroot>\zero.txt" (Pulls zero1.txt from the device to zero.txt in the Master repository)

**General Rules:**
- Get operations always pull to the Master repository.
- Source and target filenames should include the complete path.
- The destination path should be defined with `<regroot>`.

**Get Registry**

*Verb:*
GR

*Description:*
Exports the specified device registry branch. The resulting local filename will be in REGEDIT4 format.

*Support:*
- XPe

1. **XPe Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     1. Device registry branch
     2. Master repository filename (destination)
   - Examples:
     GR "HKEY_LOCAL_MACHINE\SOFTWARE\Rappport" "<regroot>\Rapport.reg" (Exports WDM registry settings to Rapport.reg in the script folder)
General Rules:

- Get operations always pull to the Master repository.
- The name of the registry hive should not be abbreviated.
- The resulting local filename will be in REGEDIT format.
- The destination should include the complete path, defined with <regroot>.

Get Registry Value

Verb:

GV

Description:

Gets a single registry value to a file. The following types are supported:

- REG_SZ
- REG_MULTI_SZ
- REG_EXPAND_SZ
- REG_DWORD
- REG_BINARY

The output file types are:

- Windows NT 4.0: REGEDIT4 format, PC/ANSI
- Windows 2K/XP: Regedit v5.00, PC/UNICODE

NOTE:

Certain registry keys may be locked by the OS and interfere with GV operations. Verify with the device manufacture that the registry value is not locked.

Registry value changes will not be persistent unless the device is rebooted using one of the following:

- Via the RB (reboot) command
- Right-click reboot
- Manual operation

Support:

- XPe
- CE 3.0

1. XPe Usage

   - Continue if Script Command Fails: No
   - Arguments:

     1. The full path of the registry key, including the registry entry name
     2. Master repository filename (destination)
• Examples: GV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestValue1" "<regroot>\TestValue1.reg" (Pulls TestValue1 to TestValue1.reg in the script folder)

2. **CE Usage**

• Continue if Script Command Fails: No
• Arguments:
  1. The full path of the registry key, including the registry entry name
  2. Master repository filename (destination)
• Examples:
  GV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestValue1" "<regroot>\TestValue1.reg" (Pulls TestValue1 to TestValue1.reg in the script folder)

**General Rules:**
• Get operations always pull to the Master repository.
• The name of the registry hive should not be abbreviated.
• The resulting local filename will be in REGEDIT format.
• The destination should include the complete path, defined with <regroot>.

**Local Pause**

**Verb:**
LP

**Description:**
Pauses the server for a number of seconds. This allows the server to pause after commands that may take a while.

**Support:**
• XPe
• CE 3.0

1. **XPe Usage**

• Continue if Script Command Fails: No
• Arguments:
  1. Number of seconds to pause
• Examples:
  LP "30" (Pauses script processing for 30 seconds)

2. **CE Usage**

• Continue if Script Command Fails: No
• Arguments:
  1. Number of seconds to pause
• Examples:
  LP "30" (Pauses script processing for 30 seconds)
**General Rules:**
None

**Lockout User**

**Verb:**
LU

**Description:**
Display a splash screen on the device explaining an update is occurring.

**Support:**
- XPe
- CE 3.0

1. **XPe Usage**
   - Continue if Script Command Fails: Yes
   - Arguments:
     1. Yes or No (Optional)
   - Examples:
     - LU (Displays splash screen on device, splash is not removed if package fails or ends)
     - LU “Yes” (Displays splash screen on device, splash automatically removed if package fails or ends)
     - LU “No” (Displays splash screen on device, splash is not removed if package fails or ends)

2. **CE Usage**
   - Continue if Script Command Fails: Yes
   - Arguments:
     1. Yes or No (Optional)
   - Examples:
     - LU (Displays splash screen on device, splash is not removed if package fails or ends)
     - LU “Yes” (Displays splash screen on device, splash automatically removed if package fails or ends)
     - LU “No” (Displays splash screen on device, splash is not removed if package fails or ends)

**General Rules:**
- This command should always be used in conjunction with an EL. It is recommended that all non-image scripts use this command.

**Merge Registry**

**Verb:**
MR
**Description:**
Merges the specified device filename. The device filename must be in REGEDIT format (analogous to regedit -s). The option username is used to change user specific registry values. The REDEDIT4 file must use HKEY_CURRENT_USER. WDM will change this to HKEY_USERS_USERSID.

**Support:**
- XPe
1. **XPe Usage**
   - Continue if Script Command Fails: Yes
   - Arguments:
     1. Local filename
     2. User profile [Optional]
   - Examples:
     MR "<regroot>\control_panel.reg" "user" (Merges control_panel.reg into 'user's' profile)

**General Rules:**
- The filename should include the complete path, defined with <regroot>.
- The filename specified must be a REGEDIT file.
- MR must be followed by the Reboot command (RB) for the changes to take effect.
- The optional username argument is used to change user specific registry values.

**NOTE:**
The REDEDIT file must specify HKEY_CURRENT_USER. WDM will change this to HKEY_USERS_USERSID at runtime.

The WDM Agent runs in the system security context. Because of this, HKEY_CURRENT_USER for WDM is the system user, not the currently logged in user. To overcome this, a special username argument must exist that tells the agent to apply the changes to the specified user rather than the system user. The specified user must be logged into the box for this command to succeed. Note that the user profile name is used to resolve the hive location. The profile name and username can be different.

**Query User**

**Verb:**
QU

**Description:**
Query the user regarding the pending update. Allows the user to accept the update now, postpone the update 5 minutes or until next Logon to NT Server (NT/XP only).

