About SolarWinds

SolarWinds, Inc. develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today’s network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Copyright

© 2016 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds and other SolarWinds marks, identified on the SolarWinds website, as updated from SolarWinds from time to time and incorporated herein, are registered with the U.S. Patent and Trademark Office and may be registered or pending registration in other countries. All other SolarWinds trademarks may be common law marks or registered or pending registration in the United States or in other countries. All other trademarks or registered trademarks contained and/or mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective companies.

Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

<table>
<thead>
<tr>
<th>Team</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales</td>
<td>1.866.530.8100</td>
</tr>
</tbody>
</table>
Documentation Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Specifying</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Window items, including buttons and fields.</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>Book and CD titles, variable names, new terms</td>
</tr>
<tr>
<td><strong>Fixed font</strong></td>
<td>File and directory names, commands and code examples, text typed by you</td>
</tr>
<tr>
<td><strong>Straight brackets, as in [value]</strong></td>
<td>Optional command parameters</td>
</tr>
<tr>
<td><strong>Curly braces, as in {value}</strong></td>
<td>Required command parameters</td>
</tr>
<tr>
<td>**Logical OR, as in value1</td>
<td>value2**</td>
</tr>
</tbody>
</table>

SolarWinds Patch Manager Documentation Library

The following documents are included in the SolarWinds Patch Manager documentation library:

<table>
<thead>
<tr>
<th>Document</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Guide</td>
<td>Provides detailed setup, configuration, and conceptual information.</td>
</tr>
<tr>
<td>Evaluation Guide</td>
<td>Provides installation, setup, and common scenarios for which Patch Manager provides a simple, yet powerful, solution.</td>
</tr>
<tr>
<td>Evaluation Guide for ConfigMgr</td>
<td>Targeted at users implementing Patch Manager in a Microsoft System Center Configuration Manager (ConfigMgr) environment. Provides installation, setup, and common scenarios for which Patch Manager provides a simple, yet powerful, solution.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Release Notes</td>
<td>Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at <a href="http://www.solarwinds.com">www.solarwinds.com</a>.</td>
</tr>
</tbody>
</table>
# Table of Contents

**About SolarWinds** .................................................................................................................. 2

Copyright ...................................................................................................................................... 2

Contacting SolarWinds .................................................................................................................. 2

Documentation Conventions ......................................................................................................... 3

SolarWinds Patch Manager Documentation Library ................................................................. 3

**Table of Contents** ..................................................................................................................... 5

**Introduction** ............................................................................................................................... 17

Patch Manager Server .................................................................................................................... 18

Microsoft SQL Server .................................................................................................................... 19

Administration Console ............................................................................................................... 19

Web Console ................................................................................................................................... 19

Managed Computers .................................................................................................................... 19

Agents (Optional) ........................................................................................................................... 19

**Installing Patch Manager** ........................................................................................................ 20

Requirements ................................................................................................................................. 20

Notes on Windows Server 2008 R2 with SP1 .............................................................................. 24

Port and Firewall Information ......................................................................................................... 24

Port 135 TCP – RPC Endpoint Mapper ......................................................................................... 24

Port 445 TCP – SMB over TCP ...................................................................................................... 25

Port 4092 – Console-to-Server Communication ............................................................................ 25

Port 8787 TCP – Web Console Connections ............................................................................... 25

Port 17777 TCP – SolarWinds Information Service ...................................................................... 25


Dynamic Ports 1024-65536 – DCOM or RPC ............................................................................. 25

Deployment Best Practices .............................................................................................................. 25
Best deployment practice ............................................................... 26
Single server deployment ............................................................ 26
Installing the Patch Manager PAS .............................................. 26
Patch Manager Licensing ............................................................ 28
Going from Evaluation to Production ........................................... 28
Licensing Servers with Internet Access ........................................ 29
Licensing Servers without Internet Access .................................... 29
Maintaining Licenses with License Manager ............................... 30
Maintaining licenses ................................................................. 30
License Manager Requirements .................................................. 30
Installing License Manager ....................................................... 31
Activating Licenses with the License Manager .............................. 32
Deactivating and Registering Licenses with the License Manager .... 34
Upgrading and Synchronizing Licenses ........................................ 34
Installing Your First Updates ....................................................... 35

**Configuring Patch Manager** ...................................................... 37
Initial Configuration ..................................................................... 37
Configuring Managed Resources ................................................ 37
Configuring Credentials and Credential Rings Rules .................... 38
Configuring Update Services ...................................................... 39
Configuring Publishing Servers .................................................. 39
Configuring Managed Clients ..................................................... 40
Using Group Policy to Configure Managed Clients ...................... 41
Exporting the WSUS Certificate .................................................. 41
Configuring the Group Policy Object .......................................... 42
Configuring Clients from the Patch Manager Console .................. 43
Cross-compatibility .................................................................57
Adding Extension Pack Features Later .....................................57
The Navigation Pane .............................................................57
The Enterprise Node .............................................................58
The Administration and Reporting Node .................................58
The Patch Manager System Configuration Node .......................59
The Data Grid Pane ..............................................................59
Selecting Columns ..................................................................60
Reorganizing Columns ............................................................60
Sorting Column Data ..............................................................61
Filtering Column Data ............................................................61
  Filtering by Specific Values ...................................................61
  Creating Custom Filters .......................................................61
Grouping Column Data ............................................................62
The Task Options Wizard .........................................................62
The Computer Selection Page ..................................................63
  Add Computers ....................................................................63
  Browse Computers ..............................................................63
  Select Computers Using Rules ..............................................64
Other Options .........................................................................65
The Scheduling and Notification Options Page .........................66
  Schedule Settings ...............................................................66
  Exports Options .................................................................67
  Email Notification ...............................................................67
The Summary Page ..................................................................68
Patch Manager Computer Groups .............................................68
Managing Published Third-party Updates ................................................................................. 69
Managing Publishing Servers ................................................................................................. 69
Importing and Exporting Catalogs .......................................................................................... 70
Creating and Publishing Software Packages ........................................................................ 71
Creating Software Packages .................................................................................................. 72
Completing the Package Wizard ............................................................................................. 72
Defining Package Metadata ..................................................................................................... 73
Defining the Package Source ................................................................................................... 75
Using PackageBoot .................................................................................................................. 76
Managing Software Package Rulesets ...................................................................................... 77
Publishing Custom Software Packages .................................................................................... 79
Managing Third-party Packages .............................................................................................. 81
Auto-Publishing Third Party Updates to WSUS ........................................................................ 83

Inventory and Reporting ........................................................................................................ 86
Inventory Tasks ....................................................................................................................... 86
Configuring the WSUS Inventory Task ...................................................................................... 87
Configuring the Managed Computer Inventory Task .............................................................. 87
Scheduling the Managed Computer Inventory Task ............................................................... 88
Collecting File, Folder, or Registry Information ........................................................................ 89
Patch Manager Report Viewer and Report Builder ................................................................. 90
Using Patch Manager Report Viewer ..................................................................................... 90
Running WSUS Reports .......................................................................................................... 90
Customizing Report Layouts .................................................................................................... 91
Filtering and Sorting Report Results ...................................................................................... 92
Configuring Report Viewer Email Settings ............................................................................ 92
Exporting and Emailing Report Results .................................................................................. 92
Customizing a Patch Manager Report ................................................................. 93
Creating a Custom Report ............................................................................... 95
Creating a Custom WSUS Report .................................................................. 95
Installing Updates from a WSUS Report ...................................................... 97
Report Data Sources ....................................................................................... 97

Administrating WSUS Using Patch Manager ............................................... 98
Synchronizing WSUS Servers ......................................................................... 98
Cleaning Up WSUS Servers ........................................................................... 98
Repairing and Maintaining the Windows Update Agent .................................. 100
  Repair Options .............................................................................................. 100
  Maintenance .................................................................................................. 100
Administrating Windows Update Agent Local Policy .................................... 101

Advanced Configuration Options .................................................................... 103
Patch Manager Management Groups ............................................................. 103
  Adding Management Groups ...................................................................... 103
  Adding and Removing Managed Resources ................................................ 104
    Add or Configure WSUS Server ................................................................. 104
    Configuration Manager Site Server Registration Management ................ 104
    Management Group Wizard ...................................................................... 105
Configuring Remote Administration Consoles .............................................. 106
  Installing the Patch Manager Console ......................................................... 106
Configuring Additional Patch Manager Servers ........................................... 107
  Installing the Patch Manager Server .......................................................... 107

Managing Patch Manager Users and Security ................................................ 110
  Credentials .................................................................................................... 110
  Managing Credentials ................................................................................... 110
Adding Patch Manager User Accounts ................................................................. 119
Orion Accounts ................................................................................................. 119
Windows Accounts ......................................................................................... 120
Defining User Settings .................................................................................... 121

Managing Client WMI Connectivity ................................................................ 122
WMI Requirements .......................................................................................... 122
Security and Permissions ............................................................................... 123
Provisioning the WMI Providers ...................................................................... 123
Troubleshooting WMI Connections ................................................................ 124
Viewing WMI Connectivity Details ................................................................. 124
Last DNS resolution attempt ........................................................................ 125
Last ARP resolution attempt ......................................................................... 125
Last Endpoint Mapper connection attempt .................................................... 125
Last File and Printer Sharing connect attempt ............................................. 125
Last WMI connect attempt ........................................................................... 126
Fixing WMI Connectivity Issues ..................................................................... 126
SolarWinds WMI Providers Actions ................................................................. 126
Additional Options ........................................................................................ 127
Additional Requirement for Windows XP ....................................................... 128
Verifying WMI Connectivity .......................................................................... 128

Patch Manager Agents ..................................................................................... 130
Agent Requirements ......................................................................................... 130
Deploying Agents ............................................................................................ 130
Deploy from the Patch Manager Console ....................................................... 131
Offline Deployment ........................................................................................ 132
<table>
<thead>
<tr>
<th>Manual</th>
<th>132</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approving Agents</td>
<td>133</td>
</tr>
<tr>
<td>Configuring Agents</td>
<td>134</td>
</tr>
<tr>
<td><strong>Using the Patch Manager Web Console</strong></td>
<td><strong>135</strong></td>
</tr>
<tr>
<td>Using the Web Console Notification Bar</td>
<td>135</td>
</tr>
<tr>
<td>Viewing Consolidated Patch Manager Data</td>
<td>135</td>
</tr>
<tr>
<td>Default Tabs and Related Views</td>
<td>135</td>
</tr>
<tr>
<td>Default Home Tab Views</td>
<td>136</td>
</tr>
<tr>
<td>Default Patches Tab Views</td>
<td>136</td>
</tr>
<tr>
<td>Customizing Views</td>
<td>137</td>
</tr>
<tr>
<td><strong>Administrating the Patch Manager Web Console</strong></td>
<td><strong>138</strong></td>
</tr>
<tr>
<td>Creating and Managing Views</td>
<td>138</td>
</tr>
<tr>
<td>Creating New Views</td>
<td>138</td>
</tr>
<tr>
<td>Editing Existing Views</td>
<td>139</td>
</tr>
<tr>
<td>Adding Custom Views to Menu Bars</td>
<td>140</td>
</tr>
<tr>
<td>Customizing Menu Bars</td>
<td>140</td>
</tr>
<tr>
<td>Creating New Menu Bars</td>
<td>140</td>
</tr>
<tr>
<td>Editing Existing Menu Bars</td>
<td>141</td>
</tr>
<tr>
<td>Adding Custom Links to Menu Bars</td>
<td>141</td>
</tr>
<tr>
<td>Customizing the Web Console Banner</td>
<td>142</td>
</tr>
<tr>
<td>Setting the Web Console Refresh Rate</td>
<td>142</td>
</tr>
<tr>
<td><strong>Maintaining Patch Manager</strong></td>
<td><strong>144</strong></td>
</tr>
<tr>
<td>Managing Patch Manager Tasks</td>
<td>144</td>
</tr>
<tr>
<td>Managing Scheduled Tasks</td>
<td>144</td>
</tr>
<tr>
<td>Managing Task History</td>
<td>145</td>
</tr>
</tbody>
</table>
Integrating Patch Manager and ConfigMgr ............................................................. 164
Verifying that Patch Manager is Integrated with ConfigMgr .................................... 166
Publishing Third-party Updates .............................................................................. 168
Verifying SUP is Configured to Synchronize Locally Published Updates ................. 168
Publishing Third-party Updates without Direct Download URL ......................... 169
Publishing Third-party Updates with Direct Download URL ............................... 170
Deploying Third-party Updates ............................................................................. 171
Installing Third-party Updates in Client Machine ................................................ 174
Managing Published Third-party Updates .............................................................. 175
Creating a Third-party Updates View .................................................................... 175
Managing Publishing Servers .............................................................................. 176
Importing and Exporting Catalogs ....................................................................... 176
Creating and Publishing Software Packages ....................................................... 178
Managing Third-party Packages .......................................................................... 181
Administrating WSUS Using Patch Manager ........................................................ 183
Synchronizing WSUS Servers ............................................................................... 183
Cleaning Up WSUS Servers ................................................................................. 184
Repairing and Maintaining the Windows Update Agent ........................................ 185
Administrating Windows Update Agent Local Policy ........................................... 185
Provisioning the WMI Providers ........................................................................... 186
Fixing WMI Connectivity Issues ........................................................................... 186
SolarWinds WMI Providers Actions ....................................................................... 187
Additional Options ............................................................................................... 187
Additional Requirement for Windows XP ............................................................. 188
Verifying WMI Connectivity ................................................................................ 188

Appendix B ............................................................................................................. 190
Patch Manager Server Settings ............................................................... 190
Automation Server Settings ...................................................................... 190
Application Server Settings ....................................................................... 192
Management Server Settings ..................................................................... 197
Appendix C .................................................................................................. 199
Patch Manager Web Console User Settings ............................................... 199
Appendix D .................................................................................................. 202
SolarWinds Orion Web Console Components .............................................. 202
Appendix E .................................................................................................. 205
Advanced Setup CLI Commands ................................................................. 205
Appendix F .................................................................................................. 207
Table of Status Icons .................................................................................. 207
Appendix G .................................................................................................. 209
First Time Usage Wizard FAQ ..................................................................... 209
  Why does it take so much time to install an update? ................................. 209
  What is the First Time Usage Wizard doing when it is installing packages? 209
  How can I decrease the amount of time the wizard takes? ......................... 209
  Can I mass add computers? ..................................................................... 209
Introduction

SolarWinds Patch Manager extends native Microsoft Windows Server Update Services (WSUS) and Microsoft System Center Configuration Manager (ConfigMgr) functionality using an enhanced Microsoft Management Console (MMC) interface. For ConfigMgr, Patch Manager integrates with the new ribbon-style console to extend ConfigMgr's functionality.

The Patch Manager console has the following functionality:

- View and manage Microsoft updates on your WSUS server or ConfigMgr software update point (SUP).
- Publish and manage third party updates using built-in WSUS functionality in both WSUS and ConfigMgr environments.
- Deploy updates on demand by leveraging the Windows Update Agent on target systems.
- Execute configuration management tasks on one or more managed computers.
- Run flexible and detailed reports about the updates and assets in your publishing environment.

Patch Manager is composed of several components to integrate with the WSUS or ConfigMgr servers in your publishing environment. Each of the following components is modular to allow a high level of flexibility in large or complex deployment scenarios:

- **Patch Manager Server**
- **Microsoft SQL Server**
- **Administration Console**
- **Web Console**
- **Managed Computers**
- **Agents (Optional)**

The following diagram illustrates a typical Patch Manager installation. For additional information about alternative deployment scenarios, see "Advanced Deployment Scenarios" in the Administrator Guide "Advanced Deployment Scenarios" on page 152.

_A Typical Patch Manager Deployment Scenario_
Note: In ConfigMgr environments, the WSUS Server in this diagram corresponds to the ConfigMgr software update point (SUP).

**Patch Manager Server**

The Patch Manager server consists of several components, which you can install on a single server or distribute across several servers by the three Patch Manager server roles.

**Application Server**

Interfaces with the MMC-based or integrated ConfigMgr administration consoles, and manages all communication between the console and the rest of the Patch Manager environment.

**Management Server**

Maintains all inventory and discovery data for specific systems in the Patch Manager environment. Each Management role server has a defined collection of managed entities, specified by their corresponding domain, workgroup, or WSUS server.

**Automation Server**

Manages the local Patch Manager worker processes on each Patch Manager server. The worker processes perform the inventory and configuration management tasks and interface with the Windows Management Instrumentation (WMI) providers to collect data and supervise remote management capabilities.
The Express installation option installs all three server roles and the Patch Manager console on a single server. You can also deploy multiple Patch Manager servers in one or more of these roles in a distributed environment.

By default, the first Patch Manager server you install is the Primary Application Server (PAS). It contains the primary configuration management database for the application and also serves as a Certificate Authority for the certificates used to register and encrypt Patch Manager communications.

All Patch Manager servers run as the EminentWare Data Grid Server service, named for the original developer of the product. This service runs automatically at system startup, and manages all aspects of the Patch Manager server except those provided by SQL Server.

**Microsoft SQL Server**

Patch Manager stores all of its configuration and inventory data on a Microsoft SQL Server database. You can install a local copy of SQL Server Express directly on the Patch Manager server, or connect Patch Manager to a remote SQL server.

**Administration Console**

The Patch Manager administration console is an MMC 3.0-based snap-in that connects to the Patch Manager PAS. In ConfigMgr environments, there is an additional Patch Manager console integrated with the ConfigMgr console. In any case, you can install the administration console directly on the Patch Manager server, or on one or more remote administration workstations.

**Web Console**

The Patch Manager web console is a read-only interface that displays detailed information from a Patch Manager Application role server. You can install the web console server on any Windows web server that can connect to the Patch Manager Application role server. Access the web console from any computer with access to the host web server's website.

**Managed Computers**

Managed computers include all WSUS servers, ConfigMgr servers, and managed clients in the enterprise. For optimal inventory and reporting functionality, deploy the Patch Manager Windows Management Interface (WMI) providers to all managed clients.

**Agents (Optional)**

Agents are an optional component that you can choose to deploy to managed computers. Agents are usually deployed to computers if the computers cannot be managed directly over the network with WMI.
Installing Patch Manager

Install Patch Manager on a server that exceeds or meets the minimum requirements. After installing the initial Patch Manager server, use the automated configuration wizards to complete setup. This section addresses the following topics regarding the initial setup:

- Requirements
- Deployment Best Practices
- Installing the Patch Manager PAS
- Patch Manager Licensing

Requirements

The following table provides the minimum requirements for a SolarWinds Patch Manager installation.

<table>
<thead>
<tr>
<th>SOFTWARE/HARDWARE</th>
<th>REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System (Patch Manager servers and consoles)</td>
<td>Install the Patch Manager web console server on a 32- or 64-bit computer running IIS on any of the following operating systems:</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 with SP1</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Additionally, SolarWinds supports the following operating systems for evaluation purposes:</td>
</tr>
<tr>
<td></td>
<td>• Windows 7</td>
</tr>
<tr>
<td></td>
<td>• Windows 7 SP1</td>
</tr>
<tr>
<td></td>
<td>• Windows 8</td>
</tr>
<tr>
<td></td>
<td>• Windows 8.1</td>
</tr>
<tr>
<td></td>
<td>• Windows 10</td>
</tr>
<tr>
<td>Operating System (managed clients)</td>
<td>Patch Manager manages 32- or 64-bit computers running any of the following operating systems:</td>
</tr>
<tr>
<td></td>
<td>• Windows XP Professional SP3 or later</td>
</tr>
<tr>
<td></td>
<td>• Windows Vista Business, Enterprise, or Ultimate SP2 or later</td>
</tr>
<tr>
<td></td>
<td>• Windows 7 Professional, Enterprise, or Ultimate</td>
</tr>
<tr>
<td></td>
<td>• Windows 8</td>
</tr>
</tbody>
</table>
| Operating System (web console) | Windows 8.1  
|                               | Windows Server 2003 SP2 or later  
|                               | Windows Server 2003 R2 SP2 or later  
|                               | Windows Server 2008 SP2 or later  
|                               | Windows Server 2008 R2  
|                               | Windows Server 2012  
|                               | Windows Server 2012 R2  
|                               | Windows 10  

Install the Patch Manager web console server on a 32- or 64-bit computer running IIS on any of the following operating systems:
- Windows Server 2008 R2 with SP1
- Windows Server 2012
- Windows Server 2012 R2

Additionally, SolarWinds supports the following operating systems for evaluation purposes:
- Windows 7
- Windows 7 SP1
- Windows 8
- Windows 8.1
- Windows 10

| Internet Browser (web console) | The Patch Manager web console is compatible with the following Internet browsers:
|                               | - IE11, Edge (Spartan)
|                               | - Firefox - two most recent versions at the time of shipping
|                               | - Chrome - two most recent versions at the time of shipping
|                               | - IE6, IE7, IE8, IE9, IE10 and other non-supported browsers are not supported but are not blocked.
|                               | - Safari - latest version

| CPU Speed | Pentium 1.5 GHz equivalent or faster (x86, x64, or AMD64)  
|           | Dual Core recommended

<p>| Memory | 1 GB RAM |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard Drive Space</td>
<td>5 GB*</td>
</tr>
<tr>
<td></td>
<td>10 GB or more recommended</td>
</tr>
<tr>
<td>Database</td>
<td>Patch Manager is compatible with Microsoft SQL Server instances running the following versions:</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2008</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2008 R2 SP1</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2008 R2 SP2</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2008 R2 SP3</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2008 SP1</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2008 SP2</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2008 SP3</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2008 SP4</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2012</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2012 SP1</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2012 SP2</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2012 SP3</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2014</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2014 SP1</td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2016</td>
</tr>
<tr>
<td></td>
<td>Express, Standard, or Enterprise editions</td>
</tr>
<tr>
<td>WSUS</td>
<td>Patch Manager supports WSUS servers running the following versions:</td>
</tr>
<tr>
<td></td>
<td>- Windows Server Update Services 3.0 SP2 or later with Microsoft KB2734608 applied</td>
</tr>
<tr>
<td></td>
<td>- Windows Server Update Services 6.0 installed on Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>- Windows Server Update Services 6.2 installed on Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>- Windows Server Update Services 6.3 installed on Windows Server 2012 R2</td>
</tr>
<tr>
<td>ConfigMgr (if applicable)</td>
<td>Patch Manager supports SCCM (ConfigMgr) servers running the following versions:</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• System Center Configuration Manager 2007 SP2 or later</td>
</tr>
<tr>
<td></td>
<td>• System Center Configuration Manager 2012</td>
</tr>
<tr>
<td></td>
<td>• System Center Configuration Manager 2012 R2</td>
</tr>
<tr>
<td></td>
<td>• System Center Configuration Manager 1511</td>
</tr>
<tr>
<td></td>
<td>• System Center Configuration Manager 1602</td>
</tr>
<tr>
<td>Note:</td>
<td>System Center Configuration Manager must be installed before Patch Manager.</td>
</tr>
<tr>
<td>Visual C++ Runtime</td>
<td>Microsoft Visual C++ Secure Runtime 9.0 SP1</td>
</tr>
<tr>
<td>Note:</td>
<td>The Patch Manager installer installs this component if it is not already installed.</td>
</tr>
<tr>
<td>Web Server</td>
<td>Microsoft IIS 6.0 or later</td>
</tr>
<tr>
<td>(web console server)</td>
<td>.NET Framework</td>
</tr>
<tr>
<td></td>
<td>• Version 3.5 for Patch Manager server</td>
</tr>
<tr>
<td></td>
<td>• Version 4.5 for Web server</td>
</tr>
<tr>
<td>Internet Access</td>
<td>Install Patch Manager on a server that can access the following:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.microsoft.com">www.microsoft.com</a> if you do not have a local copy of the WSUS installer</td>
</tr>
<tr>
<td></td>
<td>3pupcontent.solarwinds.com if you plan on evaluating the third party update functionality</td>
</tr>
<tr>
<td>Ports</td>
<td>Server and console components use port 4092 TCP</td>
</tr>
<tr>
<td></td>
<td>Servers communicate with managed computers using the following ports:</td>
</tr>
<tr>
<td></td>
<td>• 135 TCP</td>
</tr>
<tr>
<td></td>
<td>• 445 TCP</td>
</tr>
<tr>
<td></td>
<td>• Dynamic ports 1024 to 65536 (varies by operating system)</td>
</tr>
</tbody>
</table>
The Patch Manager web console server uses the following ports:

- 8787 TCP
- 17777 TCP

*Note: Patch Manager is not likely to use the recommended 5-10 GB of hard drive space when properly managed. However, we recommend the higher capacity to accommodate fluctuations in space requirements over the course of operating the product.