**Support:**
- XPe
- CE 3.0
- Linux
1. **XPe Usage**

- Continue if Script Command Fails: No
- Arguments:
  1. Buttons (Optional)
     - 1 = Now only
     - 2 = Delay 5 Minutes only
     - 3 = Now and Delay 5 Minutes
     - 4 = Update on Log in only
     - 5 = Now and Update on Log in
     - 6 = Delay 5 minutes and Update on Log in
     - 7 = Now, Delay 5 minutes and Update on Log in
     - 8 = Custom message with configurable notification and postpone reminder
  2. Timeout in seconds (Optional)

     **NOTE:** If one argument is used, both must be specified.

- Examples:
  - QU (Displays query user dialog with buttons and timeout as set by preferences on the WDM server)
  - QU "2" "5" (Displays query user dialog with ‘Delay 5 Minutes’ button for 5 seconds)
  - QU "3" "120" (Displays query user dialog with ‘Update Now’ and ‘Delay 5 Minutes’ buttons for 120 seconds)

2. **CE Usage**

- Continue if Script Command Fails: No
- Arguments:
  1. Buttons (Optional)
     - 1 = Now only
     - 2 = Delay 5 Minutes only
     - 3 = Now and Delay 5 Minutes
     - 4 = Update on Log in only
     - 5 = Now and Update on Log in
     - 6 = Delay 5 minutes and Update on Log in
     - 7 = Now, Delay 5 minutes and Update on Log in
     - 8 = Custom message with configurable notification and postpone reminder
  2. Timeout in seconds (Optional)

     **NOTE:** If one argument is used, both must be specified.

- Examples:
  - QU (Displays query user dialog with buttons and timeout as set by preferences on the WDM server)
  - QU "2" "5" (Displays query user dialog with ‘Delay 5 Minutes’ button for 5 seconds)
  - QU "3" "120" (Displays query user dialog with ‘Update Now’ and ‘Delay 5 Minutes’ buttons for 120 seconds)
3. **Linux Usage**

   - Continue if Script Command Fails: No
   - Arguments:
     1. Buttons (Optional)
        - 1 = Now only
        - 2 = Delay 5 Minutes only
        - 3 = Now and Delay 5 Minutes
        - 4 = Update on Log in only
        - 5 = Now and Update on Log in
        - 6 = Delay 5 minutes and Update on Log in
        - 7 = Now, Delay 5 minutes and Update on Log in
        - 8 = Custom message with configurable notification and postpone reminder
     2. Timeout in seconds (Optional)

   **NOTE:** If one argument is used, both must be specified.

   - Examples:
     QU ‘1” “5’ (Displays query user dialog with 'Update Now' and '5 Minute Delay' buttons for 5 seconds)

**General Rules:**

- Check your company’s policies concerning updating a computer without user confirmation.
- If no arguments are defined, global values from WDM Preferences are used.
- If the user does not make a selection within the allotted timeout, the update automatically occurs.

**Reboot**

*Verb:*

 RB

*Description:*

Reboots the device.

**Support:**

- XPe
- CE 3.0
- Linux

1. **XPe Usage**

   - Continue if Script Command Fails: No
   - Arguments:
     None
   - Examples:
     RB (Reboots device)

2. **CE Usage**
- Continue if Script Command Fails: No
- Arguments:
  None
- Examples:
  RB (Reboots device)

3. **Linux Usage**

- Continue if Script Command Fails: No
- Arguments:
  None
- Examples:
  RB (Reboots device)

**General Rules:**
None

**Send File**

**Verb:**
SF

**Description:**
Copies the specified local filename to the specified device filename (analogous to the COPY or CP DOS command).

**Support:**
- XPe
- CE 3.0
- Linux

1. **XPe Usage**

- Continue if Script Command Fails: No
- Arguments:
  1. Repository path and filename (source)
  2. Device path and filename (destination)
- Examples:
  SF "<regroot>\logos.bmp" "c:\winnt\logos.bmp" (Copies logos.bmp from the repository to c:\winnt\logos.bmp on the device)

2. **CE Usage**

- Continue if Script Command Fails: No
- Arguments:
  1. Repository path and filename (source)
  2. Device path and filename (destination)
- Examples:
SF "<regroot>\sol.exe" "\Windows\sol.exe" (Copies sol.exe from the repository to \Windows \sol.exe on the device)

Wyse devices have limited SF support:
- SF "CEFirmware" "<regroot>\image.bin" (Loads image.bin (either an Add-on or entire CE image) to the device)
- SF "CEConfig" "<regroot>\setting.reg" (Applies settings.reg to the device; Note that the .reg file will be filtered before it is applied)

3. **Linux Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     1. Repository path and filename (source)
     2. Device path and filename (destination)
   - Examples:
     SF "<regroot>\SendTest\zero.txt" "/wfs/SendTest/zero1.txt" (Copies zero.txt from the repository to /wfs/SendTest/zero1.txt on the device)

**General Rules:**
- Both source and destination should include the full path, and the source path should be defined with <regroot>.
- The destination filename does not have to be the same as the source filename.

**Set Device Information**

**Verb:**
SC

**Description:**
This command allows easy configuration of the device information.

**Support:**
- XPe
- CE 3.0
- Linux

1. **XPe Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     1. CN=Computer Name
     2. CO=Contact
     3. LO=Location
     4. C1=Custom1
     5. C2=Custom2
     6. C3=Custom3
   - Examples:
SC "CN=DeviceName" "LO=location" "CO=contact" "C1=custom1" "C2=custom2" "C3=custom3" (Renames device and sets all custom information)

2. **CE Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     1. CN=Computer Name
     2. CO=Contact
     3. LO=Location
     4. C1=Custom1
     5. C2=Custom2
     6. C3=Custom3
   - Examples:
     - SC "CN=DeviceName" "LO=location" "CO=contact" "C1=custom1" "C2=custom2" "C3=custom3" (Renames device and sets all custom information)
     - SC "LO=Here" "CO=Admin" (Sets Location and Contact without altering computer name or Custom 1-3)

3. **Linux Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     1. CN=Computer Name
     2. CO=Contact
     3. LO=Location
     4. C1=Custom1
     5. C2=Custom2
     6. C3=Custom3
   - Examples: SC "CN=DeviceName" "LO=location" "CO=contact" "C1=custom1" "C2=custom2" "C3=custom3" (Renames device and sets all custom information)

**General Rules:**
- Each argument is optional; as many or as few as desired can be set (however, you must set at least one).
- Do not set multiple devices with the same computer name (CN=).