**Notes on Windows Server 2008 R2 with SP1**

Complete the following additional setup tasks if you plan to use or manage servers running Windows Server 2008 R2 SP1 with Patch Manager:

- To ensure Remote Procedure Call (RPC) connectivity to deploy the WMI Provider, enable the WMI and Remote Administration Inbound rules on managed computers running Windows Firewall on Windows Server 2008. Windows Server 2008 blocks these firewall rules by default.
- If any workgroups are exclusively hosted on Windows Server 2008 or Windows Server 2008 R2 resources, enable and start the Computer Browser service and enable Network Discovery on at least one system in the workgroup. This system provides a Master Browser for the Managed Resource Enterprise Configuration Wizard.


**Port and Firewall Information**

The following sections describe the ports used in the Patch Manager environment.

**Port 135 TCP – RPC Endpoint Mapper**

The Patch Manager server uses this port to establish WMI connections to remote computers. It also uses this port to connect to the Service Control Manager (SCM) when it provisions the WMI providers dynamically on the remote computer.

Create a firewall exception to allow traffic from the Patch Manager server to your managed computers over this port. To do this if you are using Windows Firewall on your managed computers, enable the Inbound Rules in the **Windows Management Instrumentation (WMI)** group.
Port 445 TCP – SMB over TCP

The Patch Manager server uses this port when it provisions the WMI providers to a remote computer.

Enable File and Print Sharing on the client systems using the applicable network management tools.

Port 4092 – Console-to-Server Communication

The Patch Manager console uses this port to communicate to an independent Patch Manager application server. This is a one-way communication channel, so it only requires inbound TCP traffic on the application server.

Patch Manager servers in a distributed environment also use this port in the same manner for "downstream" communication. For example, the Patch Manager Primary Application Server (PAS) uses port 4092 to communicate with remote Patch Manager servers in secondary server roles.

Port 8787 TCP – Web Console Connections

By default, users connect to the Patch Manager web console server on port 8787. You can specify an alternative port in the SolarWinds Configuration Wizard on the server running the Patch Manager web console server.

Port 17777 TCP – SolarWinds Information Service

The SolarWinds Information Service (SWIS) facilities data exchange for the Patch Manager web console, along with the web console Application Programing Interface (API). Ensure this port is not blocked on servers running the Patch Manager web console server.

Port 389 TCP – Lightweight Directory Access Protocol

Patch Manager servers use this port for Active Directory authentication.

Dynamic Ports 1024-65536 – DCOM or RPC

WMI technology is based on Distributed Component Object Model (DCOM)/RPC communication. DCOM/RPC allocates the ports used by the server within a dynamic port range. This range is typically between 1024 and 65536. To configure these ports using Windows Firewall on your managed computers, enable the Inbound Rules in the Windows Management Instrumentation (WMI) group.

Deployment Best Practices

Follow these guidelines to help establish the optimum software and hardware configuration for deploying Patch Manager in your environment.

For information about deploying Patch Manager in a distributed environment, see "Advanced Deployment Scenarios".
Best deployment practice

Install Patch Manager on its own server, using a remote SQL server. For evaluation purposes, the installer deploys a local SQL server on the Patch Manager server.

Single server deployment

If you do not have a dedicated server for Patch Manager, install Patch Manager on the same server as a WSUS server. We do not recommend you co-locate these servers if you are installing Patch Manager with a local SQL server.

Installing the Patch Manager PAS

Complete the following procedure to install the initial Patch Manager server and console with the Primary Application Server (PAS) server role. Patch Manager installs components that you may be missing, such as C++ Runtime and/or Microsoft .NET Framework. Depending on the number of prerequisites your computer is missing and the number of components you are installing, the Patch Manager install process may take an hour or more. Pre-installing Microsoft .NET versions 4.0 and 3.5 SP1 may save you time during the installation process.

Notes:

- SolarWinds does not support Patch Manager installed on domain controller servers.
- You must set the server’s Region and Language to English (United States) when you install Patch Manager.
- If you plan on integrating Patch Manager with ConfigMgr, the ConfigMgr console must already be installed before installing Patch Manager consoles and servers.
- To install Patch Manager using a remote SQL instance, you must run the installer as an existing, fully qualified domain account with SysAdmin rights on the remote SQL server and select Advanced Install.
- Products using the Orion platform cannot be installed on a computer with a WSUS server on Windows 2003 x64.
- Install the Patch Manager PAS on Windows 2012 to manage WSUS v6 (Windows 2012) servers.
- Install the Patch Manager PAS on Windows 2012 R2 to manage WSUS v6.3 (Windows 2012 R2) servers.

To install the Patch Manager Primary Application Server:

1. Log on as an administrator to the server on which you want to install Patch Manager.
2. Temporarily disable any antivirus software.
3. Run the SolarWinds Patch Manager installer. The installer will prompt you to install any missing prerequisites.
4. Select Install the Patch Manager server components and Install the Patch Manager administration console, and click Next.
5. Click Next.

6. If you choose to install the Patch Manager Orion web interface and you do not have IIS installed, select Continue with Orion installation (Recommended). The installer will install IIS.

7. Accept the End User License Agreement (EULA), and then click Next.

8. Click Next to use the default installation folder. Click Browse to choose a different folder.

9. Select Express Install - Recommended, and click Next. This selection will also install a WSUS server and SQL Express.
   
   Note: If you have a WSUS server or an SQL instance you want to use, or if you want to install different server roles, select Advanced Install. To complete your PAS installation, select Primary Application Server (Recommended) when prompted.

10. Click Next. The Patch Manager components are installed.

11. Click Finish.

12. Configure the Microsoft Management Console for a WSUS or SCCM environment by selecting either the WSUS Extension Pack or the System Center Configuration Manager Extension Pack.

13. Click Continue.

14. Enter the local Administrator credentials, and click Save.

To install the Patch Manager Primary Application Server with ConfigMgr:

1. Log on as an administrator to the server on which you want to install Patch Manager.

2. Temporarily disable any antivirus software.

3. Run the SolarWinds Patch Manager installer. The installer will prompt you to install any missing prerequisites.

4. Select Patch Manager server components and Patch Manager administration console, and click Next.

5. Click Next.

6. Accept the End User License Agreement (EULA), and then click Next.

7. Click Next to use the default installation folder. Click Browse to choose a different folder.

8. Select Advanced Install, and then click Next.

9. Click Next. The Patch Manager components are installed.

10. Click Next to begin configuring your Patch Manager components.

11. Select an SQL server, enter the credentials, and then click Next.

12. Select Create a new database, and then click Next.

13. If you select a different role, enter the Patch Manager Primary Application Server information or select Provision this service offline, and click Next.

14. Enter the management group and ensure that Configure the Windows Firewall for the Server is selected.
15. Click **Next**.

16. If you do not have a WSUS server, select **Install the Patch Manager WSUS service (Recommended)**. If you already have your own WSUS server, select **I'll supply my own WSUS server**.

17. Click **Next**.

18. Select how Patch Manager should configure IIS.

19. Enter a location that Patch Manager can use to store updates locally.

20. Select **Provision the WSUS Server to the Patch Manager** to manage WSUS from Patch Manager.

21. Click **Next**.

22. Enter the administrator credentials for Patch Manager, and click **Next**.

23. Select your SQL instance and supply the credentials.

24. Click **Next**.

25. Select **Use the default service account** or enter different service account credentials for Patch Manager.

26. Click **Next**.

27. Click **Finish**.

**Patch Manager Licensing**

SolarWinds licenses Patch Manager according to its number of managed computers. Managed computers include all WSUS, ConfigMgr, and Patch Manager servers, along with all managed clients. The Primary Application Server (PAS) calculates the number of managed computers using two sources:

- The Enterprise > Managed Computers node
- The Administration and Reporting > Task History node

If you find you have inadvertently exceeded your product license, see the KB article, "The Patch Manager console says I'm over the allowed license count," [http://knowledgebase.solarwinds.com/kb/questions/3693/](http://knowledgebase.solarwinds.com/kb/questions/3693/) for steps to resolve the issue.

**Going from Evaluation to Production**

After you have purchased a license from SolarWinds, activate Patch Manager using the SolarWinds Licensing application. If you have not purchased a license, you can do so from the SolarWinds Licensing application, which links you to [www.solarwinds.com](http://www.solarwinds.com).

Note: If you have deployed multiple Patch Manager servers in various server roles, you only have to activate the Primary Application Server (PAS). By default, this is the first server you deployed.
**Licensing Servers with Internet Access**

Complete the following procedure to license your Patch Manager PAS if it has access to the Internet.

To license Patch Manager on a server with Internet access:

1. Click Start > All Programs > SolarWinds > Patch Manager > SolarWinds Licensing.
2. Click Enter Licensing Information.
3. Select I have internet access and an activation key.
4. Click the [http://customerportal.solarwinds.com](http://customerportal.solarwinds.com) link to access the customer portal on the SolarWinds web site.
5. Log on to the portal using your SolarWinds customer ID and password.
6. On the left navigation bar, click License Management.
7. Navigate to your product, choose an activation key from the Unregistered Licenses section, and then copy the activation key.
8. **If you cannot find an activation key in the Unregistered Licenses section**, contact SolarWinds customer support.
9. Return to the Activate Patch Manager window, and then enter the activation key in the Activation Key field.
10. **If you access Internet web sites through a proxy server**, select I access the internet through a proxy server, and then enter its proxy address and port.

Note: If your Patch Manager server accesses the Internet through an authenticated proxy server, complete the procedure for activating without Internet access instead.

11. Click Next.
12. Enter your email address and other registration information, and then click Next.

**Licensing Servers without Internet Access**

Complete the following procedure to license your Patch Manager PAS if it does not have access to the Internet.

To license Patch Manager on a server without Internet access:

1. Click Start > All Programs > SolarWinds > Patch Manager > SolarWinds Licensing.
2. Click Enter Licensing Information.
3. Select This server does not have internet access, and then click Next.
4. Click Copy Unique Machine ID.
5. Paste the copied data into a text editor document.
6. Transfer the document to a computer with Internet access.
7. On the computer with Internet access, complete the following steps:
a. Browse to http://customerportal.solarwinds.com/customerportal/LicenseManagement.aspx, and then log on to the portal with your SolarWinds customer ID and password.

b. Navigate to your product, and then click Manually Register License.

c. If the Manually Register License option is not available for your product, contact SolarWinds customer support.

d. Provide the Machine ID from Step 5, and then download your license key file.

8. Transfer the license key file to the Patch Manager server.

9. Return to the Activate Patch Manager window, browse to the license key file, and then click Next.

**Maintaining Licenses with License Manager**

**Maintaining licenses**

After you finish an Orion product installation, you are automatically prompted to activate your license. You can either activate your product straight away, or if you are under active maintenance, you can activate the license later, using the SolarWinds License Manager.

SolarWinds License Manager is an easily installed, free utility that gives you the ability to manage Orion licenses without contacting SolarWinds Customer Service.

SolarWinds License Manager provides the following capabilities:

- Deactivating licenses on one computer and activating them on another computer without contacting SolarWinds Customer Service
- Upgrading from one production license level to another
- Upgrading from evaluation licenses to production licenses

Note: To be able to use the License Manager, you need to have an active maintenance.

The following sections provide more information about the following License Manager-related topics:

- [License Manager Requirements](#)
- [Installing License Manager](#)
- [Activating SolarWinds Licenses](#)
- [Deactivating and Registering Licenses with the License Manager](#)
- [Upgrading and Synchronizing Licenses](#)

**License Manager Requirements**

The following table lists the requirements for SolarWinds License Manager.
<table>
<thead>
<tr>
<th><strong>ITEM</strong></th>
<th><strong>REQUIREMENT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Location</td>
<td>SolarWinds License Manager must be installed on the same computer as the products to be migrated.</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Computer must have access to the Internet.</td>
</tr>
<tr>
<td>.NET Framework</td>
<td>2.0 or later, links to the framework are included in the installation</td>
</tr>
<tr>
<td>Operating System</td>
<td>The following operating systems are supported:</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2008 and higher, including R2</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>■ Windows Vista</td>
</tr>
<tr>
<td></td>
<td>■ Windows 7</td>
</tr>
<tr>
<td></td>
<td>■ Windows 8</td>
</tr>
<tr>
<td>Browser</td>
<td>The following browsers are supported:</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 8 or later</td>
</tr>
<tr>
<td></td>
<td>Firefox 2.0 or later</td>
</tr>
<tr>
<td></td>
<td>Chrome latest version</td>
</tr>
</tbody>
</table>

Notes:

- SolarWinds License Manager does not reset Storage Manager, Virtualization Manager, Mobile Admin, Log & Event Manager, Web Help Desk, and DPA/Confio licenses.
- ipMonitor versions 10 or later are now supported by License Manager. You can reset ipMonitor licenses previous to version 10 by launching the ipMonitor Configuration Program, clicking Software Licensing, and then clicking Park License.
- License Manager must be installed on a computer with the correct time. If the time on the computer is off 24 hours in either direction from the Greenwich Mean Time clock, you will be unable to reset licenses. Time zone settings do not affect and do not cause this issue.

**Installing License Manager**

Install License Manager on the computer on which you want to activate, upgrade or synchronize your license or on which you want to deactivate currently licensed products.
Warning: You must install License Manager on a computer with the correct time. If the time on the computer is even slightly off, in either direction, from Greenwich Mean Time (GMT), you cannot reset licenses without contacting SolarWinds Customer Service. Time zone settings neither affect nor cause this issue.

To install License Manager via SolarWinds UI:

1. Click Start > All Programs > SolarWinds > SolarWinds License Manager Setup.
   Note: If problems with License Manager occur, download and install the latest version of License Manager.
2. Click Next to accept the SolarWinds EULA.
3. If you are prompted to install the SolarWinds License Manager application, click Install.

Downloading the License Manager from the Internet

To download and install the latest version of the License Manager:

2. Unzip the downloaded file, and then run LicenseManager.exe.

Activating Licenses with the License Manager

Activating licenses with the License Manager allows you to manage licenses for multiple SolarWinds products.

You need to activate your license after you have purchased and installed your Orion product, or after you purchase a license key for a currently installed evaluation version of your product.

To activate licenses with the License Manager:

1. Start the License Manager in your SolarWinds program folder.
   Note: If the License Manager is not installed on the computer, install it first. For more information, see Installing License Manager.
2. Click Activate next to the appropriate SolarWinds product.
3. Select whether you have access to the Internet or whether you want to activate your license offline.

Activating Licenses with Internet Access

If you have installed your SolarWinds product on a computer which is connected to the Internet, the license key will be activated via the Internet.
To activate the license, launch the Activation Wizard, and complete the following steps:

i. Select I have Internet access...

ii. Find out your activation key in the customer portal, and provide it in the Activation Key field.
   a. Browse to https://customerportal.solarwinds.com, and then log in using your Customer ID and password, or your individual user account information.
      Note: If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support at http://www.solarwinds.com/support/ticket/serviceticket.aspx.
   b. Under Licensing Management section on the top bar, select License Management.
   c. Browse to the appropriate SolarWinds product, and then click the plus sign next to the product to display your activation key.
   d. Copy your unregistered activation key for the appropriate SolarWinds product to the clipboard, and then paste it into the Activation Key field on the Activate NPM window.

iii. **If you are using a proxy server to access the Internet**, select I access the Internet through a proxy server, and then type the proxy address and port number.

iv. Click Next and complete the Activation Wizard.

**Activating Licenses Offline**

If the computer on which you are installing your Orion product is not connected to the Internet, you need to provide the unique machine ID in the SolarWinds customer portal, download the license key, and complete the activation on the offline computer.

To activate your SolarWinds license for an offline computer, launch the Activation Wizard and complete the following procedure:

i. On the Activate NPM screen, select This server does not have Internet access, and click Next.

ii. On the Activate Product window to finalize your registration, click Copy Unique Machine ID.

iii. Paste the copied data into a new document in a text editor, and then save the text document.

iv. Transfer the document to a computer with Internet access. For example, transfer the document to a shared location.

v. Log on to the SolarWinds customer portal and find out your activation key:
   a. Browse to https://customerportal.solarwinds.com from a computer with Internet access, and then log in using your Customer ID and password, or your individual user account information.
      Note: If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support at http://www.solarwinds.com/support/ticket/serviceticket.aspx.
   b. Click License Management.
   c. Browse to the appropriate SolarWinds product, such as Network Performance Monitor, and then click Manually Register License.
   d. Provide the Unique Machine ID you transferred earlier, and then download your license key.
   e. Transfer the license key to a shared location.

vi. Return to the offline computer where you have been running the activation wizard, and browse to the shared License Key File location from the Activate Product window.

vii. Click Next to continue.
4. Provide your customer data, and then complete the Activation Wizard.
   a. Provide your First Name, Last Name, Email address, and Phone Number to register your Orion product, and then click Next.
   b. Click Finish when your license is activated.
   c. Review and record the information provided on the License Status window, and then click Close.

**Deactivating and Registering Licenses with the License Manager**

If you decide to move your SolarWinds product to another server, you need to deactivate the license on the computer with the currently licensed product and reactivate it on the server with the new installation.

To be able to deactivate and reuse a license without contacting SolarWinds Customer Service, your product needs to be under active maintenance.

To deactivate a SolarWinds license and register it on another computer:

1. Log in to the computer where the currently licensed SolarWinds product is installed.
2. Click Start > All Programs > SolarWinds > SolarWinds License Manager.
3. Select products you want to deactivate on this computer, and then click Deactivate.
   - You can deactivate more than one product at the same time. In this case, the deactivation file will contain information about each product.
   - In certain products, you can deactivate licenses by using the internal licensing tool of the product.
4. Complete the deactivation wizard, and save the deactivation file.
5. Log in to the SolarWinds Customer Portal, and navigate to the License Management page.
6. Select your product instance, and click Deactivate license manually.
7. In the Manage License Deactivation page, browse for the deactivation file you created in License Manager, and click Upload.
   - Deactivated licenses are now available to activate on a new computer.
   - The new License Manager tool allows offline deactivation with a created file that can be uploaded to the customer portal.
8. Log in to the computer on which you want to install your products, and then begin installation.
9. When asked to specify your licenses, provide the appropriate information. The license you deactivated earlier is then assigned to the new installation.

**Upgrading and Synchronizing Licenses**

To upgrade a currently installed license:

1. Start the License Manager from the SolarWinds Program group.
2. Click Upgrade in the Action column next to the products for which you want to upgrade the license
on this computer.

3. Complete the Activation Wizard to upgrade your license.

**Synchronizing Licenses**

You can synchronize the data available on your customer portal with the data in the License Manager for most licenses.

Synchronizing might include:

- Updating the maintenance end date
- Registering the license anew, if it was reset

To synchronize a currently installed license with the SolarWinds Customer Portal:

1. Start the License Manager from the SolarWinds Program group.
2. Select the product whose license you want to synchronize, and then click Synchronize.
3. Click Synchronize again in the Synchronize Licenses window.

**Installing Your First Updates**

After you have installed Patch Manager, the **First Time Usage Wizard** displays. This wizard guides you through updating your first computers. If you want to launch the wizard after you have closed it, open the Patch Manager Console and select **Administration and Reporting**. Launch the wizard from the center pane. You must run Patch Manager as an administrator to run the First Time Usage Wizard.

Before you begin, have the following information available:

- Client computer information such as the host name or IP address
- Any additional local administrator credentials needed to access the client computers

**To patch your computer using the wizard:**

1. Click Tell Us About Your Environment.
2. Click Add a computer.
3. Enter the client computer information.
   - Tip: Click Resolve to have Patch Manager gather the information about the computer and fill out the rest of the information.
4. Click Add. You can add another computer or click Next to continue.
5. Enter credentials.
6. **If you want to use the credentials for all the computers you have added**, select Use these credentials for all the computers I've selected.
7. **If you want to use different credentials for some computers**, select Use these credentials, but let me enter different credentials for some computers.

8. Click Next.

Patch Manager uses the credentials you supplied to gather information about the computers, such as OS and installed software, configure them for use with Patch Manager, and determine which patches are available for the software.

If errors occur during this process, Patch Manager will alert you to the error and either provide the error or steps to correct the error. You also have the option to ignore the computers with errors.

After Patch Manager has successfully connected to and configured at least one client computer, the Install Patches option is available.

9. Click Install Patches.

10. Expand a computer and select a patch to apply.

    Tip: Select one or two available patches.

11. Click Finish. The patches are downloaded to the PAS, pushed to the client, and installed on the client.

For more information on what the wizard does, see the [First Time Usage Wizard FAQ](#).
Configuring Patch Manager

Initial Configuration

After you finish installing Patch Manager and installed your first updates, use the following wizards to further configure your Patch Manager server:

- Configuring Managed Resources
- Configuring Credentials and Credential Rings Rules
- Configuring Update Services
- Configuring Publishing Servers

Configuring Managed Resources

Use the Managed Resource Enterprise Configuration Wizard to configure the domains, workgroups, ConfigMgr Site servers, and WSUS servers you want to manage with Patch Manager.

To configure managed resources:

1. In the tree view in the left pane of the application, select **Patch Manager System Configuration**.
2. Click **Configure Managed Resources in your Enterprise** in the center pane.
3. On the first page of the wizard, select the appropriate domains and workgroups, and then click Next.
4. Manage ConfigMgr Site servers by adding them on the next page:
   a. Enter the server name, and then click **Resolve**.
   b. Fill in any missing information.
   c. Click **Add**.
   d. Repeat these steps for any additional ConfigMgr Site servers.
3. Click Next.
4. Manage WSUS servers (SUPs) by adding them on the next page:
   a. Enter the server name, and then click **Resolve**.
   b. Fill in any missing information.
   c. Click **Add**.
   d. Repeat these steps for any additional WSUS servers.
5. Click Next.
6. Patch Manager automatically creates the Managed Enterprise management group on the PAS. Click Next.
7. Review the summary screen, and then click Finish.

**Configuring Credentials and Credential Rings Rules**

Use the Credential and Credential Rings Rules Wizard to configure the credentials and credential rings rules Patch Manager needs to use to communicate with each of the managed resources defined in the previous section.

Patch Manager needs administrator permissions on managed resources to execute certain tasks. The following procedure allows you to specify the credentials for each group, or type of system. You can also limit Patch Manager users' access to resources using User Preferences and additional credential rings.

For additional information about managing access to Patch Manager resources, see "Managing Patch Manager Users and Security" on page 110.

**To configure credentials and credential rings rules:**

1. In the tree view in the left pane of the application, select **Patch Manager System Configuration**.
2. Click **Configure Security and User Management** in the center pane.
3. On the first page of the wizard, enter new credential information for each managed resource:
   a. In the User Name field, enter the username in UPN or flat format. For example, enter `DOMAIN\user`.
      
      Note: To add a common local computer account, enter `.\` before the username. For example, enter `.\administrator` to specify the local Administrator account for several computers.
      
      b. Enter and confirm the password for that user account.
      c. Click Add.
      d. Repeat these steps for any additional accounts you want to add.

2. Click Next.
3. **If you entered more than one credential**, map each resource to the appropriate credential:
   a. Select the resource you want to modify, and then click Change Assigned Credential.
   b. Select the credential you want to assign to that resource.
   c. Click OK.
   d. Repeat these steps to customize any additional resources.
4. Click Finish.

**Configuring Update Services**

Use the Third Party Updates Configuration Wizard to configure the Patch Manager server to synchronize with the SolarWinds third party update library.

Note: The evaluation version of Patch Manager includes access to a limited selection of third party updates. When you purchase a Patch Manager license, it includes complete access to all available catalogs.

To configure update services:

1. In the tree view in the left pane of the application, select Administration and Reporting, and then select Software Publishing.
2. Click Patch Manager Update Configuration Wizard from the Actions pane.
3. Verify you meet the requirements listed on the first page of the wizard:
   - You can browse to 3pupcontent.solarwinds.com from the server.
   - If you use a proxy server to access the Internet from the Patch Manager server, you have the server name, port number, and user credentials for the proxy server.
4. Click Next.
5. If the Patch Manager server accesses the Internet using a proxy server, enter the required information.
6. Click Next.
7. Click Start Connecting.
8. After the wizard scans for the available catalogs, click Next.
9. Select the products you want to synchronize with the Patch Manager server.
10. Click Next.
11. Configure the synchronization and notification preferences.
12. Click Finish.

**Configuring Publishing Servers**

Use the Server Publishing Setup Wizard to generate the WSUS self-signed publishing certificate, if necessary, and copy it to the Patch Manager server's certificate store.
Note: This task establishes a WMI connection with your publishing servers to configure them. If you installed Patch Manager on its own server and opted not to allow Patch Manager to automatically deploy the SolarWinds WMI Providers, this wizard will not work. Manually deploy the WMI Providers to your WSUS servers, or distribute the publishing certificate using Group Policy. For additional information about WMI connections, see "Managing Client WMI Connectivity" on page 122.

To configure Patch Manager as a publishing server:

1. In the tree view in the left pane of the application, select Administration and Reporting, and then select Software Publishing.
2. Click Server Publishing Setup Wizard from the Actions pane.
3. On the first page of the wizard, select the upstream WSUS server from the WSUS Server menu.
4. If the wizard returns details for an existing publishing certificate, select Distribute existing WSUS signing certificate to required servers.
5. If the wizard does not return details for an existing publishing certificate, select Create self-signed certificate.
6. Click Next.
7. Select the Patch Manager servers, publishing servers, and downstream WSUS servers to which you want to distribute the publishing certificate, and then click Next.
8. Review the summary screen for any errors, and then click Finish.
9. On the dialog that instructs you to configure your managed clients, click OK. Review the following section for additional information about this process.

Note: If you need to use Group Policy to configure your publishing servers, see "Using Group Policy to Configure Managed Clients" on page 41. The Group Policy procedure is the same whether you are configuring publishing servers or managed clients.

Configuring Managed Clients

There are two methods to provision the WSUS publishing certificate to all clients you want to manage, and then configure those clients to accept updates from the Patch Manager server:

- Using Group Policy to Configure Managed Clients (recommended)
- Configuring Clients from the Patch Manager Console (alternative)
Note: The second method requires WMI connections with the managed clients to configure them. If you opted not to allow Patch Manager to automatically deploy the SolarWinds WMI Providers to your managed clients, this method will not work. Manually deploy the WMI Providers, or use the Group Policy method to configure the clients. For additional information about WMI connections, see "Managing Client WMI Connectivity" on page 122.

Using Group Policy to Configure Managed Clients

Use Group Policy to configure managed clients if you do not want to use the WMI connections required by the Client Publishing Setup Wizard. This process consists of the following procedures:

- Exporting the WSUS Certificate
- Configuring the Group Policy Object

Exporting the WSUS Certificate

Use the following procedure to export the WSUS publishing certificate to a file from the Patch Manager console.

To export the WSUS publishing certificate to a file:

1. Open the Patch Manager console.
2. In the left pane, expand Enterprise > Update Services.
3. Select the WSUS server from which you want to export the certificate.
4. In the Actions pane (right), click Software Publishing Certificate.

   **If this dialog does not display the WSUS server's certificate information:**
   
   a. Click Close.
   
   b. Click Refresh Update Server in the Actions pane (right).
   

5. Click [...].
6. Click the Details tab.
7. Click Copy to File.
8. Click Next.
9. Leave DER encoded binary X.509 (.CER) selected, and then click Next.
10. Specify a name and location in the File name field, and then click Next.
11. Click Finish.
12. Click OK.
Configuring the Group Policy Object

Use the following procedures to configure the Group Policy Object (GPO) to push to managed clients. The GPO puts the WSUS certificate into the appropriate certificate stores and configures the managed clients to accept third-party updates from non-Microsoft sources.

To configure managed clients using Group Policy on Windows Server domains:

2. Create or edit a Group Policy Object to configure the clients.
4. Import the WSUS publishing certificate to the Trusted Root Certification Authorities and Trusted Publishers stores:
   a. Under Public Key Policies, select Trusted Root Certification Authorities.
   b. Click Action > Import.
   c. Click Next.
   d. Click Browse, and then browse to the certificate you saved in the previous procedure.
   e. Click Next.
   f. Click Next again.
   g. Click Finish.
   h. Click OK on success dialog.
   i. Repeat these steps for the Trusted Publishers certificate store.
5. Expand Computer Configuration > Administrative Templates > Windows Components, and then select Windows Update.
6. Enable the Allow signed updates from an intranet Microsoft update service location policy:
   a. In the center pane, select Allow signed updates from an intranet Microsoft update service location.
   b. Click Action > Edit.
   c. Select Enabled.
   d. Click OK.
Configuring Clients from the Patch Manager Console

Provided you have already provisioned your managed clients with the SolarWinds WMI Providers, use the following tasks in the Patch Manager console to configure those clients to receive third-party updates from Patch Manager:

- Client Certificate Management
- Windows Update Local Policy Management

Client Certificate Management

Use the Client Certificate Management task, also known as the Client Publishing Setup Wizard, to distribute and install the WSUS self-signed publishing certificate to managed clients.

To complete the Client Certificate Management task:

1. In the left pane of the Patch Manager console, select Administration and Reporting.
2. In the center pane, click Client Certificate Management.
3. On the Client Certificate Management window, specify the WSUS publishing certificate to distribute:

   a. Select Distribute and install Update Services Signing Certificate.
   b. If you want to distribute the certificate directly from the WSUS server, select Select certificate from WSUS server, and then select the WSUS server from the active menu.
   c. If you want to distribute the certificate from a .CER file, select Select certificate from file, and then click [...] to browse to the file location.

   If the managed clients require SSL for remote connections:

   a. Select Distribute and install Update Services Server SSL Certificate.
   b. Next to the File Name field, click [...] to browse to the file location.

4. Click Distribute.
5. Complete the Task Options Wizard to specify the target systems and schedule and/or execute the task. For additional information, see "The Task Options Wizard" on page 62.

After you complete this task, Patch Manager notifies you that you must configure Windows Update Group Policy on your managed clients to enable them to allow third-party updates from Patch Manager. The following section addresses this requirement using Local Policy. When possible, enable the requisite policy in Group Policy instead.
Windows Update Local Policy Management

Use the Windows Update Local Policy Management task to configure your managed clients to accept third-party updates from Patch Manager using Local Policy.

To complete the Windows Update Local Policy Management task:

1. In the left pane of the Patch Manager console, select Administration and Reporting.
2. In the center pane, click Windows Update Local Policy Management.
3. On the Windows Update Local Policy Settings window, create a new local policy template for the managed clients:
   a. Click the check box next to Allow signed content from intranet Microsoft update service location twice so the value in the State column is Enabled.
   b. Modify any other policies you want to configure for the managed clients.

Note: Changes made to Local Policy do not override any policies already enforced by Group Policy.

4. Click OK.
5. Complete the Task Options Wizard to specify the target systems and schedule and/or execute the task. For additional information, see "The Task Options Wizard" on page 62.

Configuring the Web Console

The Patch Manager web console is a read-only interface that displays detailed information from a Patch Manager Application role server. You can install the web console server on any Windows web server that can connect to the Patch Manager Application role server. Access the web console from any computer with access to the host web server's website.

This section addresses the following procedures:

- Adding the Patch Manager Module to an Orion Server
- Installing the Web Console Server on a Separate Server
- Configuring the Patch Manager Web Console

Adding the Patch Manager Module to an Orion Server

Complete the following procedure to add the Patch Manager web console as a new module on an existing SolarWinds Orion web console.

To add the Patch Manager module to an Orion server:

Note: You cannot use the SolarWinds-Orion-PM-v2.0-WebOnly.exe installer on an existing Orion web console server. Use the web-only installer to install all of the Orion Platform components along with the Patch Manager web console module on a separate web server.

2. Run the installer.

Note: The installer's initial verification steps may take several minutes to complete. At times during this process, the installer GUI may disappear.

3. Click Next to start the installation.

4. Accept the End User License Agreement (EULA), and then click Next.

5. **If the installer needs to update or install the Microsoft Visual C++ Secure Runtime**, click Next to proceed.

6. On the Select setup type screen, select Web Console Only, and then click Next.

7. On the Patch Manager Web Console Setup window, click Next.

Note: SolarWinds recommends you create a current backup of your Orion database before adding or removing modules. Do not proceed with this installation until you have a current backup.

8. Accept the End User License Agreement (EULA), and then click Next.

9. On the Orion Install Selection screen, leave Express Install - Recommended selected, and then click Next.

Note: Patch Manager and the Orion platform use different levels of security for SQL authentication. If you are installing web console server on the Patch Manager server, SolarWinds recommends installing the Patch Manager web console server with its own instance of SQL Server Express. If this is not possible, you must have mixed mode authentication enabled on the SQL server instance to share the same SQL instance with Patch Manager and the Patch Manager Orion integration.

10. Click Next to begin the installation.

11. On the SolarWinds Configuration Wizard window, click Next twice to configure the Patch Manager web module.

12. After the Configuration Wizard completes successfully, click Finish to exit the installer and launch the Orion web console.
Installing the Web Console Server on a Separate Server

Complete the following procedure to install the Patch Manager web console server on its own web server. This can be the Patch Manager server or a dedicated web server. For the web console to function, it must be able to connect to a Patch Manager Application role server.

Note: This procedure installs several SolarWinds Orion components. For a detailed list of these components, see "SolarWinds Orion Web Console Components" on page 202.

To install and configure the Patch Manager web console:

1. **If you want to install the web console server on the Patch Manager server**, run the Patch Manager installer and select Install the Patch Manager Orion web interface.
2. **If you want to install the web console server on a dedicated web server**, download and run Patch-Manager-v2.0-WebOnly.zip from the SolarWinds Customer Portal.
3. Click Next to start the installation wizard.
4. Accept the End User License Agreement (EULA), and then click Next.
5. Specify a custom installation folder, or accept the default.
6. Click Next.
7. Select the setup type. Select Express to install the Patch Manager web console with its own instance of SQL Server Express (recommended).

Note: Patch Manager and the Orion platform use different levels of security for SQL authentication. If you are installing web console server on the Patch Manager server, SolarWinds recommends installing the Patch Manager web console server with its own instance of SQL Server Express. If this is not possible, you must have mixed mode authentication enabled on the SQL server instance to share the same SQL instance with Patch Manager and the Patch Manager Orion integration.

8. Click Next.
9. Click Next. After the installer finishes, it launches the SolarWinds Configuration Wizard.
10. After the SolarWinds Configuration Wizard finishes, click Finish to launch the Patch Manager web console.

Configuring the Patch Manager Web Console

After you launch the Patch Manager web console for the first time, complete the following procedure to configure it for first use.

To configure the Patch Manager web console:
1. On the Discovery Central web page, click Go to Orion Home.
2. Click the hyperlink in any of the resources to add your Patch Manager server:
   a. In the Server name or IP address field, enter the hostname or IP address of your Patch Manager server.
   b. In the Port field, specify a port or accept the default.
   c. In the Windows Credentials section, specify the username and password to use to access the Patch Manager server.
   d. Click Test.
   e. Click Submit.
3. To view Patch Manager resources, click the Patches tab.

**Administrative Configuration**

The following configuration procedures are optional, depending on your environment and how you plan on using Patch Manager.

- Configuring Email Settings
- Configuring Proxy Settings
- Creating a Third Party Updates View

**Configuring Email Settings**

When you create tasks in Patch Manager, you have the option to configure email notifications for when the task is finished. For this option to work, you need to configure SMTP settings on the Patch Manager server.

To configure SMTP settings on the Patch Manager server:

1. In the left pane of the Patch Manager console, expand Patch Manager System Configuration > Patch Manager Servers, and then select Application Servers.
2. In the upper-center pane, select the Patch Manager server.
3. In the lower-center pane, click the Application Server Settings tab.
4. Filter the Category column for Email Configuration:
   a. On the Category column, click ⌫.
   b. Select Email Configuration.
5. Select each of the settings in the Email Configuration category, and then click Modify Setting in the Actions pane (right) to open a dialog for that setting.
6. Modify the settings as appropriate, and then click OK to close the dialog. For additional information, see "Email Configuration" on page 193.

**Configuring Proxy Settings**

Both the Patch Manager console and Application role server need to connect to the Internet. If you require either component to connect to the Internet using a proxy server, enter the proxy server information in the applicable dialogs.

**Configuring Console Proxy Settings**

Complete the following procedure to configure proxy settings for connections from the Patch Manager console.

To configure proxy settings for the console:

1. In the left pane of the Patch Manager console, select Administration and Reporting.
2. In the center pane, click General Settings.
3. Click Proxy Configuration.
4. In the Console Proxy Settings window, select Use a proxy server while synchronizing, and then complete the form for your environment.
5. Click OK to save your settings and close the dialog.

**Configuring Server Proxy Settings**

Complete the following procedure to configure proxy settings for connections from the Patch Manager Application role server(s).

To configure proxy settings for the Patch Manager Application server:

1. In the left pane of the Patch Manager console, expand Administration and Reporting, and then select Software Publishing.
2. In the Actions pane (right), click Synchronization Settings.
3. In the Third Party Updates Options window, click the Proxy Settings tab.
4. Select Use a proxy server when synchronizing, and then complete the form for your environment.
5. Click OK to save your settings and close the dialog.

**Creating a Third Party Updates View**

One extension Patch Manager offers is the ability to publish, manage, and deploy third party updates from the Patch Manager server. Create a third party updates view in the Patch Manager console to separate these types of updates from the Microsoft updates you would normally see in your WSUS console.
The procedure for this is different for the Patch Manager console in WSUS, ConfigMgr 2007, and ConfigMgr environments. See the applicable section for the correct procedure:

- [Third-party Updates View for WSUS](#)
- [Saved Searches in ConfigMgr 2007](#)
- Creating a Third Party Updates View for ConfigMgr

**Third-party Updates View for WSUS**

Complete the following procedure to create a third-party updates node under your WSUS server in the Patch Manager console.

To create a third party updates view in WSUS environments:

1. In the left pane of the Patch Manager console, expand Enterprise > Update Services, and then expand your WSUS server.
2. Under your WSUS server, select Updates.
3. In the Actions pane (right), click New Update View.
4. Under Step 1: Select properties, select Updates have a specific approval and installation status and Updates are from Microsoft Update, Third Parties, or both.
5. Under Step 2: Edit the properties (click an underlined value), define the properties:
   a. Click any update source.
   b. Select Only updates from a Third Party.
   c. Click OK.
   d. Click approved and needed.
   e. In the Approved State menu, select All.
   f. In the Update Status menu, select Any.
   g. Click OK.
6. Under Step 3: Specify the update view name and description, enter a name and description for the new view.
7. Click OK.

**Saved Searches in ConfigMgr 2007**

ConfigMgr 2007 uses search folders to save searches in the ConfigMgr console. Search folders make it easy to differentiate between third-party update vendors.

To create a search folder in ConfigMgr 2007 for third-party updates:
1. In the left pane of the ConfigMgr console, expand Site Database > Computer Management > Software Updates > Update Repository.
2. Right-click Search Folders, and then select New Search Folder. The system displays the Search Folder Criteria window.
3. In the Step 1 area, select Vendor.
4. In the Step 2 area, click the underlined value, and then select the vendor for which you want to create the search folder.
5. In the Step 3 area, select Search all folders under this feature.
6. In the Step 4 area, enter a name for the search folder. For example, enter the name of the vendor you selected in Step 2.
7. Click OK.
Getting Started with Third Party Updates

This chapter addresses the publishing and reporting capabilities of Patch Manager. Review the following sections to get started with Patch Manager:

- Publishing Trial Updates
- Approving Updates
- Installing Updates

Note: The "Approving Updates" and "Installing Updates" sections do not apply to ConfigMgr environments. If you use ConfigMgr to manage your updates, use the typical ConfigMgr methods to deploy the updates you publish using Patch Manager.

Publishing Trial Updates

If you configured third party updates, the next step is to publish some trial packages to your WSUS server. For evaluation purposes, we recommend you complete the following procedures in this order:

- Publishing Adobe Reader Updates
- Publishing Java Runtime Environment Updates
- Publishing Adobe Flash Updates

Note: For ConfigMgr instructions see Appendix A: "System Center Configuration Manager 2012 and 2012 R2 Procedures" on page 164.

Publishing Adobe Reader Updates

Use the Publishing Wizard to download the Adobe Reader update package and copy the installation file and update definition to the WSUS server.

To publish the Adobe Reader updates:

1. In the left pane of the Patch Manager console, expand Administration and Reporting > Software Publishing.
3. In the center pane, select the Reader <version> Update package you want to publish.
4. In the Actions pane (right), click Publish Packages.
5. Click Next.
6. After the publishing wizard downloads the package, select it, and then click Next.
7. Click Finish.
Publishing Java Runtime Environment Updates

Use the Package Download Assistant to download the Java Runtime Environment update files. Then use the Publishing Wizard to copy the installation file and update definition to the WSUS server.

The following video illustrates the steps in this procedure:

"Prevent Failed Java Updates," http://www.youtube.com/watch?v=-SBd_9jinRY

To publish the Java Runtime Environment updates:

1. In the left pane of the Patch Manager console, expand Administration and Reporting > Software Publishing.
2. Select Sun Packages.
3. In the center pane, select a Java Runtime Environment (JRE) update that you want to publish.
4. In the Actions pane (right), click Download Content.
5. Click OK.
6. In the Package Download Assistant window, double-click the download link.
7. Select Accept License Agreement, and then download the following files:
   - Windows x86 Offline
   - Windows x64
8. Return to the Package Download Assistant window, and then click Import Source.
9. Browse to the folder that contains the file you want to import, and then click Open.

Note: The file you select here must match the update you selected in Step 3. The Package Download Assistant provides the correct filename by default, so you do not need to select the file after you browse to the appropriate folder.

10. Click OK.

11. **If you want to publish another JRE update**, select it back in the Patch Manager console, and then import the file into the Patch Manager server:
   a. In the Actions pane (right), click Download Content.
   b. Click OK.
   c. On the Package Download Assistant window, click Import Source.
   d. Browse to the file you want to import, and then click Open.
   e. Click OK.
   f. Repeat these steps for any other JRE updates for which you want to import files.
12. To view the files you imported, click Refresh in the Actions pane (right).
13. Select the JRE update packages you want to publish.
14. In the Actions pane (right), click Publish Packages.
15. Click Next.
16. Click Finish.

**Publishing Adobe Flash Updates**

Use the Package Download Assistant to download the Adobe Flash update files. Then use the Publishing Wizard to copy the installation file and update definition to the WSUS server.

To publish the Adobe Flash updates:

1. In the left pane of the Patch Manager console, expand Administration and Reporting > Software Publishing.
2. Select Adobe Packages.
3. In the center pane, select the Flash Player <version> ActiveX package you want to publish.
4. In the Actions pane (right), click Download Content.
5. Click OK.
6. In the Package Download Assistant window, double-click the download link.
7. Download the archive for the version you want to publish.
8. Extract the contents of the archive to your local computer.
9. Return to the Package Download Assistant window, and then click Import Source.
10. Browse to the folder that contains the file you want to import, and then click Open.

Note: The file you select here must match the update you selected in Step 3. The Package Download Assistant provides the correct filename by default, so you do not need to select the file after you browse to the appropriate folder.

11. Click OK.
12. To view the files you imported, click Refresh in the Actions pane (right).
13. Select the Flash update packages you want to publish.
14. In the Actions pane (right), click Publish Packages.
15. Click Next.
16. Click Finish.
Approving Updates

After you have published the updates you want to evaluate, approve them for the appropriate WSUS target groups. Complete the following procedure to approve any update from the Patch Manager console.

Note: This section does not apply to ConfigMgr environments. If you use ConfigMgr to manage your updates, use the ConfigMgr console to deploy the updates you publish using Patch Manager.

To approve published updates:

1. In the left pane of the Patch Manager console, expand Enterprise > Update Services > Your WSUS Server > Updates.
2. Select your third party updates view.
3. In the center pane, select one or more of the update packages you published. Use Ctrl+click to select multiple packages.
4. In the Actions pane (right), click Approve.
5. On the Approve Updates window, select the WSUS computer groups for which you want to approve the updates. Use Ctrl+click to select multiple groups.
6. At the top of the window, click the appropriate approval option.
7. Click OK.
8. On the Approval Progress window, click Close.

Installing Updates

Use the Update Management task to install updates on a WSUS server on the approved target systems. The following procedure is an alternative to waiting for the Windows Update Agent on the target systems to sync with the WSUS server for scheduled updates.

Note: This section does not apply to ConfigMgr environments. If you use ConfigMgr to manage your updates, use the ConfigMgr console to deploy the updates you publish using Patch Manager.