**Set Network Information**

**Verb:**

SN

**Description:**

This new command will allow easy configuration of the network information.

**Support:**
- XPe
1. XPe Usage

- Continue if Script Command Fails: No
- Arguments:
  1. IP=IP Address
  2. ED=DHCP on/off
  3. SM=Subnet Mask
  4. GW=Gateway Address
  5. 0D=DNS manual (0) or auto (1)
  6. 1D=DNS manual entry 1
  7. 2D=DNS manual entry 2
  8. OW = WINS manual (0) or auto (1)
  9. 1W=WINS manual entry 1
  10. 2W=WINS manual entry 2
  11. DM=Domain suffix

- Examples: SN "IP=192.168.1.10" "ED=0" "SM=255.255.255.0" "GW=192.168.1.1" "0D=0"
  "1D=192.168.3.21" "2D=192.168.3.22" "0W=0" "1W=192.168.1.2" "2W=192.168.1.3"
  "DM=MyDomain"

The above example will set the following:

Disable DHCP Assign Static IP as 192.168.1.10 Subnet Mask 255.255.255.0 Gateway 192.168.1.1
Set manual entry of DNS Assign primary DNS as 192.168.3.21 Assign secondary DNS as 192.168.3.22 Assign the DNS domain to MyDomain Set manual entry of WINS Assign primary WINS as 192.168.1.2 Assign secondary WINS as 192.168.1.3

2. CE Usage

- Continue if Script Command Fails: No
- Arguments:
  1. IP=IP Address
  2. ED=DHCP on/off
  3. SM=Subnet Mask
  4. GW=Gateway Address
  5. 0D=DNS manual (0) or auto (1)
  6. 1D=DNS manual entry 1
  7. 2D=DNS manual entry 2
  8. 0W = WINS manual (0) or auto (1)
  9. 1W=WINS manual entry 1
  10. 2W=WINS manual entry 2
11. DM=Domain suffix

- Examples: SN "IP=192.168.1.10" "ED=0" "SM=255.255.255.0" "GW=192.168.1.1" "0D=0" "1D=192.168.3.21" "2D=192.168.3.22" "0W=0" "1W=192.168.1.2" "2W=192.168.1.3" "DM=MyDomain"

The above example will set the following:

- Disable DHCP
- Assign Static IP of 192.168.1.10
- Subnet Mask 255.255.255.0
- Gateway 192.168.1.1
- Set manual entry of DNS
- Assign primary DNS as 192.168.3.21
- Assign secondary DNS as 192.168.3.22
- Assign the DNS domain to MyDomain
- Set manual entry of WINS
- Assign primary WINS as 192.168.1.2
- Assign secondary WINS as 192.168.1.3

3. Linux Usage

- Continue if Script Command Fails: No

- Arguments:

  1. IP=IP Address
  2. ED=DHCP on/off
  3. SM=Subnet Mask
  4. GW=Gateway Address
  5. 0D=DNS manual (0) or auto (1)
  6. 1D=DNS manual entry 1
  7. 2D=DNS manual entry 2
  8. 0W=WINS manual (0) or auto (1)
  9. 1W=WINS manual entry 1
  10. 2W=WINS manual entry 2
  11. DM=Domain suffix

- Examples: SN "IP=192.168.1.10" "ED=0" "SM=255.255.255.0" "GW=192.168.1.1" "0D=0" "1D=192.168.3.21" "2D=192.168.3.22" "0W=0" "1W=192.168.1.2" "2W=192.168.1.3" "DM=MyDomain"

The above example will set the following:

- Disable DHCP
- Assign Static IP of 192.168.1.10
- Subnet Mask 255.255.255.0
- Gateway 192.168.1.1
- Set manual entry of DNS
- Assign primary DNS as 192.168.3.21
- Assign secondary DNS as 192.168.3.22
- Assign the DNS domain to MyDomain
- Set manual entry of WINS
- Assign primary WINS as 192.168.1.2
- Assign secondary WINS as 192.168.1.3

General Rules:

- Do not set multiple devices with the same IP address (IP=).
- Sending ED=1 (DHCP on) will overrule the other entries
- 1D & 2D are only processed if 0D=0
- 1W & 2W are only processed if 0W=0
Set Profile

Verb:
SP

Description:
This command is used to update ini files. The device filename specifies the name of the ini file to update. The section, key, and value determine what to update in the ini file.

Support:
- XPe
- CE 3.0
- Linux

1. XPe Usage
   - Continue if Script Command Fails: No
   - Arguments:
     1. Device path and filename
     2. Section
     3. Key
     4. Value
   - Examples:
     SP "c:\winnt\system.ini" "drivers" "timer" "timer.drv" (Edits System.ini to:

     [drivers]
     timer=timer.drv)

2. CE Usage
   - Continue if Script Command Fails: No
   - Arguments:
     1. Device path and filename
     2. Section
     3. Key
     4. Value
   - Examples:
     SP "\Windows\SetProfile.txt" "SetProfile" "Test" "Worked" (Edits SetProfile.txt to:

     [SetProfile]
     test=worked)

3. Linux Usage
   - Continue if Script Command Fails: No
   - Arguments:
1. Device path and filename
2. Section
3. Key
4. Value
   • Examples:
     SP "/wfs/SetProfile.txt" "SetProfile" "Test" "Worked" (Edits SetProfile.txt to:

     [SetProfile]

     Test=Worked

**General Rules:**

• If the file does not exist it will be created.
• Most INI files are organized by Section and Key. A section will be defined by a line that contains bracketed text ([Example]). A Key will be followed by an equal sign and a value (Key=value).
• Keys must be located on a line by themselves.

**Set Registry Value**

**Verb:**

SV

**Description:**

Sets a single registry value.

⚠️ **NOTE:** Certain registry keys may be locked by the OS and interfere with SV operations. Please verify with the device manufacture that the registry value is not locked. Registry value changes will not be persistent unless the device is rebooted using one of the following:

• RB (reboot) command
• Right-click reboot
• Manual operation

**Support:**

• XPe

1. **XPe Usage**

   • Continue if Script Command Fails: No
   • Arguments:

     1. The full path of the registry key, including the registry entry name
     2. The value to set the registry entry to
     3. The registry type to use for argument #2. Currently only REG_SZ (string) and REG_DWORD (number) are supported. [Optional] ![endif]

   • Examples:

     – SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestValue1" "5551234" Possible scenarios:

     * TestValue1 already exists as a REG_SZ and will be set to string “5551234”
* TestValue1 already exists as a REG_DWORD and will be set to the number 5551234
* TestValue1 already exists as another type and the agent will return an error
* TestValue1 doesn’t exist and will be set to string “5551234”

- SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestValue2" "StringValue"
  Possible scenarios:
  * TestValue2 already exists as a REG_SZ and will be set to string “StringValue”
  * TestValue2 already exists as another type and the agent will return an error
  * TestValue2 doesn’t exist and will be set to string “StringValue”

- SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestDWORD" “2833” “REG_DWORD”
  Possible scenarios:
  * TestDWORD already exists as a REG_DWORD and will be set to the number 2833
  * TestDWORD already exists as another type and the agent will return an error
  * TestDWORD doesn’t exist and will be set to the number 2833

- SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestString" “MyString” “REG_SZ”
  Possible scenarios:
  * TestString already exists as a REG_SZ and will be set to string “MyString”
  * TestString already exists as another type and the agent will return an error
  * TestString doesn’t exist and will be set to string “MyString”

2. **CE Usage**
   - **Continue if Script Command Fails:** No
   - **Arguments:**
     - **Description**
       1. The full path of the registry key, including the registry entry name
       2. The value to set the registry entry to
       3. The registry type to use for argument #2. Currently only REG_SZ (string) and REG_DWORD (number) are supported. [Optional] 

   - **Examples:**
     - SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestValue1" "5551234" Possible scenarios:
       * TestValue1 already exists as a REG_SZ and will be set to string “5551234”
       * TestValue1 already exists as a REG_DWORD and will be set to the number 5551234
       * TestValue1 already exists as another type and the agent will return an error
       * TestValue1 doesn’t exist and will be set to string “5551234”

     - SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestValue2" "StringValue"
       Possible scenarios:
       * TestValue2 already exists as a REG_SZ and will be set to string “StringValue”
       * TestValue2 already exists as another type and the agent will return an error
       * TestValue2 doesn’t exist and will be set to string “StringValue”

     - SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestDWORD" “2833” “REG_DWORD”
       Possible scenarios:
       * TestDWORD already exists as a REG_DWORD and will be set to the number 2833
       * TestDWORD already exists as another type and the agent will return an error
       * TestDWORD doesn’t exist and will be set to the number 2833
Possible scenarios:

* TestDWORD already exists as a REG_DWORD and will be set to the number 2833
* TestDWORD already exists as another type and the agent will return an error
* TestDWORD doesn’t exist and will be set to the number 2833

– SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestString" "MyString" "REG_SZ"

Possible scenarios:

* TestString already exists as a REG_SZ and will be set to string "MyString"
* TestString already exists as another type and the agent will return an error
* TestString doesn’t exist and will be set to string "MyString"

**General Rules:**

- The name of the registry hive should not be abbreviated.
- If three arguments are supplied then the agent will either create non-existing keys of the supplied type, or error out if the type does not match an existing key’s type.
- If only two arguments are supplied and the key does not already exist then the type REG_SZ (string) is assumed.
- If only two arguments are supplied and the key does exist and it is of type REG_DWORD then the agent will confirm the value is a number and set it as a DWORD.

**Shutdown**

**Verb:**
SD

**Description:**
Shuts down the device and sets the power state.

**Support:**

- XPe
- CE 3.0
- Linux

1. **XPe Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     None
   - Examples:
     SD (Shut down device)

2. **CE Usage**
   - Continue if Script Command Fails: No
   - Arguments:
     None
   - Examples:
     SD (Shut down device)
3. **Linux Usage**
   - Continue if Script Command Fails: No
   - Arguments: None
   - Examples: SD (Shut down device)

**General Rules:**
None

**Synch Time**

**Verb:**
ST

**Description:**
Changes the device time to match the update server time.

**Support:**
- XPe
- CE 3.0
- Linux

1. **XPe Usage**
   - Continue if Script Command Fails: Yes
   - Arguments: None
   - Examples: ST (Synchronizes the device time to the WDM server time)

2. **CE Usage**
   - Continue if Script Command Fails: Yes
   - Arguments: None
   - Examples: ST (Synchronizes the device time to the WDM server time)

3. **Linux Usage**
   - Continue if Script Command Fails: Yes
   - Arguments: None
   - Examples: ST (Synchronizes the device time to the WDM server time)

**General Rules:**
- There may be a slight time difference between server and device due to network latency.
- Time Zone offset is taken into account, please ensure that the proper time zone is set on the device.
Wake On LAN

Verb:
WL

Description:
Boots a device that is shutdown (the device must have Wake On LAN enabled in its BIOS).