To deploy updates using the Update Management task:

1. In the left pane of the Patch Manager console, expand Enterprise > Update Services > Your WSUS Server > Updates.
2. Select your third party updates view. If you have not yet created this view, see "Creating a Third Party Updates View" on page 48.
3. In the center pane, select one or more of the update packages you published. Use Ctrl+click to select multiple packages.
4. In the Actions pane (right), click Update Management.
5. On the Update Management window, click OK.
6. In the Task Options Wizard window, add the computers on which you want to install the updates.
7. Click Next.

8. Complete the Scheduling and Notification Options form, and then click Next.

9. Click Finish.
Using the Patch Manager Administration Console

The Patch Manager administration console (Patch Manager console) is an MMC 3.0-based snap-in that connects to the Patch Manager data grid server. Use the Patch Manager console to view, manage, and deploy updates, as well as perform a variety of other administrative functions.

ConfigMgr Note: The MMC-based Patch Manager console is available regardless of the Microsoft product you are extending. Although you cannot perform all administrative functions from within the ConfigMgr console, all of the Patch Manager functionality is available in the stand-alone MMC-based console.

This chapter addresses the following components of the Patch Manager console:

- **Optional Product Features**
- **The Navigation Pane**
- **The Data Grid Pane**
- **The Task Options Wizard**
- **Patch Manager Computer Groups**

Optional Product Features

During the initial configuration, Patch Manager gives you the option to select from the following options on the Product Features Selection dialog:

- WSUS Extension Pack
- System Center Configuration Manager Extension Pack

Even though you can run both extension packs with a single Patch Manager license, they each provide certain features that the other does not. Select the appropriate extension pack(s) when you first configure your Patch Manager server, or use the procedure in this section to add features later.

Extension Pack Features

Patch Manager includes the following features for each extension pack.

Windows Server Update Services (WSUS)

If you select WSUS Extension Pack when you configure Patch Manager, you will see these WSUS-specific features.
- WSUS tasks in the Enterprise > Update Services node
- The Update Management and Update Management Wizard tasks
- The Inventory task
- WSUS Reports in the Administration and Reporting > Reporting node

**System Center Configuration Manager (ConfigMgr)**

If you select System Center Configuration Manager Extension Pack when you configure Patch Manager, you will see these ConfigMgr-specific features.

- The Enterprise > Configuration Manager Site Servers node
- ConfigMgr tasks/tabs in Computer Explorer
- The client management and health monitoring tasks
- The Configuration Manager agent configuration tasks

**Cross-compatibility**

The following WSUS Extension Pack features are sometimes useful in ConfigMgr environments:

- The Update Management and Update Management Wizard tasks
- The Inventory task
- WSUS Reports in the Administration and Reporting > Reporting node

The WMI Maintenance and Repair task related to the ConfigMgr Extension Pack is sometimes useful in WSUS environments.

**Adding Extension Pack Features Later**

If you decide to add features from either of these extension packs after the initial configuration phase, complete the following procedure.

To add extension pack features after configuring Patch Manager:

1. Open the Patch Manager console.
2. In the left pane, select Patch Manager System Configuration.
3. In the center pane, click Select Products and Features.
4. Select the extension pack(s) you want, and then click Continue.
5. To refresh your options in the Actions pane (right), click Refresh at the top of the Actions pane.
6. To refresh your options in the Navigation pane (left), restart the Patch Manager console.

**The Navigation Pane**

The navigation pane is the left pane of the Patch Manager console. It consists of the following nodes:
The Enterprise Node

The Enterprise node contains all of the resources you manage with Patch Manager. It consists of the following child nodes:

**Update Services**

This node contains a child node for each WSUS server you manage with Patch Manager. Use this node to view and manage updates, computers, and WSUS groups on the selected WSUS server.

**Configuration Manager Site Servers**

This node contains a child node for each ConfigMgr 2007 site server you manage with Patch Manager. Use this node to view and manage collections on the selected ConfigMgr site server.

**Microsoft Windows Network**

This node contains a child node for each domain, workgroup, and/or Patch Manager computer group available to the Patch Manager application server. Aside from the Patch Manager computer groups, which you add yourself, this node replicates the Patch Manager application server’s Windows network browser.

**Managed Computers**

This node displays the list of computers included in one or more Managed Computer inventory events. This node also displays all Patch Manager and WSUS servers.

The Administration and Reporting Node

The Administration and Reporting node contains a variety of day-to-day operational tasks and views. It consists of the following child nodes:

**Software Publishing**

This node contains a child node for each third-party update vendor you are synchronizing, which displays all of the updates for the selected vendor. It also contains a Rules node, which lists all of your software publishing rules.

**Task History**

This node displays a list of past Patch Manager tasks, along with details about whether the task completed or failed.
Scheduled Tasks

This node displays a list of scheduled Patch Manager tasks. Use this node to view, manage, or run previously-scheduled tasks.

Active Tasks

This node provides a real-time view of the progress of all active Patch Manager tasks.

Reporting

This node contains a child node for the following report containers:

- WSUS Reports
- System Center Configuration Manager Reports
- Configuration Management Reports
- Task History Reports

Use this node to view, run, manage, and create pre-configured and custom reports.

The Patch Manager System Configuration Node

The Patch Manager System Configuration node contains a variety of one-time configuration tasks and management views. It consists of the following child nodes:

Management Groups

This node contains a child node for each Patch Manager Management Group. A Management Group is a container of computers managed by a single Patch Manager server in the Management role. By default, this node consists of the single Management Group, Managed Enterprise.

Patch Manager Servers

This node contains a child node for each Patch Manager server role in the Patch Manager environment. Each child node displays a list of servers in the selected role.

Security and User Management

This node consists of a tabbed view to view and manage security and user settings.

The Data Grid Pane

The data grid pane is the center pane of the Patch Manager console. When you select an item in the navigation pane, the data grid pane displays relevant information about that item, including container contents, item details, and general options.

When you select a specific data grid, you can customize its presentation in the following ways:
The Patch Manager console saves these customizations in the current user's profile, and they persist each time that user opens the console.

To save a data grid layout:

1. In the navigation pane, select the view you want to customize.
2. In the center pane, customize the view as applicable.
3. In the Actions pane (right), click Save View Layout.

**Selecting Columns**

You can choose which columns to show or hide in the Patch Manager console by right-clicking on any of the column headers. Show or hide columns on a one-time basis, or save your layout to make your preferences persist.

To specify which columns to show or hide:

1. In the navigation pane, select the view you want to customize.
2. In the center pane, right-click any column header.
3. In the Column Chooser window, select the columns you want to show in the Patch Manager console.
4. Clear the columns you want to hide in the Patch Manager console.
5. Click [x] to close the Column Chooser window.
6. **If you want to save the current layout**, click Save View Layout in the Actions pane.

**Reorganizing Columns**

You can change the order in which Patch Manager displays a view's columns by dragging columns to new positions. Change columns' positions on a one-time basis, or save your layout to make your preferences persist.

To specify the order of a view's columns:

1. In the navigation pane, select the view you want to customize.
2. In the center pane, drag the column you want to move to a new position. The Patch Manager
console displays arrows above and below the header bar to indicate where the column will go.

3. **If you want to save the current layout**, click Save View Layout in the Actions pane.

### Sorting Column Data

You can sort entries in a data grid by clicking one or more of its column headers. Change the sort order of entries in a data grid on a one-time basis, or save your layout to make your preferences persist.

To change the sort order of entries in a data grid:

1. In the navigation pane, select the view you want to customize.
2. In the center pane, click a column header once to sort the data grid by values in that column in ascending (A-Z) order. Patch Manager displays an upward-pointing arrow in the column header.
3. Click the column header again to sort in descending (Z-A) order. Patch Manager displays a downward-pointing triangle in the column header.
4. **If you want to sort a data grid by values in more than one column**, hold Shift while you click consecutive sorting columns.
5. **If you want to save the current layout**, click Save View Layout in the Actions pane.

### Filtering Column Data

You can filter entries in a data grid by the value(s) in one or more of its column headers. Filter the entries in a data grid on a one-time basis, or save your layout to make your preferences persist.

**Filtering by Specific Values**

Complete the following procedure to filter the data grid for rows that contain specific values in a column.

To filter a view by a specific column entry in the data grid:

1. In the navigation pane, select the view you want to customize.
2. In the center pane, click ![filter](filter.png) in a column header to expose its filter menu.
3. Select the values for which you want to see entries in the data grid.
4. Clear the values for which you do not want to see entries in the data grid.
5. Click OK. The filtered column header displays a filled-in filter button: ![filter](filled-filter.png).
6. **If you want to clear a column's filter**, click ![filter](filter.png), and then select Clear Filter in the filter menu.
7. **If you want to save the current layout**, click Save View Layout in the Actions pane.

### Creating Custom Filters

Complete the following procedure to create custom filters for the data grid view.

To create a custom filter for a data grid view:
1. In the navigation pane, select the view you want to customize.
2. In the center pane, click ☐ in a column header to expose its filter menu.
3. In the filter menu, point to Text Filters, and then select one of the available operators.
4. In the Custom Filter window, enter your custom filter as a search string using the fields and menus provided.
5. Click OK. The filtered column header displays a filled-in filter button: ☐
6. **If you want to clear a columns filter**, click ☐, and then select Clear Filter in the filter menu.
7. **If you want to save the current layout**, click Save View Layout in the Actions pane.

### Grouping Column Data

You can group entries in a data grid by one or more columns by dragging the column(s) to the grouping bar. The grouping bar is the dark grey bar directly above the column headers. After you have grouped them, you can expand or collapse entries in each group to view only the data you want to see. Group the entries in a data grid on a one-time basis, or save your layout to make your preferences persist.

To group entries in a data grid view by one or more columns:

1. In the navigation pane, select the view you want to customize.
2. In the center pane, drag the column header by which you want to group into the grouping bar.
3. **If you want to group the entries by more than one column**, drag the additional column header(s) into the grouping bar. The Patch Manager console displays arrows above and below the existing column header(s) in the grouping bar to indicate where the new header will go.

   The header at the far left of the grouping bar serves as the parent node for the grouped data, and subsequent headers serve as child nodes to the header directly to their left.

4. **If you want to remove a header from the grouping bar**, drag the header out of the grouping bar, away from the data grid. This restores the column header to its previous position in the data grid.
5. **If you want to save the current layout**, click Save View Layout in the Actions pane.

### The Task Options Wizard

Patch Manager provides the Task Options Wizard for many of the tasks available in the Patch Manager console. The Task Options Wizard consists of three primary pages:

- [The Computer Selection Page](#)
- [The Scheduling and Notification Options Page](#)
- [The Summary Page](#)
Depending on your preferences, these pages can open secondary pages for more advanced settings. The following sections describe these pages and their options in detail.

**The Computer Selection Page**

The first page of the Task Options Wizard allows you to select the computers you want to include in the task. This page can appear populated or blank, depending on your method for launching the task.

**Add Computers**

To add a computer, click Add computers. This displays the Add Computer dialog, which allows you to add a computer and its related information including:

- **Computer Name (NetBIOS):** Enter the computer name and then click Resolve to auto-fill other parts of the form. Provided DNS is set up correctly, the Resolve command populates the remaining fields.
- **Domain/Workgroup:** Enter the domain or workgroup for the selected computer.
- **Hostname or FDQN:** Enter the hostname or Fully Qualified Domain Name (FDQN) for the selected computer.
- **Canonical Name:** Optional. For Active Directory computers only.
- **IP Address:** Enter the IP address of the selected computer.
- **Operating System Version:** Select from a predefined list of operating system version numbers.

**Browse Computers**

To search for computers to add, click Browse computers. This displays the Select Computer dialog, which allows you to select computers from WSUS Server Groups, Active Directory Domains and Organizational Units, Workgroups, and Patch Manager Computer Groups.

To add computers using the Select Computer dialog:

1. In the left pane, use the network browser to select the container that contains the computer(s) you want to add.
2. If applicable, select the individual computer(s) you want to add. Hold CTRL while clicking to select multiple computers.
3. Add one or more computer(s) to the bottom-right pane:
   - Click Add selected to add the selected computer(s).
   - Click Select all and add to add all of the computers.
   - Click Enter the object to add in the bottom-right pane to launch the Add Computer dialog and manually enter objects to add.
4. To add the computer(s) in the bottom-right pane to your task, click OK.
Select Computers Using Rules

To add computers dynamically every time the task runs, click Select computers using rules. This displays the Computer Selection Rule Management dialog, which allows you to select or define a computer selection rule to apply when the task runs. Computer selection rules are based primarily on any of the following container types:

- Active Directory Domain or Workgroup
- Active Directory Organizational Unit
- WSUS Computer Group
- Patch Manager Computer Group

After you select a container, specify the types of computers you want to add using the following filtering options:

Include Workstations

Include Servers

Include Domain Controllers (Active Directory only)

Only include computers that have a reported time

This option allows you to specify a relative "reported time" to use as a filter. The definition for "reported time" depends on the container you selected. For example, if the computers are retrieved from a WSUS Group, then "reported time" references the last reported time in WSUS. On the other hand, if the computers are retrieved from an Active Directory Domain or Organizational Unit, "reported time" references the computers' domain account password age.

Include Operating System Version

This option allows you to specify a relative operating system version to use as a filter. For example, select < 6.0.6000.0 to specify pre-Vista computers.

Include child container computers

This option allows you to specify whether to include computers that belong to a child container. For example, if a computer is contained indirectly by a parent OU called 'Development' and the computer itself is in a child OU called 'workstations' and this option is enabled, then the computer will be included.
Exclude disabled computers (Active Directory only)

Only include computers that are a member of Active Directory Group

This option allows you to specify an Active Directory Security group for your rule. This option does not allow you to specify a Distribution group. Click [...] to browse to the group you want to specify.

To save a rule:

1. Enter a descriptive name into the Select an existing computer selection rule field
2. Click Save Rule.

To delete a rule:

1. Select an existing rule from the Select an existing computer selection rule field
2. Click Delete Rule.

Other Options

The Task Options Wizard also includes the following options on the "computer selection" page:

Remove

Remove the selected computer(s).

Remove All

Remove all computers from the "computer selection" page.

Change Domain/Workgroup

This option allows you to change the Domain/Workgroup value for the computer(s) highlighted on the "computer selection" page.

Change canonical path

This option allows you to change the Canonical Path value for the computer(s) highlighted on the "computer selection" page.

New Patch Manager Computer Group

This option opens the Patch Manager Computer Group Management window, which allows you to define a new Patch Manager Computer Group that contains the selected computer(s).

After you complete the Computer Selection page, click Next to proceed to the Scheduling and Notification Options page.
The Scheduling and Notification Options Page

After you complete the Computer Selection page of the Task Options Wizard, you see the Scheduling and Notification Options page. Use this portion of the wizard to define:

- When and how often the task will run,
- Whether or not SolarWinds Patch Manager should export the task results, and
- Whether or not SolarWinds Patch Manager should send an email upon completing the task.

The following sections describe these three options in detail.

Schedule Settings

You can schedule almost all the tasks in SolarWinds Patch Manager to run immediately or at a later time.

To create a task that runs immediately:

Select Run Task now in the Schedule Settings section.

To schedule a task for a later time:

1. In the Schedule Settings section, select Schedule the task to run daily, weekly or monthly, and then click Edit.
2. On the Schedule window, complete the following sections:
   - Schedule Time: Enter or select a start time and date for the scheduled task.
     Note: The time you select here corresponds to the local time on the Patch Manager Application Role Server where the task was created.
     For example, a task scheduled for 3pm central time will occur at:
       - 1pm for target computers in the pacific time zone
       - 2pm for target computers in the mountain time zone
       - 4pm for target computers in the eastern time zone

     If you select the Universal Time check box, the wizard converts the scheduled time to GMT, but target computers in varying time zones are affected in the same way.
   - Recurrence pattern: Select whether you want the task to run hourly, daily, weekly, or monthly. Set additional parameters as appropriate.
   - Range of recurrence: Select the end date (if any) for the task. Set additional parameters as appropriate.
3. Click OK.
Exports Options

Use this section to instruct SolarWinds Patch Manager whether or not to export the task results upon completion. If you want, you can export these results in a variety of formats, including XLS and CSV.

To run tasks without exporting their results:

Select Do not export in the Export Options section.

To configure a task that exports its results:

1. In the Export Options section, select Export results of the task to one of several formats, and then click Edit.
2. On the Export Options window, complete the following sections:
   - Export File Format: Select the format in which you want the results exported.
   - File Options: Specify a file name for the export. If you want to dynamically add the date and time to the file name, select Append date and time to file name.
   - Export Record Filter: Select whether you want to export all records or only those for either successful or failed operations.
3. Click OK.

Email Notification

Use this section to instruct SolarWinds Patch Manager whether or not to send an email upon completion. This email can include the exported results file, but it does not have to.

To configure tasks without email notifications:

- Select Do not send an email notification on task completion in the Email Options section.

To configure a task that notifies you with an email upon completion:

1. In the Email Options section, select Send an email notification on completion to, and then click Edit.
2. On the Email Notification Options window, select or complete the following fields as appropriate:
   - Include task results as attachment: Select this option if you want the exported results with the email notification. If selected, provide a file name for the export or accept the default.

Note: Attachments are automatically zipped and cannot exceed 10 MB in size.

- Only send notification email if export contains records: Select this option if you want to suppress notification for tasks that do not yield results. This option is only available if you opt to
attach exported results.

- Recipients (required): Enter one or more email addresses as recipients. Separate multiple entries with commas.

3. Click OK.

After you complete the Scheduling and Notification Options page, click Next to proceed to the Summary page.

The Summary Page

After you complete the first two pages of the Task Options Wizard, Patch Manager displays a summary page with an overview of the task you just configured. Review the settings on this page and do one of the following as appropriate:

- Click Back to change options on one or both of the previous pages, or
- Click Finish to save and/or run the task according to the task settings.

Patch Manager Computer Groups

Use Patch Manager computer groups to manage similar computers that are not otherwise part of a dedicated group in your Windows network. You create Patch Manager computer groups using rules so Patch Manager can evaluate group membership at runtime. Then you can target the dynamic group in tasks and reports as needed.

For example, create a Patch Manager computer group to contain all managed clients running Windows 7 RTM. Then target these computers in an Update Management task to upgrade them to Windows 7 Service Pack 1. After the computers are upgraded to Windows 7 SP1, they no longer show as members of the "Windows 7 RTM" computer group, so they are exempt from any future Update Management tasks targeted to that group.

To create a Patch Manager computer group:

1. In the left pane of the Patch Manager console, expand Enterprise, and then select Microsoft Windows Network.
2. In the Actions pane (right), click Add Patch Manager Computer Group.
3. In the Patch Manager Computer Group Management window, enter a new name for the computer group in the Computer Group Name field.
4. In the Description field, enter an optional description for the new group.
5. Select the computers to add to the group. For additional information, see "The Computer Selection Page" on page 63.
Note: To create a dynamic computer group, select Add computers using rules, and then create the requisite rule(s) for the types of computers you want in the group. For additional information, see "Select Computers Using Rules" on page 64.

6. Click Save.

Note: Patch Manager computer groups appear in the Microsoft Windows Network node in the navigation pane.

Managing Published Third-party Updates

The sections in this chapter provide general instructions for publishing and managing third-party updates from the Patch Manager console. For detailed examples of how to publish specific updates, see "Publishing Trial Updates" on page 51.

This chapter addresses the following procedures:

- Managing Publishing Servers
- Importing and Exporting Catalogs
- Creating and Publishing Software Packages
- Managing Third-party Packages
- Auto-Publishing Third Party Updates to WSUS

Note: For ConfigMgr instructions see Appendix A: "System Center Configuration Manager 2012 and 2012 R2 Procedures" on page 164.

Managing Publishing Servers

Use the Server Publishing Verification Wizard to determine whether a WSUS server has a publishing certificate. If it does, the wizard also determines the status of the publishing certificate with respect to the other server resources associated with that WSUS server.

To complete the Server Publishing Verification Wizard:

1. In the left pane of the Patch Manager console, expand Administration and Reporting, and then select Software Publishing.
2. In the Actions pane (right), click Server Publishing Verification Wizard.
3. In the PublishingWSUS Server menu, select a WSUS server.
4. If the WSUS server does not have a publishing certificate, the wizard returns a dialog to indicate that. Click OK to proceed.
5. **If the WSUS server has a publishing certificate**, the wizard returns a list of related server resources, indicating the status of the WSUS server's publishing certificate on each. Select a server resource to view its details in the bottom pane.

6. Click Close to exit the wizard.

If a server requires any action based on the results you see in this wizard, complete the Server Publishing Setup Wizard to create and/or deploy publishing certificates as necessary. For additional information, see "Configuring Publishing Servers" on page 39.

**Importing and Exporting Catalogs**

Import and export package catalogs to move catalogs amongst Patch Manager servers. This section addresses the following procedures:

- Importing Catalogs
- Exporting Catalogs

**Importing Catalogs**

Use the Import Catalog Wizard to import selected packages or an entire catalog from a portable catalog (.cab) file created by another Patch Manager server, System Center Updates Publisher, or any other product that complies with the Microsoft package and catalog specifications.

To import packages from a portable catalog file:

1. In the left pane of the Patch Manager console, expand Administration and Reporting, and then select Software Publishing.
2. In the Actions pane (right), click Import Catalog.
3. On the Select Catalog File screen, browse to or enter the complete path for the catalog (.cab) file you want to import.
4. Click Next.
5. On the Import Details screen, select the package(s) you want to import.
6. Click Next.
7. Review the import results, and then click Finish.

**Exporting Catalogs**

Use the Export Catalog Wizard to export one or more packages into a portable catalog (.cab) file that can be imported into another Patch Manager server, System Center Updates Publisher, or any other product that complies with the Microsoft package and catalog specifications.

Use the Export Catalog Wizard to do either of the following:
• Export the entire library of packages into a catalog file.
• Export one or more selected packages into a catalog file.

The following define the export options in this wizard.

**Include downloaded package content when exporting**

Select this check box if you want to export all installers and other files you have downloaded for the packages you are exporting. If you select this option, use the Additional Files dialog to select files on a per-file basis.

**Export the selected software packages to a cabinet file that can be imported by other publishers**

Select this option if you selected one or more packages to export prior to launching the wizard.

**Export all software packages to a cabinet file that can be imported by other publishers**

Select this option if you want to export all packages in your library.

**Export File Name**

Enter or browse to the file you want to use for the export. This field requires a fully qualified file path.

To export packages to a portable catalog file:

1. In the left pane of the Patch Manager console, expand Administration and Reporting > Software Publishing.
2. Select any container in the Software Publishing node.
3. Select one or more packages in the center pane. The wizard lets you export specific packages based on your selection, or all packages regardless of your selection. Use Ctrl+click to select multiple packages.
4. In the Actions pane (MMC) or ribbon (ConfigMgr), click Export Catalog.
5. Complete the Export Options screen as described previously.
6. Click Next.
7. Review the export results, and then click Finish.