Support:
Hardware dependent, not agent dependent

X Copy

Verb:
XC

Description:
Copies the specified device directory and its contents to the specified local directory (analogous to XCOPY or cp -R).

Support:
- XPe
- CE 3.0
- Linux

1. XPe Usage
   - Continue if Script Command Fails: No
   - Arguments:
     1. Repository directory (source)
     2. Device directory (destination)
   - Examples:
     XC "<regroot>\Files\winnt\system32\*" "C:\winnt\system32" (Copies all files in the system32 folder of the package to the device’s system32 folder)

2. CE Usage
   - Continue if Script Command Fails: No
   - Arguments:
     1. Repository directory (source)
     2. Device directory (destination)
   - Examples:
     XC "<regroot>\system\*" "\system" (Copies all files in the system folder of the package to the device’s system folder)

3. Linux Usage
   - Continue if Script Command Fails: No
• Arguments:
  1. Repository directory (source)
  2. Device directory (destination)
• Examples:
  XC `<regroot>`\`XCTest`\* `/wfs/` (Copies all files in the XCTest folder of the package to the device’s wfs folder)

**General Rules:**
• The source path should be defined with `<regroot>`.
• The source path should end in `\*` (`*` is a wildcard to indicate all files and directories).

**Understanding the Script File Structure**

A WDM script (.rsp) file is one of two components that make up a WDM Package:

• The Package script (.rsp) file (ImgXL24.rsp)
• The Package folder that contains the required application or image files (ImgXL24)

The Package script (.rsp) file must conform to a specific structure and should contain two sections:

• Version
• Script

**Version**

The Version section contains information required for package registration and distribution purposes. The following describes each of the elements of the Version section:

• `[Version]` - Required section header
• `Number=` - Must be the same as the Package Script File name
• `Description=` - A brief description of what the Package is to achieve
• `OS=` - The Operating System the Package is intended for
• `USE_REMOTE=` - YES/NO, specifies whether or not a Remote Repository (if it exists) should be used. Default is YES. (OPTIONAL)
• `DEPLOYEDSW=` - YES/NO defines whether package should be added to the WDM deployed package table for device. Default is YES. (OPTIONAL)
• `Category=` - The WDM Package Manager category in the GUI where the Package will reside. Note if the category does not exist it will be created.

**Image Category Special Tags**

• `[Version]` - Required section header
• `ImageSize=` - size of image in Megabytes
• `BootFloppy=` - name of bootfloppy; default = RAPPORT
• `Use_PXE=` - YES/NO default value is YES for all scripts with Category=IMAGES
• `IMAGE=` - name of image file to be used; by default WDM uses the first file in file found in the package folder (excluding CRC.text)
• `Command=` - the image operation to be performed
Script
The Script section contains the commands that are carried out when the script is distributed. Each command is executed in order as they appear within the [Script] section.

Recommended Scripting Template

[Version]

Number=Script name (matching the RSP_ file name and Package folder name)

Description=Detailed description with version number and valid images

OS=XX

Category=Other Packages

[Script]

Written by: Your Name and Company

; ....................................................................................

; >Check the Operating System

; >Check the Image Version

; ....................................................................................

CO "NT"
CI "XXXX"

; ....................................................................................

; >Check Free Space

; >Check Minimum Memory, if necessary

; >Check User, if necessary

; ....................................................................................

CF "X" "XXX"
CR "XXXX"
CU "XXXXXXXX"

; ....................................................................................

; > Query User then lock Workstation
Understanding WDM Agent Error Codes

This section contains information on the following errors:

- **File Transfer Protocol Error Codes** - The File Transfer Protocol (FTP) is a protocol that is able to transfer files between machines with different operating systems. The FTP utility issues an error, or reply, code to every user command. FTP errors are discussed in [File Transfer Protocol (FTP) Error Codes](#).

- **Windows Sockets Error Codes** - When using any TCP/IP application, it is possible for errors to occur in both configuration and networking. Many applications do not report these errors, but simply tell you that you have a network error. A list of possible errors (as reported by Microsoft) is shown in [Windows Sockets Error Codes](#).
File Transfer Protocol (FTP) Error Codes

NOTE: The following are excerpts from RFC 959 for FTP.

An FTP reply consists of a three-digit number (transmitted as three alphanumeric characters) followed by some text. The number is intended for use by automata to determine what state to enter next; the text is intended for the human user.

The three digits of the reply each have a special significance. This is intended to allow a range of very simple to very sophisticated responses by the user-process. The first digit denotes whether the response is good, bad or incomplete. An unsophisticated user-process will be able to determine its next action (proceed as planned, redo, retrench, and so on) by simply examining this first digit. A user-process that wants to know approximately what kind of error occurred (for example, file system error, command syntax error) may examine the second digit, reserving the third digit for the finest gradation of information.

First Digit

There are five values for the first digit of the reply code:

- **1yz Positive Preliminary reply** - The requested action is being initiated; expect another reply before proceeding with a new command (the user-process sending another command before the completion reply would be in violation of protocol; but server-FTP processes should queue any commands that arrive while a preceding command is in progress). This type of reply can be used to indicate that the command was accepted and the user-process can now pay attention to the data connections, for implementations where simultaneous monitoring is difficult. The server-FTP process can send at most, one 1yz reply per command.

- **2yz Positive Completion reply** - The requested action has been successfully completed. A new request can be initiated.

- **3yz Positive Intermediate reply** - The command has been accepted, but the requested action is being held in abeyance, pending receipt of further information. The user should send another command specifying this information. This reply is used in command sequence groups.

- **4yz Transient Negative Completion reply** - The command was not accepted and the requested action did not take place, but the error condition is temporary and the action may be requested again. The user should return to the beginning of the command sequence, if any. It is difficult to assign a meaning to transient, particularly when two distinct sites (Server- and User-processes) have to agree on the interpretation. Each reply in the 4yz category might have a slightly different time value, but the intent is that the user-process is encouraged to try again. A rule of thumb in determining if a reply fits into the 4yz or the 5yz (Permanent Negative) category is that replies are 4yz if the commands can be repeated without any change in command form or in properties of the User or Server (for example, the command is spelled the same with the same arguments used; the user does not change his file access or user name; the server does not put up a new implementation).

- **5yz Permanent Negative Completion reply** - The command was not accepted and the requested action did not take place. The User-process is discouraged from repeating the exact request (in the same sequence). Even some permanent error conditions can be corrected, so the human user may want to direct his User-process to re-initiate the command sequence by direct action at some point in the future (for example, after the spelling has been changed, or the user has altered his directory status).

Second digit (Function Groupings)

The following function groupings are encoded in the second digit:
• **x0z Syntax** - These replies refer to syntax errors, syntactically correct commands that do not fit any functional category, non-implemented or superfluous commands.

• **x1z Information** - These are replies to requests for information, such as status or help.

• **x2z Connections** - Replies referring to the control and data connections.

• **x3z Authentication and accounting** - Replies for the login process and accounting procedures.

• **x4z** - Unspecified as yet.

• **x5z File system** - These replies indicate the status of the Server file system through the requested transfer or other file system action.

**Third Digit**

The third digit gives a finer gradation of meaning in each of the function categories specified by the second digit, as shown in the following list:

**NOTE:** The text associated with each reply is recommended, rather than mandatory, and may even change according to the command with which it is associated. The reply codes, on the other hand, must strictly follow the specifications in the last section; that is, Server implementations should not invent new codes for situations that are only slightly different from the ones described here, but rather should adapt codes already defined.

**• 100**
- 110 Restart marker reply.
- 120 Service ready in minutes.
- 125 Data connection already open; transfer starting.
- 150 File status okay; about to open data connection.

**• 200**
- 200 Command okay.
- 202 Command not implemented, superfluous at this site.
- 211 System status, or system help reply.
- 212 Directory status.
- 213 File status.
- 214 Help message.
- 215 NAME system type.
- 220 Service ready for new user.
- 221 Service closing control connection. Logged out if appropriate.
- 225 Data connection open; no transfer in progress.
- 226 Closing data connection. Requested file action successful (for example, file transfer or file abort).
- 227 Entering Passive Mode (h1, h2, h3, h4, p1, p2).
- 230 User logged in, proceed.
- 250 Requested file action okay, completed.
- 257 PATHNAME created.

**• 300**
- 331 User name okay, need password.
- 332 Need account for login.
- 350 Requested file action pending further information.
• **400**
  - 421 Service not available, closing control connection. This may be a reply to any command if the service knows it must shut down.
  - 425 Can't open data connection.
  - 426 Connection closed; transfer aborted.
  - 450 Requested file action not taken. File unavailable (for example, file busy).
  - 451 Requested action aborted: local error in processing.
  - 452 Requested action not taken. Insufficient storage space in system.

• **500**
  - 500 Syntax error, command unrecognized. This may include errors such as command line too long.
  - 501 Syntax error in parameters or arguments
  - 502 Command not implemented.
  - 503 Bad sequence of commands.
  - 504 Command not implemented for that parameter.
  - 530 Not logged in.
  - 532 Need account for storing files.
  - 550 Requested action not taken. File unavailable (for example, file not found, or no access).
  - 551 Requested action aborted: page type unknown.
  - 552 Requested file action aborted. Exceeded storage allocation (for current directory or data set).
  - 553 Requested action not taken. File name not allowed.

**Windows Sockets Error Codes**

WINSOCK Errors are generated when a script is running on a WDM Agent. In such a case, the WDM Agent either had trouble obtaining or sending a file as part of the script. The following is a list of possible errors (as reported by Microsoft):