**Creating and Publishing Software Packages**

Use Patch Manager to create custom software packages to publish to WSUS. Publish custom packages or packages from the SolarWinds third-party updates library so WSUS can deploy them to the applicable clients. This section addresses the following procedures:

• [Creating Software Packages](#)
• [Managing Software Package Rulesets](#)
Publishing Custom Software Packages

Creating Software Packages

The Package Wizard is a guided interface for creating or editing a package definition. A package definition is an XML file that defines the attributes and behavior of an update package. Use the Package Wizard to view or define the following:

- Package metadata
- Prerequisite rules
- Update source
- Applicability rules
- Installed rules

Note: SolarWinds fully supports packages created and provided by the company; however, we do not provide customer support for custom packages created by outside sources. For help with custom packages browse or engage in the SolarWinds community at thwack.solarwinds.com.

To open the Package Wizard:

1. In the left pane of the Patch Manager console, expand Administration and Reporting > Software Publishing.
   
   If you want to create a new package:
   a. Select any container in the Software Publishing node.
   b. In the Actions pane, click New Package.

   If you want to view a package’s details:
   a. Select the container that contains the package you want to view.
   b. In the center pane, select the package you want to view.
   c. In the Actions pane, click Edit.

4. Complete the Patch Manager Package Wizard as described in "Completing the Package Wizard" on page 72.

Completing the Package Wizard

The following procedure describes each step of the Package Wizard. For detailed information about adding prerequisite, applicability, and installed rules in the wizard, see "Managing Software Package Rulesets" on page 77.

To complete the Package Wizard:
1. On the Enter or modify the package information page, enter the package's metadata. For additional information, see "Defining Package Metadata" on page 73.

2. On the Prerequisite Rules screen, add or modify rules to define whether a target computer should evaluate the update further based on its hardware or software attributes. For additional information, see "Prerequisite Ruleset" on page 77.

3. Click Next.

4. On the Select Package page, specify the source of the package contents. For additional information, see "Defining the Package Source" on page 75.

5. Click Next.

6. On the Applicability Rules page, add or modify rules to define whether the update applies to the target computers. For additional information, see "Applicability Ruleset" on page 78.

7. Click Next.

8. On the Installed Rules page, add or modify rules to define how to determine whether a target computer already has the update installed. For additional information, see "Installed Ruleset" on page 78.

9. Click Next. To add a rule to check whether Firefox 10.0 is installed:

10. On the Summary page, verify your settings for the package, and then click Next to save the new or modified package.

**Defining Package Metadata**

The following define the fields on the Enter or modify the package information page of the Package Wizard.

**Package Title (required)**

The text string displayed in the update listing of the administrative console and the header of the update details. Enter a string that is concise, descriptive, and 80 characters or less.

**Description (required)**

A longer length text field used to provide additional information on the update, particularly its purpose.

**Classification (required)**

A pre-defined value that describes the type of update. The options in this menu are defined by Microsoft.
Bulletin ID
The ID assigned to a Microsoft Security Response Center Security Bulletin. This field can also hold a similar value for security updates published by other vendors. For non-security updates this value would normally be left empty.

Vendor (required)
The software company responsible for the product to which the update applies. This field allows you to sort and filter updates in the administrative console. Enter a company, or select one from the menu. For optimal performance, keep this list as short as possible.

Product (required)
The vendor’s marketing name for the entity to which the update applies. This field allows you to sort and filter updates in the administrative console. Enter a product name, or select one from the menu. For optimal performance, keep this list as short as possible.

Article ID
The ID assigned to a Microsoft Knowledge Base article. This field can also hold a similar value for updates published by other vendors.

CVE ID
The ID assigned to the National Cyber Security Division’s (NCSD) Common Vulnerability and Exposures (CVE) article that describes the issue the update is intended to resolve.

Severity
The rating assigned to a security update by the Microsoft Security Response Center. This field is required for any update classified as a Security Update.

Support URL
The URL for support information for the update, such as its applicability, deployment considerations, or the publicly available download location. Enter the URL for the vendor’s authoritative source for information about the update.

More Info URL
The URL for additional information about the update, possibly not available at the time of the original update publication.

Impact (required)
A designation that dictates how target computers will handle the update. Select one of the following options:
Normal

Any update that does not fit in either of the following categories.

Minor

An update that does not require a system or service restart to be applied. Minor updates use the Windows Update Agent setting “Allow automatic updates immediate installation” to determine if the update can be installed immediately, or must wait until a directed or scheduled event.

Requires exclusive handling

An update that must be installed individually, outside of a batch of other updates. Typically this includes updates such as operating system service packs, .NET Framework service packs and redistributables, and updates to the Component-Based Servicing Stack.

Reboot Behavior (required)

How the target computer should behave after the update is installed. Select Can request reboot if a reboot may be required, but is not absolutely necessary in all installation scenarios. Otherwise, select Never reboots or Always requires reboot according to the vendor’s specifications.

Defining the Package Source

The following define the fields on the Select Package page of the Package Wizard.

Type

The package's file extension. Select whether the package is EXE, MSI, or MSP based.

I do not have the package content

Specifies the URL for a web-based or FTP-based download location. Enter the direct URL for the installer in the Download URL field. This field does not accept forwarding links.

I already have the content for the package locally on my network

Specifies the name and location of content you have already downloaded. Enter the package’s filename in the Package field, and its web-based, FTP-based, or UNC file path in the Download URL field.

Use the Package Boot Helper program when performing installation of the software

Activates the Package Boot Editor button so you can define additional files and behavior to accompany the installer. For additional information, see "Using PackageBoot" on page 76.

Include additional files with the package

Activates the Package Content Editor button so you can specify additional files to accompany the installer.
**Binary Language**

The language required by the update. If the update is not language-specific, select None.

**Success Return Codes**

The return code(s) for the package. Separate multiple codes with commas.

**Success Pending Reboot Codes**

The reboot code(s) for the package. Separate multiple codes with commas.

**Command Line (silent install)**

Additional arguments to support the unattended installation.

**Using PackageBoot**

PackageBoot is a utility designed to assist in the successful installation of certain updates by orchestrating specific actions before and after applying an update. Use PackageBoot to verify that any files that will be overwritten during the installation process are not currently locked. For example, locked files can sometimes cause issues with silent installations and require reboots. Furthermore, use PackageBoot to stop and start services before and after installation, execute programs (MSI or EXE) before or after installation, and terminate processes before installation.

The Package Boot Editor creates two files to include in the update package: PackageBoot.EXE and PackageBoot.XML. Both files are published with the installer to the WSUS server and then downloaded to the target computer. The PackageBoot.XML file provides the specifications for the activities and tasks that the Windows Update Agent will perform.

To complete the Package Boot Editor:

1. Open the Package Boot Editor from the Select Package screen of the Package Wizard.
2. In the Before applying package section, select the actions you want to run prior to installing the update. Common examples include stopping a service, running a program, or terminating a process.
3. In the After applying package section, select the actions you want to run after installing the update. Common examples include running a program or starting a service.
4. After you select a task in these sections, specify the action details in the right pane.
5. Click Save to save the PackageBoot.XML configuration file.
6. Close the Package Boot Editor.

The following define additional options on the Package Boot Editor screen:

**Import**

Import a PackageBoot.XML file from a local or network location.
View XML

View the PackageBoot.XML configuration file the editor will generate.

Add Action

Select an action to add to the active section of the editor.

Delete

Delete the selected action.

Duplicate

Duplicate the selected action.

Move Up

Move the selected action one position higher in regard to its processing order.

Move Down

Move the selected action one position lower in regard to its processing order.

Managing Software Package Rulesets

WSUS uses software publishing rules to evaluate if a package is appropriate to be deployed to a specific client and if the package is applicable or already installed. The following sections describe each type of software publishing ruleset and provide a corresponding example.

For additional information about these rulesets, see the following articles:

- The Five Rules You Need to Know to Build a Custom Update Package
- How the Windows Update Agent Determines the Status of an Update
- How to Troubleshoot Update Misbehavior Caused by Defective Rules

Note: The Rule Editor is the same regardless of the type of rule. Furthermore, it is the same whether you launch it from the Package Wizard or the New Rule task in the Administration and Reporting > Software Publishing > Rules view in the Patch Manager console.

Prerequisite Ruleset

Common prerequisite rules define the prerequisite Windows version, language, and processor architecture for the target computers. For example:

To add a rule to include only workstations running Windows XP SP 3 or later:

1. On the Rule Editor window, select Create Basic Rule.
2. In the Rule Type field, select Windows Version.
3. In the Comparison field, select Greater Than or Equal To.
4. In the Major Version field, enter or select 5.
5. In the Minor Version field, enter or select 1.
6. In the SP Major Version field, enter or select 3.
7. In the Product Type field, select Workstation.

The following are the current Windows operating system version numbers in majorVersion.minorVersion.SPMajorVersion format:

- 5.1.3: Windows XP Service Pack 3
- 5.2.2: Windows Server 2003 Service Pack 2
- 6.0.2: Windows Vista Service Pack 2 and Windows Server 2008 Service Pack 2
- 6.1.1: Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1

**Applicability Ruleset**

Common applicability rules check to see whether certain registry keys or values exist on the target computer. Generally, applicability ruleset works hand-in-hand with the installed ruleset to define whether or not a target computer requires the update. For example:

To add a rule to check whether the Firefox version is less than 10.0:

1. On the Rule Editor window, select Create Basic Rule.
2. In the Rule Type field, select File Version with Registry Value.
3. In the Registry Key field, enter HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\firefox.exe.
4. In the Registry Value field, enter Path, and then select Use 32-bit registry.
5. In the Sub-path field, enter firefox.exe.
6. In the Comparison field, select Less Than.
7. In the Version field, enter 10.0.0.441.

**Installed Ruleset**

Common installed rules check to see whether certain registry keys or values exist on the target computer. Generally, installed ruleset works hand-in-hand with the applicability ruleset to define whether or not a target computer requires the update. For example:

To add a rule to check whether the Firefox version is less than 10.0:
1. On the Rule Editor window, select Create Basic Rule.
2. In the Rule Type field, select File Version with Registry Value.
3. In the Registry Key field, enter HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\firefox.exe.
4. In the Registry Value field, enter Path, and then select Use 32-bit registry.
5. In the Sub-path field, enter firefox.exe.
6. In the Comparison field, select Equal To.
7. In the Version field, enter 10.0.0.441.

Note: The only difference between the applicability and installed rules in these examples is that the applicability rule is checking for installed versions prior to the update installer's version, and the installed rule is checking for the existence of the same version. Thus, the two rulesets combined determine whether or not the update is needed.

**Publishing Custom Software Packages**

Use the Patch Manager Publishing Wizard to publish one or more packages to a WSUS server. When publishing packages, you have the option to publish any of the following:

- Entire packages, which include all metadata and installers.
- Metadata-only packages, which you can use to determine whether or not a package is installed or needed on target computers.
- Revision-only packages, which update an existing package's metadata, but not its installation file.

**Completing the Patch Manager Publishing Wizard**

Complete the following procedure to publish packages to a WSUS server to be deployed to applicable clients.

The wizard in this procedure provides the following additional options:

**Verify WSUS version compatibility and required signing certificate is distributed**

Checks the versions and certificates throughout the publishing environment to verify publishing will be successful. WSUS requires that all components in the publishing environment are running the same WSUS version and have the same publishing certificate installed. We recommend you use this option to verify these requirements prior to large publishing jobs to avoid wasted publishing time.

**Re-sign existing selected packages**

Re-signs the selected packages with the current publishing certificate. Use this option when republishing packages that were previously signed with an earlier publishing certificate.
Delete package if it exists (select this if binaries have changed)

Replaces the existing binary files for the selected packages with new ones. Most often, you will accomplish this goal by publishing an entirely new package, but this option allows you to reuse an existing package definition.

Re-download packages that have already been downloaded

Downloads the binary content for all packages, even if the content is already on the SolarWinds Patch Manager server. Use this option to ensure the content you publish to the WSUS server is exactly the same as the content available from the vendor's update publishing site.

To publish packages to a WSUS server:

1. Expand Administration and Reporting > Software Publishing, and then select the container that contains the package(s) you want to publish.
2. In the Actions pane, click Publish Packages.
3. On the Packages to Publish screen, select the WSUS server to which you want to publish the packages.

Note: This wizard cannot publish packages to replica servers.

4. Select one of the following options as your initial selection method:
   - Publish selected packages to the WSUS server: Select this option to start with only the packages you selected before launching the wizard.
   - Publish all packages to the WSUS server: Select this option to start with all available packages selected. You can clear or modify these selections in the following step.

5. In the pane that lists the available packages, select the check box next to the packages you want to publish. Clear the check box next to the packages you do not want to publish.
6. In the Content column for each package you selected, specify whether you want to publish the Full, Metadata Only, or Revision Only version.
7. Above the package selection pane, select any of the additional options described previously.
8. Click Next.

If you need to download any additional content:

a. If any packages do not include direct download links, use Package Download Assistant to download and import the content. For additional information, see "Using Package Download Assistant" on page 81.

b. After the wizard finishes downloading the required content, select each of the packages you
want to publish.

c. Click Next.

10. Review the publishing results, and then click Finish.

**Using Package Download Assistant**

Complete the Package Download Assistant wizard to publish packages for which vendors do not include direct download links. Common examples of such packages include the Adobe Flash Player and Sun Java Runtime Environment packages.

To complete the Package Download Assistant wizard:

1. Prepare to publish the package(s) just like any other. For additional information, see "Completing the Patch Manager Publishing Wizard" on page 79.
2. On the Package Download Assistant window, select a package, and then double-click the link provided below the package list.
3. On the vendor's download page, download the file or archive for the package you selected.
4. Back on the Package Download Assistant window, complete any additional steps listed in the Package download description and instructions section. For example, extract the contents of the vendor's archive.
5. Click Import Source.
6. Browse to the folder that contains the downloaded file, and then click Open.

Note: The wizard pre-populates the Select the downloaded package file dialog with the necessary filename, so you do not need to select or specify a file during this step, just the folder.

7. Repeat Steps 2-6 for any other packages listed in the wizard.
8. Click OK.
9. Complete the publishing wizard as you would for any other package.

**Managing Third-party Packages**

After you have created a package in Patch Manager, select it in the Patch Manager console to view useful information about it in the details pane. The topics in this section address the following procedures.

- [Viewing Package Details](#)
- [Verifying Package Integrity](#)
- [Checking a Package's Publication Status](#)
Viewing Package Details
When you select a package in the Packages node of the Patch Manager console, Patch Manager displays detailed information about the package in the following tabs.

Package Details
Similar to the Update Details tab for WSUS updates. Displays the package description and metadata.

Prerequisite Rules
Displays the prerequisite rules for the package just as they appear in the Package Wizard.

Applicability Rules
Displays the applicability rules for the package just as they appear in the Package Wizard.

Installed Rules
Displays the installed rules for the package just as they appear in the Package Wizard.

Verifying Package Integrity
Use the Package Integrity Verification task to verify the content of a package before you publish it. This package compares the contents you have previously downloaded for the package to what is currently available from the vendor.

This task does the following:

- It calculates the SHA-1 hash of the downloaded file and compares it to the SHA-1 hash that was calculated when the package was created.
- It identifies the quantity of any extra files that should be included as defined by the Include Additional Files option, and the quantity of any files that are missing based on the number of files that are defined.
- It provides a Repair option to remediate any repairable conditions.

To check the integrity of one or more downloaded packages:

1. Select one or more packages that have already been downloaded.
2. In the Actions pane, click Package Integrity Verification.
3. If the wizard displays a package without a green check mark in the left column, click Repair to repair the package.
4. Click Close to exit the window.
Checking a Package's Publication Status

Use the Check Publication Status task to determine whether or not a package has been published to a WSUS server.

To check the publication status of one or more packages:

1. Select the packages you wish to check.
2. In the Actions pane, click Check Publication Status.
3. On the Package Publication Status Wizard, select the update servers you want to check against.
4. Click Next.
5. Review the results of the check, and then click Close to exit the wizard.

Auto-Publishing Third Party Updates to WSUS

Auto-publishing of third party updates allows you to automatically download and publish updates to the WSUS servers.

To auto-publish third party updates:

1. In the left pane of the SolarWinds Patch Manager console, expand Administration and Reporting.
2. Select Software Publishing.
3. In the Actions pane, click Auto-Publishing of 3rd Party Updates to WSUS.
4. Select the WSUS servers that you want to publish the third party updates.
5. Select the products as necessary.
6. Click Next. The Scheduling and Notification window appears.

Note: For safety reasons, license conditions, and efficiency, auto-publishing skips the following types of updates:

- Updates without direct link to executable file
- Updates marked as "metadata only"
- Updates marked as "expired"
- Updates created manually by user
- Driver-based packages
7. In **Auto-Publishing Schedule**, select whether to disable or enable auto-publishing. When you enable auto-publishing, you can select whether to auto-publish after each synchronization with Patch Manager content server or schedule a task to run daily, weekly or monthly. To schedule a task:
   a. Select **Schedule a task to run daily, weekly, monthly**.
   b. Click **Configure**.
   c. In **Scheduled Time**, fill-in with start time and date.
   d. In **Recurrence Pattern**, select whether to run hourly, daily, weekly, or monthly.
   e. On **Range of recurrence**, select the occurrence of the update.
   f. Click **OK**.

8. In **Export Results**, select whether to export results or not. To export results:
   a. Select **Exports results of the task to one of the several formats...**
   b. Click **Configure**.
   c. In **Export File Format**, select the file format of the export file.
   d. In **File Options**, you have the option to change the filename and append date and time to the filename.
      **Note:** The file will be exported to the predefined export directory located in the application server's installation directory.
   e. In **Export Records Filter**, select whether to export all records, only successful operations, or only failed operations.
      **Note:** This option is only valid for configuration management tasks.

9. In **Email Notification**, select whether to send an email notification on task progress or not. To send email notification:
   a. Select **Send an email notification to...**
   b. Click **Configure**.
   c. In the Email Notifications Options window:
      i. Select whether to send an email alert that 3PUP content requiring manual intervention is available.
      ii. Select whether to send a general email at the end of auto-publishing.
      iii. Select whether to export tasks results as an attachment (for configuration management and report tasks only). You can choose to send an email only when results contain records.
         **Note:** To add an attachment in your email, select the Export Results option.
      iv. Change the email subject as necessary.
      v. Add email recipients. Separate each recipient with a semicolon.
      vi. Click **OK**.

10. Click **Next**. The Task Summary window appears.

11. Review the information in the Task Summary window.
12. Click **Finish**.

**Notes:**
- If you need to update your auto-publishing settings, run the wizard again.
- If you need to delete this configuration, go to Scheduled Tasks. For more information, see Managing Scheduled Tasks.
Inventory and Reporting

Patch Manager uses Inventory tasks to pull information from your WSUS servers and managed computers so you can view and report on that information from the Patch Manager console. Schedule Inventory tasks to run regularly in order to keep your report data current.

ConfigMgr Note: The inventory and reporting tasks discussed in this chapter are available regardless of the Microsoft product you are extending. Although you cannot perform these functions from within the ConfigMgr console, all of the Patch Manager functionality is available in the stand-alone MMC-based console.

Note: If you are configuring the Inventory for the first time and the Patch Manager has not previously connected to the clients, Patch Manager installs the SolarWinds Client Components on to the clients to manage the connection between Patch Manager and the client.

This section addresses the following inventory and reporting concepts:

- Inventory Tasks
- Patch Manager Report Viewer and Report Builder
- Report Data Sources

For information about how to use the reporting interfaces in the Patch Manager console, see "Patch Manager Report Viewer and Report Builder" on page 87.

Inventory Tasks

There are two types of Inventory tasks in Patch Manager:

- WSUS Inventory
- Managed Computer Inventory

The WSUS Inventory task collects data from the WSUS server. This type of Inventory provides detailed information about WSUS server configuration, WSUS server statistics, basic computer inventory attributes, and so on. Data from the WSUS Inventory task only populates reports in two categories:

- WSUS Reports > Windows Server Update Services
- WSUS Reports > Windows Server Update Services Analytics

The Managed Computer Inventory task collects data from your managed computers. This type of task uses Windows Management Instrumentation (WMI), and you can customize it to collect the specific data you want to see. Data from the Managed Computer Inventory task populates reports in the Configuration Management Reports parent category, and the Windows Update category under WSUS Reports.
This section addresses the following procedures:

- Configuring the WSUS Inventory Task
- Configuring the Managed Computer Inventory Task
- Scheduling the Managed Computer Inventory Task
- Collecting File, Folder, or Registry Information

The following video illustrates the process to set up a WSUS Inventory and run the related reports:

"WSUS Inventory and Reporting," [http://www.youtube.com/watch?v=vH9PplbtloM](http://www.youtube.com/watch?v=vH9PplbtloM)

**Configuring the WSUS Inventory Task**

Configure the WSUS Inventory task to populate Patch Manager reports. The WSUS Inventory task pulls the Patch Manager report information from your WSUS servers using the WSUS API. SolarWinds recommends that you schedule the task to run daily, outside of normal operating hours. However, you also have the option to configure a one-time WSUS Inventory for evaluation or other purposes as-needed.

To schedule a WSUS Inventory task:

1. In the left pane of the Patch Manager console, expand Enterprise > Update Services, and then select your WSUS server.
2. In the Actions pane (right), click WSUS Inventory.
3. Specify options on the WSUS Inventory Options window, or accept the defaults.
4. Click Save.
5. Set the Scheduled Time, Recurrence pattern, and Range of recurrence on the Schedule window. Notice the Run Once option under Range of recurrence.
6. Click OK.

**If you want to run the task immediately:**

a. In the left pane of the Patch Manager console, expand Administration and Reporting, and then select Scheduled Tasks.

b. In the center pane, select the scheduled task.

c. In the Actions pane (right), click Run Task Now.

**Configuring the Managed Computer Inventory Task**

Complete the following procedure to configure the Managed Computer Inventory task.

To configure a Managed Computer Inventory task:
1. In the left pane of the Patch Manager console, expand Patch Manager System Configuration > Management Groups, and then select Managed Enterprise.

2. In the center pane, select the domain or workgroup you want to inventory.

3. In the Actions pane (right), click Inventory Configuration.

4. On the Datasource Configuration tab of the Inventory Configuration Editor, specify what data sources you want to include in the Inventory task:
   - Select the check boxes next to the data sources you want to include. If you select a parent category, it automatically selects all child categories.
   - Clear the check boxes next to the data sources you do not want to include. If you clear a parent category, it automatically clears all child categories.

5. **If you want to collect file and/or Registry information:**
   a. Select the Registry, File, and/or Directory data source(s) as applicable.
   b. Click the File, Directory and Registry Datasource Configuration tab.
   c. Specify the data you want to collect as described in "Collecting File, Folder, or Registry Information" on page 89.

6. **If you want to save this Inventory configuration for future use,** click Save Template at the top of the window, and then complete the Save Inventory Configuration Template dialog:
   a. In the Name field, enter a new name for the Inventory template.
   b. Click Save.
   c. Click OK on the confirmation dialog.

7. Click OK to save your changes and close the Inventory Configuration Editor.

### Scheduling the Managed Computer Inventory Task

Complete the following procedure to schedule the Managed Computer Inventory task.

To schedule a Managed Computer Inventory task:

1. In the left pane of the Patch Manager console, expand Patch Manager System Configuration > Management Groups, and then select Managed Enterprise.