- **WSAEINTR 10004** - Interrupted function call. A blocking operation was interrupted by a call.
- **WSAEACCES 10013** - Permission denied. An attempt was made to access a socket in a forbidden way.
- **WSAEFAULT 10014** - Bad address. The system detected an invalid pointer address.
- **WSAEINVAL 10022** - Invalid argument. Some invalid argument was supplied.
- **WSAEFILE 10024** - Too many open files. Too many open sockets.
- **WSAEWOULDBLOCK 10035** - Resource temporarily unavailable. Socket operation not available at this time.
- **WSAEINPROGRESS 10036** - Operation now in progress. A blocking operation is currently executing.
- **WSAEALREADY 10037** - Operation already in progress. An operation was attempted on a non-blocking socket with an operation already in progress.
- **WSAENOTSOCK 10038** - Socket operation on non-socket. An operation was attempted on something that is not a socket.
- **WSAENOTADDRESS 10039** - Destination address required. A required address was omitted from an operation.
- **WSAEMSGSIZE 10040** - Message too long. A message sent on a datagram socket was larger than the internal message buffer.
- **WSAEPROTOTYPE 10041** - Protocol wrong type for socket. A protocol was specified in the socket function call that is not supported.
- **WSAENOPROTOOPT 10042** - Bad protocol option. An unknown, invalid or unsupported call was made.
- **WSAEPROTOSUPPORT 10043** - Protocol not supported. The requested protocol has not been configured into the system.
- **WSAESOCKTNOSUPPORT 10044** - Socket type not supported. The support for the specified socket type does not exist.
- **WSAEOPNOTSUPP 10045** - Operation not supported. The attempted operation is not supported.
- **WSAEPFNSUPPORT 10046** - Protocol family not supported. The protocol family has not been configured into the system or no implementation for it exists.
- **WSAFAFNSUPPORT 10047** - Address family not supported. An address incompatible with the requested protocol was used.
- **WSAENOTRUSED 10048** - Address already in use. An application attempts to bind a socket to an IP address/port that has already been used for an existing socket.
- **WSAENETNOTAVAIL 10049** - Address Not available. The requested address is not valid.
- **WSAENETDOWN 10050** - Network is down. A socket operation encountered a dead network.
- **WSAENETUNREACH 10051** - Network is unreachable. A socket operation was attempted to an unreachable network.
- **WSAENETRESET 10052** - Network dropped connection. The connection has been broken due to keep-alive activity detecting a failure while the operation was in progress.
- **WSAECONNABORTED 10053** - Software caused connection abort. A connection was aborted by the software in your machine, possibly due to a TCP/IP configuration error, data transmission time-out or protocol error.
- **WSAECONNRESET 10054** - Connection reset by peer. An existing connection was forcibly closed by the remote host.
- **WSAENOBUFFS 10055** - No buffer space available. An operation on a socket could not be performed because the system lacked sufficient buffer space or because a queue was full.
- **WSAEISCONN 10056** - Socket is already connected. A connect request was made on an already-connected socket.
- **WSAENOTCONN 10057** - Socket is not connected. A request to send or receive data was disallowed because the socket is not connected.
- **WSAENETDOWN 10058** - Cannot send after socket shutdown. A request to send or receive data was disallowed because the socket had already been shut down.
- **WSAETIMEDOUT 10059** - Connection timed out. A connection did not properly respond after a period of time.
- **WSAECONNREFUSED 10060** - Connection refused. No connection could be made because the target machine actively refused it.
- **WSAHOSTDOWN 10061** - Host is down. A socket operation failed because the destination host is down.
- **WSAHOSTUNREACH 10062** - No route to host. A socket operation was attempted to an unreachable host.
- **WSAEPROCCLIM 10063** - Too many processes. A Windows Sockets implementation may have a limit on the number of applications that can use it simultaneously.
- **WSASYSCALL 10064** - Network subsystem is unavailable. This error is returned if the sockets implementation cannot function because the system is currently unavailable.
- **WSAVERNOTSUPPORTED 10065** - Winsock.dll version out of range. The current Windows Sockets implementation does not support the Windows Sockets specification version requested.
- **WSANOTINITIALISED 10066** - Startup failed. The application socket startup failed.
- **WSAEDISCON 10101** - Graceful shutdown in progress. Returned to indicate that the remote party has initiated a graceful shutdown.
• **WSATYPE_NOT_FOUND 10109** - Class type not found. The specified class was not found.
• **WSAHOST_NOT_FOUND 11001** - Host not found. No such host is known.
• **WSATRY_AGAIN 11002** - Non-authoritative host not found. A temporary error during host name resolution and means that the local server did not receive a response from an authoritative server.
• **WSANO_RECOVERY 11003** - This is a nonrecoverable error. A nonrecoverable error occurred during a database lookup.
• **WSANO_DATA 11004** - Valid name, no data record of requested type. The requested name is valid and was found in the database, but does not have the correct associated data being resolved for it.
• **ERROR_INTERNET_TIMEOUT 12002** - Internet time-out. The request has timed out.
Troubleshooting

This section provides troubleshooting information for Wyse Device Manager.

WDM Installation Failure

**Problem:** The installation fails after you install WDM.

**Solution:** Check the *WyseInstall.log* file under `C:\Program Files (x86)\Wyse\WDM` for details about the failures.

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. For more information on this utility, see [DNS-DHCP Lookup Utility](#).

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)

**Setting the Correct Logging Levels**

**Problem:** You want to set the logging levels appropriately.

**Solution:** Set logging levels to **Debug only** for isolating problems. During normal WDM functioning, set the logging levels to either **Warning** or **Error**.

**Viewing Service Logs**

The service logs include:

- **Web Services Log** - Details the activity of the WDM Web Services for device management.
- **TFTP Log** - Details the Trivial File Transfer Protocol activity for distributing software packages to devices.
- **Standard Services Log** - Details the activity of the WDM Standard Services.
- **DHCP Log** - Details the activity of the WDM Dynamic Host Configuration Protocol as it assigns IP addresses to devices.

**NOTE:** For information on setting the level of logging activity for the WDM service logs, see [Logging Preferences](#).

To view the WDM service logs:

1. Double-click the **Service Logs** icon in the WDM system tray to open the WDM Service Logs window.
2. Enable the Service Logs from the main menu of the Device Manager Service Logs **View** menu.
3. Click the **GUI Logs** tab to view the GUI logs.
The logs are color-coded. The **Warning** logs are highlighted in yellow and the **Error** logs are highlighted in red.

4. Click the Service Logs tab to view the **Web Service** logs.
If you have configured Load Balancing in your environment, the Service Logs may at times display a test connection failure. This happens when there is a routing issue from the Proxy server when it tries to contact the WDM Management Server. You can resolve this issue by checking the Alias name you have specified in the Service Preferences → Server Port Settings. If the information is correct and there is still a connection failure, you can change the Alias Server Name by providing the IP address of the Proxy Server and click OK. You can then open the window again and change the IP address back to the host name of the Proxy Server and click OK. This would resolve your problem.

**NOTE:** To expand a window for any of the logs, click its maximize button.

### Problem With HServer Init Requests

**Problem:** You are not able to see the ports in the Preferences window.

**Solution:** Restart HServerInit and verify the preferences again.

<table>
<thead>
<tr>
<th>#</th>
<th>Type</th>
<th>Time</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>Information</td>
<td>2014-04-08 22:24:00</td>
<td>DHCPSERVICE</td>
<td>[DHCP] - Packet is DHCPInform from device: 008084A7B8</td>
</tr>
<tr>
<td>23</td>
<td>Information</td>
<td>2014-04-08 22:24:18</td>
<td>DHCPSERVICE</td>
<td>[DHCP] - Packet is DHCPInform from device: 008084A7B8</td>
</tr>
<tr>
<td>28</td>
<td>Information</td>
<td>2014-04-08 22:24:52</td>
<td>DHCPSERVICE</td>
<td>[DHCP] - Packet is DHCPREQUEST from device: 008084B5DE</td>
</tr>
<tr>
<td>30</td>
<td>Information</td>
<td>2014-04-08 22:24:54</td>
<td>DHCPSERVICE</td>
<td>[DHCP] - Packet is DHCPInform from device: 008084A44D</td>
</tr>
<tr>
<td>31</td>
<td>Information</td>
<td>2014-04-08 22:24:54</td>
<td>DHCPSERVICE</td>
<td>[DHCP] - Packet is DHCPInform from device: 008084A44D</td>
</tr>
<tr>
<td>32</td>
<td>Information</td>
<td>2014-04-08 22:24:56</td>
<td>DHCPSERVICE</td>
<td>[DHCP] - Packet is DHCPInform from device: 008084A44D</td>
</tr>
<tr>
<td>34</td>
<td>Information</td>
<td>2014-04-08 22:25:15</td>
<td>DHCPSERVICE</td>
<td>[DHCP] - Packet is DHCPInform from device: 008084A44D</td>
</tr>
<tr>
<td>36</td>
<td>Information</td>
<td>2014-04-08 22:25:42</td>
<td>DHCPSERVICE</td>
<td>[DHCP] - Packet is DHCPREQUEST from device: 008084A44D</td>
</tr>
<tr>
<td>38</td>
<td>Information</td>
<td>2014-04-08 22:25:45</td>
<td>DHCPSERVICE</td>
<td>[DHCP] - Packet is DHCPInform from device: 008084A44D</td>
</tr>
<tr>
<td>39</td>
<td>Information</td>
<td>2014-04-08 22:26:06</td>
<td>DHCPSERVICE</td>
<td>[DHCP] - Packet is DHCPInform from device: 008084A44D</td>
</tr>
<tr>
<td>40</td>
<td>Information</td>
<td>2014-04-08 22:33:41</td>
<td>DHCPSERVICE</td>
<td>[DHCP] - Packet is DHCPInform from device: 008084A44D</td>
</tr>
<tr>
<td>41</td>
<td>Information</td>
<td>2014-04-08 22:34:04</td>
<td>DHCPSERVICE</td>
<td>[DHCP] - Packet is DHCPInform from device: 008084A44D</td>
</tr>
<tr>
<td>42</td>
<td>Information</td>
<td>2014-04-09 00:28:57</td>
<td>DHCPSERVICE</td>
<td>[DHCP] - Packet is DHCPDiscover from device: 008084A44D</td>
</tr>
<tr>
<td>43</td>
<td>Information</td>
<td>2014-04-09 00:28:58</td>
<td>DHCPSERVICE</td>
<td>[DHCP] - Packet is DHCPREQUEST from device: 008084A44D</td>
</tr>
<tr>
<td>44</td>
<td>Information</td>
<td>2014-04-09 00:29:01</td>
<td>DHCPSERVICE</td>
<td>[DHCP] - Packet is DHCPInform from device: 008084A44D</td>
</tr>
</tbody>
</table>
If the ports are still not visible in the Preferences window, an IIS Lockout tool might be running in your server and using the urlscan security tool which stops the request for HServer. To resolve the problem, you need to configure the urlscan.ini file and after configuring, restart the WWW service.

The urlscan.ini file contains the following sections:

1. **[Options]** - This section describes general URLScan options.
2. **[AllowExtensions]** and **[DenyExtensions]** - This section defines the file name extensions that URLScan permits.
3. **[Options]**-[AllowVerbs] and **[DenyVerbs]** - This section defines the verbs (also known as HTTP methods) that URLScan permits.
4. **[Options]**-[DenyHeaders] - This section lists HTTP headers that are not permitted in an HTTP request. If an HTTP request contains one of the HTTP headers that are listed in this section, URLScan rejects the request.
5. **[DenyURLSequences]** - This section lists strings that are not permitted in an HTTP request. URLScan rejects HTTP requests that contain a string that appears in this section.
6. **[RequestLimits]** section - This section enforces limits on the size, in bytes, of separate parts of requests reaching the server.

Configure the urlscan.ini file as follows:

- In the **[Options]** section configure the following settings:
  
  **[Options]**

  AllowDotInPath = 1

  UseAllowVerbs = 1

  UseAllowExtensions = 1

- In the **[AllowExtensions]** and **[DenyExtensions]** section configure the following settings:
  
  **[AllowExtensions]**

  .bat

  .cmd

  .com

  .exe

- If the properties shown for a file in the backup folder do not match the properties for that file in its destination folder, make a copy of the file in the backup folder and put it in the appropriate destination folder.
  
  **[Allow Verbs]**

  GET

  HEAD

  POST

  PROPFIND

  MKCOL
DELETE

PUT

MOVE

- In the [DenyHeaders] section configure the following settings:

  [DenyHeaders]

  Allow Translate header

- In the [RequestLimits] section configure the following settings:

  [RequestLimits]

    MaxAllowedContentLength = 4294967296

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.

Changing the IP Address of the WDM Server

Problem: You want to change the IP address of the WDM Server.

Solution: Change the IP address of the WDM Server by completing the following:

1. Change the following registry settings:
   - Configuration Manager\Software Repositories\Master = new IP address
   - HKLM\Software\Rapport\SWRep\FTPUserDomain = new IP address
2. Restart IIS.
3. Restart WDM services (use the Services tab).

Peer Assisted Deployment Issues

This section 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:


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, see [Device Manager Preferences](#).
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. For more information on updating the WDM Agent, see [Package Manager](#).
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 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 Ubuntu T50 or Wyse Thin OS (WTOS) 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:
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 WE57, WE57P, 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.