2. In the center pane, select the domain or workgroup you want to inventory.

3. In the Actions pane (right), click Schedule Inventory.

Note: If you have never run the Inventory Configuration task, Schedule Inventory triggers that task first. For additional information, see "Configuring the Managed Computer Inventory Task" on page 87.
4. On the Schedule window, set the Scheduled Time, Recurrence pattern, and Range of recurrence, and then click OK.

5. On the Computer Selection Rule Management window, select an existing computer selection rule, or define a new one:
   
   a. **If you want to save the new computer selection rule for future use**, enter a name for the rule in the Select an existing computer selection rule menu.
   
   b. Under Computer Filter select or clear options as appropriate.
      
      Note: Select and configure the Only include computers that have a reported time option to avoid exceeding your Patch Manager license.
   
   c. Click OK.
   
   d. Specify whether you want to save the rule settings using the name you defined in Step a.
   
   e. **If you clicked Yes on the previous dialog**, click Yes again to confirm your selection, and then click OK on the success dialog.

### Collecting File, Folder, or Registry Information

The default inventory template does not collect file, folder, or Registry information. However, you can customize inventory templates to collect that information using the File, Directory and Registry Datasource Configuration tab in the Inventory Configuration Editor.

To complete the File, Directory and Registry Datasource Configuration tab:

1. In the left pane of the tab, browse to the container that contains the file system object or Registry object you want to inventory.

2. In the upper-right pane, select the object(s) you want to add. Hold Ctrl or Shift while clicking to select multiple objects.

3. Click Add at the top of the appropriate pane in the lower-right.
   
   **If you want to manually enter the path for a file system object:**
   
   a. Above the File System Object pane in the lower-right, click Manually Add/Modify.

   b. Specify whether you want to add a File or Directory.

   c. In the Fully Qualified Path field, enter the path for the file or folder.

   Note: This field does not support UNC paths, but it does support environment variables such as %PROGRAMFILES%.

   d. Click Save.

   e. Repeat these steps for all additional files or folders you want to add.

5. If you want to manually enter the path for a Registry object:
a. Above the Registry Object pane in the lower-right, click Manually Add/Modify.
b. Specify whether the Registry setting you want to add is in the HKEY_LOCAL_MACHINE or HKEY_USERS hive.
c. In the Registry Key Path field, enter the rest of the path.
d. **If you want to provide a display name**, enter a custom value in the Friendly Display Name (optional) field.
e. **If you want to specify a Registry value**, select Include Registry Value, and then specify the type and name for the value.
f. Click Save.
g. Repeat these steps for all additional Registry objects you want to add.

6. **If you want to remove an object**, select the object in the appropriate pane in the lower-right, and then click Remove.

**Patch Manager Report Viewer and Report Builder**

Use Patch Manager Report Viewer and Report Builder to view, customize, and create reports for your WSUS servers and managed clients. For evaluation purposes, this section addresses three scenarios:

- Using Patch Manager Report Viewer
- Customizing a Patch Manager Report
- Creating a Custom Report

**Using Patch Manager Report Viewer**

When you run a Patch Manager report, Report Viewer opens in a new window. Use Report Viewer to customize the layout of your reports, filter and sort report results, and export reports to file or email. This section addresses the following topics:

- Running WSUS Reports
- Customizing Report Layouts
- Filtering and Sorting Report Results
- Configuring Report Viewer Email Settings
- Exporting and Emailing Report Results

**Running WSUS Reports**

Complete the following procedure to run WSUS reports.

To run a WSUS report:
1. In the left pane of the Patch Manager console, expand Administration and Reporting > Reporting > WSUS Reports.

2. Select a report category. For example, select Windows Server Update Services Analytics.

3. In the center pane, select a report. For example, select Computer Update Status.

4. In the Actions pane (right), click Run Report.

**Customizing Report Layouts**

Complete the following procedure to customize a report's layout.

To customize the layout of a report:

1. To increase the number of lines Report Viewer displays per page, click Navigation Configuration, and then enter a value up to 100,000.

Notes:

- The default value is 2,000.
- Any change you make persists for all reports.

2. To reorganize the columns in the report, drag and drop any column to the position you want. For example, drag the Domain or Workgroup (Update Server) and Name (Update Server) columns to the far right of the data grid.

3. To resize the columns, reposition the column separators in the header row.

4. To group results by the values in a column, drag the column header into the group bar. For example, drag Computer Name into the group bar:

5. To show or hide available columns:
   a. Click Column Chooser.
   b. Select the columns you want to show.
   c. Clear the columns you want to hide.
   d. Close the Column Chooser window.

6. To save a custom layout, click Save Layout.
Filtering and Sorting Report Results

Complete the following procedure to filter and sort report results.

To filter and sort the report results:

1. To filter a report:
   a. Click ☐ in any column to expose the filter options for that column.
   b. Clear or select values as appropriate.
   c. Click OK.

2. To sort a report by the values in a specific column:
   • Click the column header once to sort in ascending (A-Z) order.
   –or–
   • Click the column header twice to sort in descending (Z-A) order.

Configuring Report Viewer Email Settings

Complete the following procedure to configure email settings for Report Viewer.

To configure email settings for Report Viewer:

1. In the Report Viewer window, click Email Configuration.
2. Enter the SMTP Server and Sender Email Address (required).
3. **If your email server uses a custom port,** modify the Port value as appropriate.
4. **If your email server uses a secure connection,** select Use SSL or Use TLS as appropriate.
5. **If you want to specify one or more favorite recipients,** enter the email address(es) in the Favorite Recipients field. Separate two or more addresses with semicolons.
6. **If your email server requires credentials to send email,** select Use Credentials, and then complete the related fields.
7. Click OK.

Exporting and Emailing Report Results

Complete the following procedure to export report data and email it.

To export and email a report:

1. In the Report Viewer window, click Email.
2. Add at least one address to the recipients list:
a. Enter an email address in the Recipient field.

b. Click Add.

Note: If you added one or more favorite recipients to the Email Configuration form, those recipients are already present in the recipients list.

3. Click OK.

4. In the Export Options window, select the format you want to use for your report.

5. In the Export Filename field, browse to or enter a custom path/filename, or accept the default.

6. Click Export.

**Customizing a Patch Manager Report**

Use the Report Definition Builder to customize existing Patch Manager reports to refine or expand the scope of their results. You can also customize certain layout options, such as the order in which the report displays its columns. Use the following example to customize the Computer Update Status report to show only updates that are needed, but not already installed.

To customize a WSUS report (example):

1. In the left pane of the Patch Manager console, expand Administration and Reporting > Reporting > WSUS Reports.

2. Select Windows Server Update Services Analytics.

3. In the center pane, select Computer Update Status.

4. To open Report Definition Builder, click Edit and Schedule Report in the Actions pane (right).

5. Using the [-] at the far right, drag Domain or Workgroup (Update Server) and Name (Update Server) to the bottom of the list.
6. Using the [-] at the far right, drag Computer Name to the top of the list.

7. Set the report to sort by the Computer Name column:
   a. Click Not Sorted next to the column name.
   b. Point to Sort position 1, and then select Ascending.

8. Add the Update ID field to the report:
   a. Click [+] to the left of the last column.
   b. Click Select Field for the new column entry.
   c. Point to Computer Update Status, and then select Update ID.

9. Add a filter to the report for updates to install upon approval:
   a. Click [+] under Select the filter criteria for the report.
   b. Click Select Field for the new filter entry.
   c. Point to Computer Update Status, and then select Update Approval Action (Friendly Name).
   d. Next to the new field name, click Select Operator, and then select equals.
   e. Next to the new operator, click <Enter Value>, and then select Enter Value.
   f. In the text box, enter Install.

10. Add a filter to the report for updates with states that are not Installed or Unknown:
    a. Click [+] next to the existing filter.
    b. Click Select Field for the new filter entry.
    c. Point to Computer Update Status, and then select Update Installation State (Friendly Name).
    d. Next to the new field name, click Select Operator, and then select does not equal.
    e. Next to the new operator, click <Enter Value>, and then select Enter Value.
    f. In the text box, enter Installed.
    g. Click the arrow to the left of this filter, and then select Place in New Group.
    h. Click [+] within the new group.
    i. Click Select Field for the new filter entry.
    j. Point to Computer Update Status, and then select Update Installation State (Friendly Name).
    k. Next to the new field name, click Select Operator, and then select does not equal.
    l. Next to the new operator, click <Enter Value>, and then select Enter Value.
    m. In the text box, enter Unknown.
11. Click Next.
12. In the Report Name field, enter a unique name. For example, enter Computer Updates – Approved Not Installed.
13. Select Save and run report now.
14. Click Finish.
15. Examine your report and customize the layout if you want. For additional information, see "Using Patch Manager Report Viewer" on page 90.

Creating a Custom Report

Use the Report Definition Builder to create custom Patch Manager reports. Use the following example to create a WSUS report that shows all of the pending updates in your environment, along with their Update IDs and Update Revision Numbers. By including these values, you can install the updates directly from Report Viewer. This section addresses the following procedures:

- Creating a Custom WSUS Report
- Installing Updates from a WSUS Report

Creating a Custom WSUS Report

The following procedure presents an example of how to create a custom WSUS report. The report in this example is configured to allow you to install updates directly from Report Viewer.

To create a custom WSUS report (example):

1. In the left pane of the Patch Manager console, expand Administration and Reporting > Reporting > WSUS Reports.
2. Select Windows Server Update Services Analytics.
3. In the center pane, select Computer Update Status.
4. Under Available Datasources, select Computer Update Status With Update Information.
5. Under Available Fields, use Ctrl+click to select the following fields in this order:
   a. Computer Name
   b. Update Title
   c. Update Installation State (Friendly Name)
   d. Update ID
   e. Update Revision Number
   f. Name (Update Server)
6. In the Actions pane (right), click New Report.

7. Apply a sort preference to one of the columns:
   a. Click Not Sorted next to the column name.
   b. Point to Sort position 1, and then select a sort option.

8. Add a filter to the report for updates that will install upon approval:
   a. Click [+] under Select the filter criteria for the report.
   b. Click Select Field for the new filter entry.
   c. Point to Computer Update Status With Update Information, and then select Update Approval Action (Friendly Name).
   d. Next to the new field name, click Select Operator, and then select equals.
   e. Next to the new operator, click <Enter Value>, and then select Enter Value.
   f. In the text box, enter Install.

9. Add a filter to the report for updates with states that are not Installed or Unknown:
   a. Click [+] next to the existing filter.
   b. Click Select Field for the new filter entry.
   c. Point to Computer Update Status With Update Information, and then select Update Installation State (Friendly Name).
   d. Next to the new field name, click Select Operator, and then select does not equal.
   e. Next to the new operator, click <Enter Value>, and then select Enter Value.
   f. In the text box, enter Installed.
   g. Click the arrow to the left of this filter, and then select Place in New Group.
   h. Click [+] within the new group.
   i. Click Select Field for the new filter entry.
   j. Point to Computer Update Status With Update Information, and then select Update Installation State (Friendly Name).
   k. Next to the new field name, click Select Operator, and then select does not equal.
   l. Next to the new operator, click <Enter Value>, and then select Enter Value.
   m. In the text box, enter Unknown.

10. Click Next.

11. In the Report Name field, enter a unique name. For example, enter Computers to Update.

12. Select Save and run report now.
13. Click Finish.
14. Examine your report and customize the layout as needed. For additional information, see "Using Patch Manager Report Viewer" on page 90.

Installing Updates from a WSUS Report

Complete the following procedure to install updates directly from Report Viewer. In order for this to work, the report must be configured to pull specific data. For additional information, see "Creating a Custom WSUS Report" on page 95.

To install an update from a WSUS report:

1. Run a report that returns the Update ID and Update Revision Number columns.
2. In the Report Viewer window, select the update(s) you want to install.
3. Click the Actions tab.
4. Click Update Management.
5. On the Update Management window, click OK.
6. On the Task Options Wizard window, add the computers on which to install the updates.
7. Click Next.
8. Complete the Scheduling and Notification Options form, and then click Next.
9. Click Finish.

Report Data Sources

Each report category in the Administration and Reporting > Reporting node has a defined collection of data sources that you can use to build reports. In most cases, you use several data sources to build reports with all of the fields you want. However, the data sources in the Windows Server Update Services Analytics and Computer (General) categories contain supersets of other data sources, so you cannot combine data sources from these categories.

To view the available data sources and fields in a report category:

1. In the left pane of the Patch Manager console, expand Administration and Reporting > Reporting, and then expand a parent category.
2. Select the report category.
3. In the lower-center pane, browse available data sources on the left.
4. Select a data source to view its available fields to the right.
Administrating WSUS Using Patch Manager

Use the Enterprise > Update Services node in the Patch Manager console to manage your WSUS server just like you would in the native WSUS console. This node contains a child node for each WSUS server you have registered with Patch Manager. Each WSUS server node contains the native WSUS Updates and Computers and Groups child nodes.

The following sections discuss common WSUS administration tasks and how to execute them from the Patch Manager console.

- Synchronizing WSUS Servers
- Cleaning Up WSUS Servers
- Repairing and Maintaining the Windows Update Agent
- Administrating Windows Update Agent Local Policy

Note: For ConfigMgr instructions see Appendix A: "System Center Configuration Manager 2012 and 2012 R2 Procedures" on page 164.

Synchronizing WSUS Servers

Use the Synchronize Server task to synchronize the selected WSUS server with its upstream server. Review a server's synchronization information on the Details tab of the Enterprise > Update Services > yourWsusServer view.

SolarWinds recommends that you schedule regular synchronization tasks for your WSUS servers to ensure they have the latest updates at all times.

To schedule or execute a synchronization task:

1. In the left pane of the Patch Manager console, expand Enterprise > Update Services, and then select a WSUS server.
2. In the Actions pane (right), click Synchronize Server.
3. Complete the Task Options Wizard to schedule and/or execute the synchronization task for the selected WSUS server. For additional information, see "The Task Options Wizard" on page 62.

Cleaning Up WSUS Servers

Use the Server Cleanup Wizard task to clean up the selected WSUS server. It deletes expired updates and old revisions of updates from the server. This task in the Patch Manager console has two advantages over the native cleanup task in the WSUS console:
The Patch Manager task allows you to configure a threshold for the number of days WSUS keeps non-reporting computers in the console.

You can schedule the Patch Manager task to run regularly, which SolarWinds recommends.

The Server Cleanup Wizard task consists of five distinct actions, which you can run simultaneously or individually on the selected WSUS server:

**Unused updates and update revisions**

The system deletes expired updates that have remained unapproved for three months or longer. Also deletes unapproved, old revisions of updates. The system deletes revisions that have remained unapproved for 30 days or longer.

**Computers not contacting the server**

Deletes computers that have not contacted the Update Server within the computer deletion threshold.

**Configure the computer deletion threshold**

Number of days that the computer must remain out of contact with the server before the system deletes it.

**Unneeded update files**

Deletes update files that other update files and downstream servers do not require to perform their duties. Generally, these updates have been declined.

**Expired Updates**

Declines unapproved, expired updates from Microsoft.

**Superceded Updates**

Declines unapproved updates that have been superseded with approved updates. The system declines superseded updates that have remained unapproved for 30 days or longer.

To schedule or execute a WSUS server cleanup task:

1. In the left pane of the Patch Manager console, expand Enterprise > Update Services, and then select a WSUS server.
2. In the Actions pane (right), click Server Cleanup Wizard.
3. Select one or more of cleanup options, as described previously.
4. Click OK.
5. Complete the Task Options Wizard to schedule and/or execute the cleanup task for the selected WSUS server. For additional information, see "The Task Options Wizard" on page 62.
Repairing and Maintaining the Windows Update Agent

Use the Windows Update Agent Maintenance and Repair task to execute diagnostic and remediation functions on remote Windows Update Agents. In a standard WSUS environment, these functions are only available at the command line, and can only be executed on one system at a time.

The Windows Update Agent Maintenance and Repair task consists of two sections:

- **Repair Options**
- **Maintenance**

**Repair Options**

The task contains several options within this section. The following are the most notable and frequently used.

**Reset Authorization**

This option expires the client-side targeting cookie, which resets the connection to the WSUS server. Use this option when changing clients' group memberships on the WSUS server, or if you identify duplicate client IDs.

**Flush Background Intelligent Transfer Service (BITS) cache**

This option cancels all pending downloads on the client system. Use this option to remove previously-approved updates from the download queue when you remove their approvals.

**Reset Windows Update Agent SUS Client ID**

This option resets the client system's client ID. Use this option when cloning a system from one that has already registered with WSUS.

**Maintenance**

Use the options in this section to maintain, install, or reinstall the Windows Update Agent on one or more remote systems. If you choose to install or reinstall the agent, consider the following:

- The two fields for the Windows Update Agent installer path (x86 and x64) accept paths in both URL and UNC format. For example:
  - **URL Format:** http://dowload.windowsupdate.com/windowsupdate/redist/standalone/7.4.7600.226/windowsupdateagent30-x86.exe
  - **UNC Format:** \fileServer\share\windowsupdateagent30-x86.exe

- If you provide a path in URL format, ensure the clients targeted in the task have access to the internet address you provide.
If you provide a path in UNC format, ensure the clients targeted in the task have access to the server address you provide, and that the server allows access to those clients.

Note: Microsoft shipped Windows 7 and Windows Server 2008 R2 Service Pack 1 with a new version of the Windows Update Agent (WUAgent): v7.5. The current version of the WUAgent for these operating systems is 7.6. If you use this tool to update the WUAgent for these operating systems, be sure to use the current installer, as it addresses a defect in the v7.5 agent.

The following notes apply to the remaining three options in this section:

- The Delete KB Update Uninstall Directories and Delete Service Pack Uninstall Directories options only apply to Windows XP and Windows Server 2003 systems.
- The Change Update(s) Hidden Status To Un-hidden option is not commonly necessary for Windows XP or Windows Server 2003 systems, but is likely to become more widely used with Windows 7 systems.

**Administrating Windows Update Agent Local Policy**

Use the Windows Update Local Policy Management task to manage the Windows Update Agent policy using Local Policy on one or more remote systems. This is particularly useful for non-Active-Directory environments, or when you prefer not to use Group Policy.


Note: This task requires WMI connectivity with the remote system(s). For additional information about enabling WMI connectivity between the Patch Manager server and remote systems, see "Managing Client WMI Connectivity" on page 122.

To manage Windows Update Agent policy on a remote system:

1. The left pane of the Patch Manager console, expand Enterprise > Update Services, and then select a WSUS server.
2. In the Actions pane (right), click Windows Update Local Policy Management.
3. In the Windows Update Local Policy Settings window, click the checkbox next to each setting to toggle between Not Configured, Disabled, and Enabled states.
4. After you have configured the desired settings, click Save.
5. In the Windows Update Local Policy Settings Template window, enter a name for the new template, and then click Save.
6. **If you want to load an existing template**, click Load, and then browse to the template you want to load.

7. Click OK.

8. Complete the Task Options Wizard to schedule and/or execute the task for one or more remote systems. For additional information, see "The Task Options Wizard" on page 62.
Advanced Configuration Options

This chapter addresses advanced configuration options that are commonly used in distributed Patch Manager environments. Review this chapter if you use Patch Manager to manage several sites, domains, or business units, or otherwise want to deploy additional Patch Manager servers for load balancing or fault tolerance. This chapter covers the following topics:

- Patch Manager Management Groups
- Configuring Remote Administration Consoles
- Configuring Additional Patch Manager Servers

For additional information about how to deploy Patch Manager in a distributed environment, see "Advanced Deployment Scenarios" on page 152.

Patch Manager Management Groups

A management group is a logical collection of domains, workgroups, and WSUS servers. Each management group resides on its own Patch Manager Management role server, so the inventory information for each management group has its own database.

When you install the Patch Manager PAS, which includes the Management server role, Patch Manager automatically creates the management group, Managed Enterprise. During configuration you specify what resources you want to manage with the Managed Resource Enterprise Configuration wizard.

Adding Management Groups

As previously noted, each management group resides on its own Patch Manager server. So, when you create a new management group, it must correspond to a new Patch Manager server in the Management server role. The following are use cases for additional management groups:

- Use additional Management role servers to store inventory data from distinct groups of clients in separate databases. These groups must be a defined NetBIOS workgroup, Active Directory Domain, or Active Directory Subdomain.
- Use an additional Management role server with the Application server role in a testing lab. The additional Management role server, and thus the testing lab, would have its own management group.

For additional information about these and other use cases for additional Patch Manager servers, see "Advanced Deployment Scenarios" on page 152.

To add a management group to your Patch Manager environment:
1. Create the new management group and, optionally, configure one or more managed resources.
2. Deploy the new Patch Manager server in the Management role, and then assign it to the new management group.
3. Configure any additional managed resources for the new management group.

For additional information about these procedures, see:

- "Configuring Managed Resources" on page 37
- "Configuring Additional Patch Manager Servers" on page 107

## Adding and Removing Managed Resources

After you initially configure your Patch Manager management group(s), you can add or remove managed resources using one or more of the following tasks:

- Add or Configure WSUS Server
- Configuration Manager Site Server Registration Management
- Management Group Wizard

### Add or Configure WSUS Server

Use the Add or Configure WSUS Server task to register a WSUS server with Patch Manager. The WSUS server must be registered with Patch Manager before you can view it in the Patch Manager console or add it to an existing management group.

**To register a WSUS server with Patch Manager:**

1. In the left pane of the Patch Manager console, expand Enterprise, and then select Update Services.
2. In the Actions pane (right), click Add or Configure WSUS Server.
3. On the Add or Modify WSUS Server window, enter the information for the WSUS server:
   a. In the Server Name field, enter the WSUS server's hostname.
   b. Click Resolve.
   c. Complete any fields the task was not able to automatically populate.
4. Click Save.

### Configuration Manager Site Server Registration Management

Use the Configuration Manager Site Server Registration Management task to register a ConfigMgr site server with Patch Manager. The site server must be registered with Patch Manager before you can view it in the Patch Manager console.

To register a ConfigMgr site server with Patch Manager:
1. In the left pane of the Patch Manager console, expand Enterprise, and then select Configuration Manager Site Servers.
2. In the Actions pane (right), click Configuration Manager Site Server Registration Management.
3. On the Add/Modify Configuration Manager Site Server window, enter the information for the site server:
   a. In the Server Name field, enter the site server's hostname.
   b. Click Resolve.
   c. Complete any fields the task was not able to automatically populate.
4. Click Save.

Management Group Wizard

Use the Management Group Wizard to add or remove resources to/from an existing Patch Manager management group. Remember, to add a WSUS server to a management group, you must first register the server with Patch Manager. For additional information, see "Adding and Removing Managed Resources" on page 104.

To manage the resources managed by a management group:

1. In the left pane of the Patch Manager console, select Patch Manager System Configuration.
2. In the center pane, click Configure Patch Manager Management Groups.
3. On the Management Group Wizard window, select the management group you want to modify, and then click Next.
4. Select the type of resource(s) you want to add, and then click Next.

   If you selected Active Directory Domains or Workgroups:
   a. Next to the Name field, click [...] to open the network browser.
   b. On the Select Domain/Workgroup window, browse the left pane until the resource you want to add is in the upper-right pane.
   c. In the upper-right pane, select the resource you want to add, and then click Add selected.
   d. Repeat these steps for each resource you want to add.
   e. Click OK.

6. If you selected Windows Server Update Services Servers:
   a. In the Server field, select the WSUS server you want to add.
   b. Click Add Update Server.

7. Click Next.
8. On the Management Group Summary page, review your changes, and then click Finish.
Configuring Remote Administration Consoles

In addition to the Patch Manager console included on your PAS, you might want to install additional remote administration consoles throughout your environment. You must associate each console and server with a Patch Manager Application role server. This could be the PAS or any other Patch Manager server in the Application server role.

**Installing the Patch Manager Console**

Use the Patch Manager installer to install a Patch Manager administration console on a remote system. This system can be a server or workstation.

Note: If you plan on integrating Patch Manager with ConfigMgr, install all Patch Manager consoles on computers that already have the ConfigMgr console installed.

To install a Patch Manager console on a remote system:

1. Log on as an administrator to the system on which you want to install Patch Manager.
2. Temporarily disable any antivirus software.
3. Run the SolarWinds Patch Manager.exe installer program.
4. **If the server is missing C++ Runtime and/or Microsoft .NET Framework**, click Install to allow the installation wizard to install the missing component(s).
5. In the Installation Type, select only **Install the Patch Manager administration console**, and click Next. All other checkboxes should be clear.
6. After the installation wizard opens, click **Next**.
7. If necessary, enter YES to create a backup of your Orion database, and then click Next.
8. Accept the terms in the End User License Agreement, and then click Next.
9. Click **Next** to use the default installation folder. Click **Browse** to choose a different folder.
10. Select **Advanced** Install, and click **Next**.
11. Click **Next** to install the selected Patch Manager components.
12. Click **Next** to begin the configuration wizard.
13. Select **Application Server**, and click **Next**.
14. Enter the host name of the Patch Manager Primary Application Server. Click the Test button to ensure that the computer can connect to the PAS. **Note:** The Port field is pre-populated with port 4092. This is the port Patch Manager consoles use to connect to a Patch Manager server. Do not alter this value.
15. Click **Next**.
16. Enter the management group and ensure that **Configure the Windows Firewall for the Server** is selected.
17. Click **Next**.

18. If you do not have a WSUS server, select **Install the Patch Manager WSUS service (Recommended)**. If you already have your own WSUS server, select **I'll supply my own WSUS server**.

19. Click **Next**.

20. Select how Patch Manager should configure IIS.

21. Enter a location that Patch Manager can use to store updates locally.

22. Select **Provision the WSUS Server to the Patch Manager** to manage WSUS from Patch Manager.

23. Click **Next**.

24. Enter the administrator credentials for Patch Manager, and click **Next**.

25. Select your SQL instance and supply the credentials.

26. Click **Next**.

27. Select **Use the default service account** or enter different service account credentials for Patch Manager.

28. Click **Next**.

29. Click **Finish**.

### Configuring Additional Patch Manager Servers

There are several reasons to configure Patch Manager servers in addition to the default PAS. For example:

- Use additional Automation role servers to distribute the load of running Patch Manager tasks.
- Use additional Management role servers to store inventory data from distinct groups of clients in separate databases.
- Use additional Application role servers to distribute the load of running Patch Manager administration consoles.

For additional information about these and other use cases for additional Patch Manager servers, see "**Advanced Deployment Scenarios**" on page 152.

If the standard setup wizards fail, use SetupHelper.exe to provision the additional Patch Manager servers. For additional information, see "**Advanced Setup CLI Commands**" on page 205.

### Installing the Patch Manager Server

Use the Patch Manager installer with the "Advanced" option to install a Patch Manager administration console on a remote system. This system can be a server or workstation.
For additional information about which Patch Manager server roles to install, see "Advanced Deployment Scenarios" on page 152.

To install an additional Patch Manager server:

1. Log on as an administrator to the system on which you want to install Patch Manager.
2. Temporarily disable any antivirus software.
3. Run the SolarWinds Patch Manager.exe installer program.
4. If the server is missing C++ Runtime and/or Microsoft.NET Framework, click Install to allow the installation wizard to install the missing component(s).
5. In the Installation Type, select only Install the Patch Manager administration console, and click Next. All other checkboxes should be clear.
6. After the installation wizard opens, click Next.
7. If necessary, enter YES to create a backup of your Orion database, and then click Next.
8. Accept the terms in the End User License Agreement, and then click Next.
9. Click Next to use the default installation folder. Click Browse to choose a different folder.
10. Select Advanced Install, and click Next.
11. Click Next to install the selected Patch Manager components.
12. Click Next to begin the configuration wizard.
13. Select a role, and click Next.
14. If you are not installing a Primary Application Server, enter the host name of the Patch Manager Primary Application Server. Click the Test button to ensure that the computer can connect to the PAS.
   Note: The Port field is pre-populated with port 4092. This is the port Patch Manager consoles use to connect to a Patch Manager server. Do not alter this value.
15. Click Next.
16. Enter the management group and ensure that Configure the Windows Firewall for the Server is selected.
17. Click Next.
18. If you do not have a WSUS server, select Install the Patch Manager WSUS service (Recommended). If you already have your own WSUS server, select I'll supply my own WSUS server.
19. Click Next.
20. Select how Patch Manager should configure IIS.
21. Enter a location that Patch Manager can use to store updates locally.
22. Select Provision the WSUS Server to the Patch Manager to manage WSUS from Patch Manager.
23. Click **Next**.
24. Enter the administrator credentials for Patch Manager, and click **Next**.
25. Select your SQL instance and supply the credentials.
26. Click **Next**.
27. Select **Use the default service account** or enter different service account credentials for Patch Manager.
28. Click **Next**.
29. Click **Finish**.

To assign a new Patch Manager server to a management group:

1. In the left pane of the Patch Manager console, expand Patch Manager System Configuration, and then select Patch Manager Servers.
2. In the Actions pane (right), click Patch Manager Server Wizard.
3. In the Patch Manager Server Configuration window, select Edit and existing Patch Manager Server's configuration settings, and then click Next.
4. In the Server Name menu, select the new server, and then click Resolve.
5. Click Next.
6. In the Management Group menu, select the management group.
7. Specify any additional settings on this page, and then click Next.
8. On the summary page, verify the settings for the new server, and then click Finish.
Managing Patch Manager Users and Security

Patch Manager uses the following components to manage security in the Patch Manager administration console.

- **Credentials**
- **Credential Rings**
- **Security Roles**
- **User Preferences**
- **Server Certificates**

ConfigMgrNote: The security management tasks discussed in this chapter are available regardless of the Microsoft product you are extending. Although you cannot perform these functions from within the ConfigMgr console, all of the Patch Manager functionality is available in the stand-alone MMC-based console.

You specify credentials and map them to specific resources in the Default credential ring during the initial setup. As you become more familiar with the product and expand its scope in your environment, all four of these security components become necessary to configure Patch Manager to function efficiently and securely.

Additionally, Patch Manager uses specific user credentials to manage security in the Patch Manager web console. For additional information, see "Web Console User Accounts" on page 119.

**Credentials**

Credentials are pairs of user names and passwords, which you assign to credential rings to grant Patch Manager access to managed resources. Patch Manager stores credentials in its database, so it is important to update credentials in Patch Manager anytime the corresponding user name or password changes in Windows.

**Managing Credentials**

View and manage credentials on the Credentials tab of the Patch Manager System Configuration > Security and User Management view. Use the actions associated with this tab to change a password, add a new credential, or delete a credential.

**Changing Credentials' Passwords**

When you change a user account password in Windows, you must also change the corresponding credential's password in Patch Manager.
To change a credential's password:

1. In the left pane of the Patch Manager console, expand Patch Manager System Configuration, and then select Security and User Management.
2. In the center pane, click the Credentials tab.
3. Select the credential you want to modify.
4. In the Actions pane (right), click Change Password.
5. In the Change Password window, enter and confirm the new password.
6. Click Save.

Adding New Credentials

Add credentials whenever you need new or different credentials to access a managed resource.

To add a new credential:

1. In the left pane of the Patch Manager console, expand Patch Manager System Configuration, and then select Security and User Management.
2. In the center pane, click the Credentials tab.
3. In the Actions pane (right), click Add Credential.
4. In the Add user window, enter the new user name in UPN or pre-Windows 2000 format. For example:
   - user@domain.com
   - DOMAIN\userName

Note: To specify a local account with a consistent user name and password across several resources, use \ in front of the user name. For example, enter \administrator for the local Administrator account.

5. Enter and confirm the new password.
6. Click Save.

Note: When you add a new credential, map it to the appropriate resources using the Credential and Credential Ring Rules Wizard. For additional information, see "Managing Credential Rings" on page 112.

Deleting Credentials

Delete credentials in the Patch Manager console to remove them from the Patch Manager database.

To delete a credential:

1. In the left pane of the Patch Manager console, expand Patch Manager System Configuration, and then select Security and User Management.
2. In the center pane, click the Credentials tab.
3. Select the credential you want to delete.
4. In the Actions pane (right), click Delete.
5. In the confirmation dialog, click Yes.

Note: If the credential is currently associated with one or more managed resources, map the resources to a new credential in the Credential and Credential Ring Rules Wizard. For additional information, see "Managing Credential Rings" on page 112.

Credential Rings

Patch Manager uses credential rings to map credentials to managed resources. This way, Patch Manager knows what credential(s) to pull from the database before performing a task on one or more managed computers. Any credential you add to Patch Manager is useless until you map it to at least one resource in a credential ring.

By default, Patch Manager creates the Default credential ring during the initial configuration. At that time, you map credentials to the corresponding resources using rules. Credential rings allow the following types of rules:

- Rules for WSUS servers, ConfigMgr site servers, or specific computers
- Rules for Active Directory Organizational Units (OUs)
- Rules for Active Directory domains or workgroups
- The Default rule

As you add or remove credentials to/from Patch Manager, add them to a credential ring and modify these rules to map them to the appropriate resource(s).

Managing Credential Rings

Use the Credential and Credential Ring Rules Wizard to manage credential rings. You can use this wizard to both manage the credentials on the Patch Manager database, and map those credentials to the appropriate resources.

To manage a credential ring:

1. In the left pane of the Patch Manager console, expand Patch Manager System Configuration, and then select Security and User Management.
2. In the center pane, click the Credential Rings tab.
3. Select the credential ring you want to modify.
4. In the Actions pane (right), click Credential Ring Wizard.
5. On the Credential and Credential Rings Rules Wizard window, specify any credentials you want to add to the Patch Manager database:

   a. Enter the username in UPN or flat format. For example, enter user@domain.company.com or DOMAIN\user.
      Note: To add a common local computer account, enter \ before the username. For example, enter \.\administrator to specify the local Administrator account for several computers.
   b. Enter and confirm the password for that user account.
   c. Click Add.
   d. Repeat these steps for any additional accounts you want to add.

6. Click Next.

7. Create credential ring rules to map credentials to the appropriate resources:

   Note: If you do not map a resource to a specific credential, Patch Manager uses the Default rule to choose credentials for that resource. Modify the Default rule as necessary to accommodate for this.

   a. Click Add Rule, and then select the type of rule you want to add.
   b. In the left pane of the Select Computer window, browse the left pane until the resource you want to add is in the upper-right pane.
   c. In the upper-right pane, select the resource you want to add, and then click Add selected.
   d. Repeat these steps for each resource you want to add.
   e. Click OK.
   f. On the Select User for Credential Rule window, select the credential you want to map to the resource(s), and then click OK.
   g. Repeat these steps for any additional rules you want to add.

8. Click Finish.

**Security Roles**

Patch Manager uses security roles to grant or deny access to application functionality to console users. Each role grants access to specific functionality in the application, so you can be quite granular with your security management architecture.

You can think for the Patch Manager security roles as being divided into the following categories:

- Default Roles
- Operational Roles
- Special Roles
To modify the members in a security role:

1. In the left pane of the Patch Manager console, expand Patch Manager System Configuration, and then select Security and User Management.
2. In the center pane, click the Security Roles tab.
3. Select the role you want to modify.
4. **If you want to add users to the role,** click Add in the Actions pane (right), and then specify the users you want to add:
   a. In the left pane of the Select Users and Groups window, browse the left pane until the user or group you want to add is in the upper-right pane.
   b. In the upper-right pane, select the user or group you want to add, and then click Add selected.
   c. Repeat these steps for each user or group you want to add.
   d. Click OK.
5. **If you want to remove a user or group from the role,** select the user you want to remove in the lower-center pane, and then click Remove in the Actions pane (right).

**Default Roles**

By default, Patch Manager includes the server's local Administrators group in the following security roles, named for the original developer of the product:

- **EminentWare Users**
- **EminentWare Enterprise Administrators**

Important Note: In Active Directory environments, users in the Domain Admins group are default members of every domain member system's local Administrator group. If you do not want to grant membership to these two Patch Manager security roles to all Domain Admins, modify your Patch Manager security role membership as needed.

**EminentWare Users**

This role grants access to the Patch Manager console. In order to be able to do anything in the console, users in this role must also be members of at least one other security role. Similarly, users in other roles must be a member of this role in order to access the console.
EminentWare Enterprise Administrators

This role grants full access to all Patch Manager functionality. This is the only security role authorized to manage memberships in security roles from within the Patch Manager console. That said, Windows users outside of this security roles could potentially alter memberships in the following ways:

- By using the MMC Authorization Manager snap-in
- By altering the EminentWare.BusinessObjects.xml file

Patch Manager uses the AuthZ credential management features native to Windows operating systems. If any users that are not in the EminentWare Enterprise Administrators security role have access to the MMC Authorization Manager snap-in, you should revoke that access if possible.

Patch Manager stores its authorizations in the following location:

%PROGRAMFILES%\SolarWinds\Patch Manager\Server\EminentWare.BusinessObjects.xml

If any local administrator on the Patch Manager server is not a member of the EminentWare Enterprise Administrators security role, you should block access to this file, and preferably the entire ~\Server folder, if possible.

Operational Roles

Use the following operational roles to grant access to the everyday functions in the Patch Manager console in either Administrators or Viewers capacity:

- Computer Configuration
- EminentWare Report
- WSUS Server

Members of these roles in the Administrators capacity have full access to the corresponding functionality. That is, they can view, create, modify, or delete information within the scope of that role. Members in the Viewers capacity have read-only access to the corresponding functionality.

Computer Configuration

This role grants access to information obtained from direct connections to managed computers. This includes any information gathered using WMI and the WMI-based inventory tasks, including the Computer Explorer, and most notably the Update Management and Update Management Wizard tasks.

EminentWare Report

This role grants access to the reports in the Administration and Reporting > Reporting node in the Patch Manager console.
WSUS Server

This role grants access to all functionality involving WSUS servers. This role is almost the equivalent of granting a subset of the functionality available to the WSUS Administrators group on the WSUS server.

Special Roles

Use the following special roles to delegate administrative tasks within the Patch Manager application:

- EminentWare Computer Group Administrators
- WSUS Approval Delegation Administrators
- EminentWare Security Administrators

EminentWare Computer Group Administrators

This role grants complete administrative access to Patch Manager computer groups. Users in this role can create, modify, or delete Patch Manager computer groups from within the Patch Manager console.

WSUS Approval Delegation Administrators

This role grants administrative access to WSUS approval delegation. Users in this role can:

- Enable or disable approval delegation for a WSUS target group
- Grant or revoke accounts' approval privileges
- Modify accounts' update classifications

EminentWare Security Administrators

This role grants administrative access to user and credential management functions in the Patch Manager console. Users in this role are limited to managing credentials, credential rings, and user preferences.

User Preferences

Use the User Preferences tab on the Patch Manager System Configuration > Security and User Management view to create and manage profiles for specific Windows users with access to the Patch Manager console. These preferences include the following settings and assignments:

- Credential Ring
- Export Directory
- Remote Desktop Connection Settings
- Management Groups
- WSUS Servers
- Patch Manager Computer Groups
- Domains and Workgroups

If a Patch Manager console user does not have a specific profile on the User Preferences tab, Patch Manager uses the Default profile when that user connects to a console.

To specify preferences for a user profile:

1. In the Patch Manager console, expand Patch Manager System Configuration, and then select Security and User Management.
2. In the center pane, click the User Preferences tab.

   **If you want to modify the preferences for an existing profile:**
   
   a. Select the user profile you want to modify.
   b. In the Actions pane (right), click Edit.

   **If you want to add a new user profile:**
   
   a. In the Actions pane (right), click Add User.
   b. In the left pane of the Select Users and Groups window, browse the left pane until the user or group you want to add is in the upper-right pane.
   c. In the upper-right pane, select the user or group you want to add, and then click Add selected.
   d. Click OK.

5. Specify the preferences for the user profile according to the following sections.

6. Click Save.

**Credential Ring**

Use this setting to assign a specific credential ring to each user profile. Patch Manager assigns the <Default> credential ring to the Default user profile upon setup, but you can change this setting.

**Export Directory**

Use this setting to specify a default export location for each user profile. The default value is %MYDOCUMENTS%\Patch Manager. In most cases, users can change this location on demand on a per-export basis.

**Remote Desktop Connection Settings**

Use the following settings to specify what preferences Patch Manager passes to mstsc.exe to establish RDP connections:
- Default Screen Resolution
- Use an alternate port for RDP Connection
- Connect to the console session on the selected computer

Management Groups

Use this setting to limit a profile's access to specific Patch Manager management groups. Patch Manager allows the Default user profile access to all management groups.

WSUS Servers

Use this setting to show only specific WSUS servers within a profile's associated management group in the Navigation pane of the Patch Manager console. Patch Manager allows the Default user profile access to all associated WSUS servers.

Patch Manager Computer Groups

Use this setting to limit a profile's access to specific Patch Manager computer groups. Patch Manager allows the Default user profile access to all computer groups.

Domains and Workgroups

Use this setting to limit a profile's access to specific domains or workgroups within a profile's associated management group. Patch Manager allows the Default user profile access to all associated domains and workgroups.

Server Certificates

Patch Manager encrypts all communications between Patch Manager server(s) and console sessions using a 2048-bit security certificate. At a minimum, a single Patch Manager server has at least two certificates:

- One for the certificate authority (CA), which is the PAS, and
- One for each server installation, which includes the PAS

When Patch Manager revokes a certificate, it appends revoked to the beginning of the certificate name. This can happen when you replace a certificate or uninstall a Patch Manager server. In these cases, you may want to delete the revoked certificate(s).

To delete a Patch Manager certificate:

1. In the left pane of the Patch Manager console, expand Patch Manager Server Configuration, and then select Security and User Management.
2. In the center pane, click the Server Certificates tab.
3. Select the certificate you want to delete.
4. In the Actions pane (right), click Delete.
5. On the confirmation prompt, click Yes.

Web Console User Accounts

The Patch Manager web console uses separate user credentials from those Patch Manager uses for the administration console. Create a Patch Manager web console account for each user who needs access to the Patch Manager web console. This allows you to place restrictions on the Patch Manager views and data each user is permitted to access.

Apply User Settings to further restrict access to performance data in the web console. Roles allow administrators to limit the Patch Manager web console views available to groups of users.

Adding Patch Manager User Accounts

Patch Manager supports two types of accounts for web console access:

- Orion Accounts
- Windows Accounts

Orion Accounts

Create Orion accounts in the Patch Manager web console if you want to specify unique credentials for each user in the Orion SQL database.

To add Orion accounts in the Patch Manager web console:

1. Log on to the Patch Manager web console as an administrator.
2. Click Settings.
3. In the Accounts section, click ManageAccounts.
4. Click Add New Account.
5. Select Orion individual account, and then click Next.
6. In the User Name field, enter a user name for the new user.
7. Enter and confirm a new password in the respective fields.
8. Click Next.
9. Specify the account settings for the new user. For additional information, see "Defining User Settings" on page 121.
10. Click Submit.
Windows Accounts

Create Windows accounts in the Patch Manager web console if you want to allow users to access the web console using their existing local or domain Windows accounts. You can add individual Windows users or groups of Windows users.

To add individual Windows accounts as Patch Manager web console users:

1. Log on to the Patch Manager web console as an administrator.
2. Click Settings.
3. In the Accounts section, click ManageAccounts.
4. Click Add New Account.
5. Select Windows individual account, and then click Next.
6. Select the Windows account by following this procedure:
   a. In the User Name field at the top, enter a user name Patch Manager can use to authenticate to the domain you are searching. Use the format, DOMAIN\userName.
   b. In the Password field, enter the password for that account.
   c. In the Search for Account section, enter a search string for the user account you want to add as a Patch Manager web console user.

Note: This field requires the domain and at least a partial user name in DOMAIN\userName format. If you do not know the exact user name, use * as a wildcard character to represent the unknown portions. For example, enter DOMAIN\Jimmy*.
   d. Click Search.
   e. In the Add Users section, select the user(s) you want to add.
   f. Click Next.

7. Specify the account settings for the new user. For additional information, see "Defining User Settings" on page 121.
8. Click Submit.

To add Windows group accounts as Patch Manager web console users:

1. Log on to the Patch Manager web console as an administrator.
2. Click Settings.
3. In the Accounts section, click ManageAccounts.
4. Click Add New Account.
5. Select Windows group account, and then click Next.

6. Select the Windows group account by following this procedure:
   
   a. In the User Name field at the top, enter a user name Patch Manager can use to authenticate to the domain you are searching. Use the format, DOMAIN\userName.
   
   b. In the Password field, enter the password for that account.
   
   c. In the Search for Account section, enter a search string for the group account from which you want to create new Patch Manager web console users.

   Note: This field requires the domain and at least a partial group name in DOMAIN\groupName format. If you do not know the exact group name, use * as a wildcard character to represent the unknown portions. For example, enter DOMAIN\admin*.

   d. Click Search.

   e. In the Add Groups section, select the group(s) you want to add.

   f. Click Next.

7. Specify the account settings for the new users in this Windows group. For additional information, see "Defining User Settings" on page 121.

8. Click Submit.

**Defining User Settings**

When you create new users Patch Manager web console users, you have the option to configure a variety of user settings. These settings allow you to limit and customize what each user in the web console.

You can also modify user settings at any time, either individually or in batches. Only Patch Manager web console users with administrator rights have permission to change user settings.

To change Patch Manager web console user settings:

1. Log on to the Patch Manager web console as an administrator.

2. Click Settings.

3. In the Accounts section, click Manage Accounts.

4. Select the user(s) whose settings you want to modify, and then click Edit.

5. **If you selected multiple users**, select the specific setting(s) you want to modify. When you click Submit, the Patch Manager web console only modifies the selected settings for the selected users.

6. Modify the settings as necessary. For additional information, see "Patch Manager Web Console User Settings" on page 199.

7. Click Submit.
Managing Client WMI Connectivity

Patch Manager has the option to connect to managed clients using Windows Management Instrumentation (WMI). To facilitate these connections, Patch Manager uses a software component called WMI Providers. Without the WMI Providers, Patch Manager can only interface with WSUS, not directly with managed clients.

The WMI Providers enable Patch Manager to do the following on managed clients:

- Deploy updates on demand using the Update Management and Update Management Wizard tasks.
- Conduct Managed Computer Inventory tasks to retrieve detailed information about managed clients.
- Perform configuration management tasks, such as Shutdown or Reboot, Refresh Group Policy, and Client Certificate Management.
- Use the Computer Explorer to browse computer details and launch configuration management tasks.

For additional information about using the WMI Providers in your environment, see the following sections:

- WMI Requirements
- Security and Permissions
- Provisioning the WMI Providers
- Troubleshooting WMI Connections
- Fixing WMI Connectivity Issues
- Verifying WMI Connectivity

WMI Requirements

To make a successful WMI connection with a remote system, Windows requires the following:

- File & Print Sharing enabled on the remote system
- WMI Firewall Exception on the remote system
- Credentials with local administrator rights on the remote system in the Patch Manager Credential Ring
- RPC Service enabled on the remote system
- Distributed COM (DCOM) enabled on the remote and local systems
• Ports 135, 445, and dynamic ports 1024 to 65536 open between Patch Manager and the remote system

For additional information about the port requirements for WMI connections, see "Port and Firewall Information" on page 24.

Security and Permissions

The WMI Providers only run on demand when Patch Manager tasks require their capabilities. They run as a process on the remote system when needed; they do not run as a service. By default, the SolarWinds WMI Providers run under their own process using the Local System account. Their operations impersonate the security context of the caller when executed. That is, they use appropriate credential stored in the Patch Manager database as assigned in the console user's credential ring.

For additional information about credentials and credential rings, see "Managing Patch Manager Users and Security" on page 110.

Provisioning the WMI Providers

If you want to deploy WMI Providers manually using Tasks, complete the following procedure.

Note: For ConfigMgr instructions see Appendix A: "System Center Configuration Manager 2012 and 2012 R2 Procedures" on page 164.

To create a task to deploy WMI Providers to managed computers using Computer Access Management:

1. In the left pane of the Patch Manager console, select Administration and Reporting.
2. In the center pane, click Check and Manage Computer Access.
3. In the Computer Access Management dialog, select Install the WMI Providers if not already installed, and then click OK.
4. Complete the Task Options Wizard to specify the target systems and schedule and/or execute the task. For additional information, see "The Task Options Wizard" on page 62.

To deploy WMI Providers using the Deploy Client Components action:

1. In the left pane of the SolarWinds Patch Manager console, expand Enterprise > Managed Computers.
2. Select a computer from the center pane.
3. In the Actions pane, click Deploy Client Components.
4. The system displays the Task Options Wizard.
5. Select Install or Repair Client Components.
6. Click Next.
7. Select **Install WMI Providers** - Installs the correct providers on your managed computer.
8. Click **Next**.
9. Choose **Install using Remote install Service** - Installs the components immediately.
10. Click **Next**.
11. Select the clients you want to deploy the components.
12. Click **Next**.
13. Review your selections.
14. Click **Finish**.

**Troubleshooting WMI Connections**

When you target a remote system for a Managed Computer Inventory task, Patch Manager displays that system in the Enterprise > Managed Computers node. Select a system in the center pane of this view to see useful information about the most recent WMI connection attempt.

**Viewing WMI Connectivity Details**

The Computer Details tab on the Enterprise > Managed Computers view is particularly helpful when diagnosing WMI connectivity issues with remote systems. Computers with connectivity issues appear in the top pane of this view with either a red circle or yellow triangle over the computer icon in the Name column. Use the details in the lower pane to troubleshoot the issues.

To view WMI connectivity details for a remote system:

1. In the left pane of the Patch Manager console, expand Enterprise, and then select Managed Computers.
2. In the upper-center pane, select a computer.
3. In the lower-center pane, note the statuses for the following connection attempts:
   - Last DNS resolution attempt
   - Last ARP resolution attempt
   - Last Endpoint Mapper connection attempt
   - Last File and Printer Sharing connect attempt
   - Last WMI connect attempt
4. Troubleshoot any Failed statuses as described in the following sections.
Note: In some cases, all of these statuses can report as Success while Patch Manager returns a connection error at the bottom of this view. In these cases, troubleshoot the specific data source or object cited in the error message, or modify your Inventory task to exclude that data source.

**Last DNS resolution attempt**

Reports the status of the attempt to resolve the computer name Patch Manager obtained from the computer container defined in the Inventory task. If Patch Manager can resolve the name, it stores the IP address in the computer record, and the status here is Success. If Patch Manager cannot resolve the name, the status here is Failed.

Troubleshooting: If Patch Manager cannot resolve the computer name of a remote system, check the network's DNS records and/or the local hosts file.

**Last ARP resolution attempt**

Reports the status of the attempt to resolve the IP address Patch Manager obtained from DNS. If Patch Manager can resolve the IP address, it stores the MAC address in the computer record, and the status here is Success. If Patch Manager cannot resolve the IP address, the status here is Failed.

Note: If a remote system is on the other side of a network boundary, such as a router or gateway, the boundary device responds to an ARP resolution attempt with its own MAC address. In these cases, Patch Manager identifies the MAC address as coming from a boundary device and returns a status of Failed. This is normal for systems in remote networks and is not necessarily indicative of WMI connection failure.

**Last Endpoint Mapper connection attempt**

Reports the status of the attempt to connect to the RPC Endpoint Mapper on port 135 on the remote system. If Patch Manager can connect to the RPC Endpoint Mapper, the status here is Success. If Patch Manager cannot connect, the status here is Failed.

Troubleshooting: If the status here is Failed and DNS resolution was successful, ensure a firewall is not blocking traffic to the remote system on port 135.

**Last File and Printer Sharing connect attempt**

Reports the status of the attempt to establish a file sharing session on port 445 using SMB over IP. If Patch Manager can establish the file sharing session, the status here is Success. If Patch Manager cannot establish the session, the status here is Failed.

Troubleshooting: If the status here is Failed, ensure the File and Printer Sharing service is enabled on the remote system. If there are intermediate firewalls between the Patch Manager server and the remote system, ensure the intermediate firewalls are not blocking traffic to the remote system on port 445.
Last WMI connect attempt

Reports the status of the attempt to establish the WMI session. If Patch Manager can establish the WMI session, the status here is Success. If Patch Manager cannot establish the session, the status here is Failed.

Troubleshooting: If the status here is Failed and the previous statuses are Success, ensure the credentials defined in the credential ring for the remote system are correct. The account used to establish the WMI session must have local Administrator permissions on the remote system.

Fixing WMI Connectivity Issues

If you recognize an issue with WMI connectivity to a remote system, use the Check and Manage Computer Connectivity task to help resolve the issue. This launches the same dialog you can use to provision the WMI providers to remote systems. The difference is you execute this task from the Enterprise > Managed Computers view.

Note: For ConfigMgr instructions see Appendix A: "System Center Configuration Manager 2012 and 2012 R2 Procedures" on page 164.

To complete the Check and Manage Computer Connectivity task:

1. In the left pane of the Patch Manager console, expand Enterprise, and then select Managed Computers.
2. **If you want to specify a single computer**, select the computer you want to fix in the center pane.
3. In the Actions pane (right), click Check and Manage Computer Connectivity.
4. On the Computer Access Management window, select the appropriate options as described in the following sections.
5. Click OK.
6. Complete the Task Options Wizard to specify the target systems and schedule and/or execute the task. For additional information, see "The Task Options Wizard" on page 62.

The following sections provide additional information related to this task:

- [SolarWinds WMI Providers Actions](#)
- [Additional Options](#)
- [Additional Requirement for Windows XP](#)

### SolarWinds WMI Providers Actions

The first section of the Computer Access Management window addresses options to install, reinstall, or uninstall the SolarWinds WMI Providers. Choose one of the following:
**Check if WMI Providers are installed**

Checks for the WMI Providers on the remote system. View results from this check in the Patch Manager Task History, or configure the task to email you the results.

**Install the WMI Providers if not already installed**

Installs the WMI Providers if needed. This option also allows you to reinstall the WMI Providers if necessary.

**Uninstall the WMI Providers**

Uninstalls the WMI Providers from the remote system.

**Additional Options**

The remainder of the Computer Access Management window addresses options to configure remote systems to allow WMI connections. Select any combination of the following:

**Enable DCOM if disabled**

Enables Distributed COM (DCOM) on the remote system. This is a requirement for Patch Manager to use WMI to connect to remote systems.

**Configure DCOM permissions to include 'Administrators' group if needed**

Modifies DCOM permissions to allow users from the Administrators group in Windows. Patch Manager requires local Administrator permissions on remote systems to run the WMI Providers.

**Enable the 'Remote Administration' firewall rule (Windows Firewall/Advanced Firewall only)**

Enables the Remote Administration firewall ruleset in Windows Firewall. If you are using a third party firewall solution, administer the necessary rules in your firewall through other means.

**Create ADMIN$ share if missing**

Creates the ADMIN$ share on Windows 2000 systems. Systems running Windows XP and later create the ADMIN$ share automatically on startup. However, it is possible to delete this share in Windows 2000.

**Enable Windows Installer service if disabled**

Re-enables the Windows Installer service on the remote system. Patch Manager requires this service to install the WMI Providers.

**Enable MSI Logging**

Enables MSI logging on the remote system. This option is selected by default, but you can clear it if you do not want MSI logging turned on.
Additional Requirement for Windows XP

If the systems you are troubleshooting are running Windows XP, note the following additional requirement when those systems are members of a workgroup.

To configure Windows XP Workgroup clients to allow WMI connections:

1. On the affected system, open Registry Editor (regedit.exe).
2. Expand HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control.
3. Select Lsa.
4. Change the value for the forceguest DWORD to 0:
   a. In the right pane, select forceguest.
   b. Click the Edit menu, and then select Modify.
   c. Enter 0 into the text box.
   d. Click OK.

For additional information about this requirement, see the Microsoft knowledge base article, "How to Set Security in Windows XP Professional That Is Installed in a Workgroup," http://support.microsoft.com/?kbid=290403.

Verifying WMI Connectivity

After you have WMI connectivity configured for your environment, use the Inventory – verify access only Managed Computer Inventory option to verify WMI connectivity with your remote systems.

Note: For ConfigMgr instructions see Appendix A: "System Center Configuration Manager 2012 and 2012 R2 Procedures" on page 164.

To verify WMI connectivity with your remote systems:

1. In the left pane of the Patch Manager console, expand Enterprise, and then select Managed Computers.
2. **If you want to specify a single computer**, select the computer you want to fix in the center pane.
3. In the Actions pane (right), click Inventory.
4. On the Inventory Options window, select Inventory – verify access only.
5. Click OK.
6. Complete the Task Options Wizard to specify the target systems and schedule and/or execute the task. For additional information, see "The Task Options Wizard" on page 62.
View results from this check in the Patch Manager Task History, or configure the task to email you the results.
Patch Manager Agents

While Patch Manager is an agent-less patch deployment system, there may be times when an agent is the best solution in your environment. If you have computers that spend a lot of time off the corporate networks, computers that cannot be managed with WMI, or computers protected by stringent firewall rules or VPNs, deploying Patch Manager agents would be a good option. Patch Manager will not spend time trying to update a computer that is not on the network.

You can perform most of the same actions on remote computers with an agent installed as you can using WMI providers.

After an agent is installed, the agent communicates back to the Patch Manager server and requests a certificate exchange. The certificate is based on mutual authentication and must be present on the managed computer before the agent can perform any tasks. Agents that have exchanged certificates fall in the approved category. You may deploy pre-provisioned agents that have already exchanged certificate information. Agents attempt to poll the server at set intervals using asynchronous RPC.

Use the following topics to learn more:

- Agent Requirements
- Deploying Agents
- Approving Agents
- Configuring Agents

Agent Requirements

Clients you wish to install an agent on must meet the same Operating System (managed clients) requirements as listed in the Requirements section.

Additionally, the client computers uses the following resources:

- 30 MB or more of available RAM
- 55 MB hard disk

The consumed resources also include the space taken for the WMI providers.

Deploying Agents

Agents can be deployed in four ways:
Deployed from the Patch Manager Console

- Offline deployment using the Patch Manager Console
- Distributed using WSUS
- Manually installed on the client

**Deploy from the Patch Manager Console**

You can push the agent to the client computer from the Patch Manager Console. After the agent is installed on the client, the agent communicates back to the server to request a certificate. After you approve the certificate exchange, the agent is ready for use.

**To push the agent:**

1. In the left pane of the SolarWinds Patch Manager console, expand **Enterprise > Managed Computers**.
2. Select a computer from the center pane.
3. In the Actions pane, click **Deploy Client Components**.
4. The system displays the **Task Options Wizard**.
5. Select **Install or Repair Client Components**.
6. Click **Next**.
7. Choose both of the following:
   - **Install WMI Providers** - Installs the correct providers on your managed computer
   - **Install the Patch Manager Agent** - Installs the client agent on your managed computer
8. Click **Next**.
9. Choose **Install using Remote install Service** - Installs the components immediately.
10. Click **Next**.
11. Select the clients you want to deploy the components.
12. Click **Next**.
13. Review your selections.
14. Click **Finish**.
Offline Deployment

Agents can be deployed to client computers not currently connected to the corporate network. This process provisions the agent with a certificate so that you do not need to approve the agent.

To provision an agent offline:

1. In the left pane of the SolarWinds Patch Manager console, expand Enterprise > Managed Computers.
2. Select a computer from the center pane. In the Actions pane, click Provision Agent Offline. The Agent Provisioning Wizard displays.
3. Ensure that the host information is correct.
4. Click Next.
5. Click Browse and select the location where you want to place the provisioning installer.
6. Select Recreate existing certificate if you do not want to use the existing certificate.
7. Enter the password used to protect the signed Patch Manager server certificate.
8. Click Finish.

Distribute using WSUS

If you wish to distribute the agent to multiple computers at once, you can create an installer package and distribute it through WSUS as you normally would.

To create a WSUS installer package:

1. In the left pane of the SolarWinds Patch Manager console, expand Enterprise > Managed Computers.
2. Select a computer from the center pane.
3. In the Actions pane, click Deploy Client Components.
4. The system displays the Task Options Wizard.
5. Select Install or Repair Client Components.
6. Click Next.
7. Choose both of the following:
   - Install WMI Providers - Installs the correct providers on your managed computer
   - Install the Patch Manager Agent - Installs the client agent on your managed computer
8. Click Next.
9. Choose Create a WSUS Installer Package.
10. Click Next.
11. Select the clients you want to deploy the components.

12. Click **Next**.

13. Review your selections.

14. Click **Finish**.

Publish this package as you would any other package.

**Manual Install**

You can manually install the agent on the client computer using the WMI Providers installer. You must have your PAS information available to install the agent.

**To create a WMI providers package:**

1. Run the WMI providers installer.

2. Click **Next**.

3. Accept the EULA, and click **Next**.

4. Select Complete, and click **Next**.

5. Change the installation folder if necessary.

6. Enter the PAS information.

7. Select **Request recreating Certificate**.

8. Click **Next**.

9. Click **Next** again to complete the installation.

**Approving Agents**

Approval for agents indicate that the agent has exchanged certificate information with the Patch Manager server and is ready to accept commands. Agents must be approved before they can approve any actions on the remote client.

You can view all unapproved, approved, and preapproved agents in the **Agents** node under **Enterprise**.

**To disable or enable automatic approvals:**

1. In the tree view in the left pane of the application, expand the **Patch Manager System Configuration** level.

2. Expand the **Management Groups** level to find the management group you created.
3. Select the management group from the tree view.

4. Navigate to the Settings tab.

5. Select **Enable automatic approval of agents**.

6. In the Actions pane, click **Edit**.

7. Select **Enabled** or **Disabled**.

8. Click **OK**.

If you disable automatic approvals, you can manually approve agents by navigating to Enterprise > **Agents** and clicking **Approval Management**. Select the computer the agent is installed on from the list and click **Approve Selected**.

### Configuring Agents

You can use policies and policy templates to configure your agents. Configuration settings such as polling intervals, auto-update settings, and timeouts can be added to a policy template and assigned to an agent or multiple agents using Patch Manager routing rules.

**To create a policy:**

1. In the tree view in the left pane of the application, select **Patch Manager System Configuration**.

2. Click **Policy Editor** in the center pane.

3. Click **Create Policy**...

4. Enter the policy name, and make changes to the available settings.

5. Click **Scopes** to modify the scope of the policy.

6. Click **Save**.

**To apply a policy to specific scopes:**

1. In the tree view in the left pane of the application, select **Patch Manager System Configuration**.

2. Click **Policy Assignment**.

3. Create a scope or select a scope.

4. Select a **Policy**.

5. Click **Save**.
Using the Patch Manager Web Console

The Patch Manager web console displays read-only data collected from the Patch Manager servers. If you are a Patch Manager web console user, review the following sections:

- Using the Web Console Notification Bar
- Viewing Consolidated Patch Manager Data
- Customizing Views

Note: Some of the features in the Patch Manager web console do not work unless it is running with another Orion Platform product. The sections in this chapter only describe features that do not have this additional requirement.

Using the Web Console Notification Bar

Below the web console menu bar, the SolarWinds Notification Bar provides informational messages related to permissions, polling errors and other messages related to your SolarWinds servers.

For more information about any displayed Notification Bar message, navigate to the related setting or resource listed in the message, click the hyperlink imbedded in the message, or contact your Patch Manager administrator.

To address messages in the notification bar:

- **If you want to clear a single message**, click Dismiss Message next to the message you want to clear, or address the situation mentioned in that message.
- **If you want to clear the entire notification bar**, click [x] on the right end of the notification bar.

Note: Some messages in the notification bar cannot be dismissed. If you close the notification bar and it contains one of these messages, the notification bar reopens the next time the page refreshes. The notification bar also reopens any time a new message appears.

Viewing Consolidated Patch Manager Data

The Patch Manager web console consolidates data from Patch Manager and WSUS servers and presents the information in configurable views. You access these views from the menu bar under their respective tabs.

Default Tabs and Related Views

The Patch Manager web console displays the following tabs at the top of the web console:
When you point your mouse at either of these tabs, the web console displays their respective menu bars. The following define the default views on each menu bar. You can also customize the menu bars on these tabs on a per-user basis. For additional information about changing the menu bar related to these tabs, see "Defining User Settings" on page 121.

**Default Home Tab Views**

The Patch Manager web console displays the following views on the menu bar under the Home tab. In Orion web consoles with only the Patch Manager module, most of these views are not applicable. For information about how to customize this menu bar, see "Customizing Menu Bars" on page 140.

<table>
<thead>
<tr>
<th>View</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Overview of Orion Platform events and alerts</td>
</tr>
<tr>
<td>Groups</td>
<td>SolarWinds Orion Platform Groups data</td>
</tr>
<tr>
<td>Top 10</td>
<td>Network devices by utilization and by number of events</td>
</tr>
<tr>
<td>Events</td>
<td>Orion Platform event messages in the past 24 hours</td>
</tr>
<tr>
<td>Alerts</td>
<td>Orion Platform alerts in the past 24 hours</td>
</tr>
<tr>
<td>Message Center</td>
<td>Collection of event and alert messages in the last 24 hours</td>
</tr>
<tr>
<td>Reports</td>
<td>Orion Platform reports</td>
</tr>
<tr>
<td>thwack</td>
<td>Opens <a href="http://thwack.solarwinds.com">http://thwack.solarwinds.com</a> in a new browser window</td>
</tr>
<tr>
<td>Custom Summary</td>
<td>Customizable resources to display specific Orion Platform objects</td>
</tr>
<tr>
<td>Training</td>
<td>Collection of videos and documentation for Orion Platform products and concepts</td>
</tr>
</tbody>
</table>

**Default Patches Tab Views**

The Patch Manager web console displays the following views on the menu bar under the Patches tab.

<table>
<thead>
<tr>
<th>View</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patch Summary</td>
<td>Summary of data collected from the Patch Manager Application role server</td>
</tr>
</tbody>
</table>
Customizing Views

Users whose user settings allow customizations can customize their views by changing the layout and composition of the resources the web console displays. For additional information about allowing customizations, see "Defining User Settings" on page 121.

Note: When a user changes the layout of a view that other users also see, the changes affect the view for all users.

To customize a view:

1. Log on to the Patch Manager web console.
2. Click the view you want to change.
3. Click Customize Page.
4. **If you want to change the column layout of the view:**
   a. Click Edit next to the column definition.
   b. Select the number of columns you want in the view.
   c. Specify the width, in pixels, of each column.
   d. Click Submit.
5. **If you want to delete a resource from a column**, select the resource, and then click [x] next to the column.
6. **If you want to add a resource**, repeat the following steps for each resource you want to add.
   a. Click [+] next to the column you want to modify.
   b. Expand the appropriate resource category or categories.
   c. Select the resource(s) you want to add.
   d. Click Submit.

Note: It is possible to duplicate resources in the view.

7. **If you want to rearrange the resources in the view**, use the directional arrows next to each Resources in Column box.
8. **If you want to preview your view in a new browser tab**, click Preview. Return to the Customize page to save your changes.
9. Click Done.
**Administrating the Patch Manager Web Console**

The Patch Manager web console displays read-only data collected from the Patch Manager servers. If you are a Patch Manager administrator, review the following sections:

- Creating and Managing Views
- Customizing Menu Bars
- Customizing the Web Console Banner
- Setting the Web Console Refresh Rate

**Notes:**

- Some of the features in the Patch Manager web console do not work unless it is running with another Orion Platform product. The sections in this chapter only describe features that do not have this additional requirement.
- The Patch Manager web console uses different credentials from those Patch Manager uses for the administration console. Configure specific users for the Patch Manager web console as described in "Web Console User Accounts" on page 119.

**Creating and Managing Views**

Views are configurable presentations of Patch Manager information. A view can include maps, charts, summary lists, reports, events, and links to other resources. As an administrator, you can assign views to menu bars, and customize each view. You may also select the charts and device properties that are displayed on each view. This section addresses the following procedures:

- Creating New Views
- Editing Existing Views
- Adding Custom Views to Menu Bars

**Creating New Views**

You can begin customizing the Patch Manager web console by creating new views. Complete the following procedure to create a new view.

To create a new view:

1. Log on to the Patch Manager web console as an administrator.
2. Click Settings.
3. In the Views section, click Add New View.
4. In the Name of New View field, enter a distinct name for the new view.
5. In the Type of View menu, select the type of view you want to create. The bottom of the Add New View web page defines each view type.
6. Click Submit.
7. **If you want to change the column layout of your view:**
   a. Click Edit next to the column definition.
   b. Select the number of columns you want in the view.
   c. Specify the width, in pixels, of each column.
   d. Click Submit.
8. In each Resources in Column box, add resources for the new view:
   a. Click [+] next to the column you want to modify.
   b. Expand the appropriate resource category or categories.
   c. Select the resource(s) you want to add.
   d. Click Submit.
9. Use the directional arrows next to each Resources in Column box to rearrange the resources you have added.
10. **If you want to preview your view in a new browser tab**, click Preview.
11. Click Done.

**Editing Existing Views**

You can configure an existing view by completing the following procedure.

To edit an existing view:

1. Log on to the Patch Manager web console as an administrator.
2. Click Settings.
3. In the Views section, click Manage Views.
4. Select the view you want to edit, and then click Edit.
5. Complete the task as if creating a new view. For additional information see "Creating New Views" on page 138.
Adding Custom Views to Menu Bars

After you create a custom view, add it to a menu bar to access it quickly from the Patch Manager web console.

To add a view to a menu bar:

1. Log on to the Patch Manager web console as an administrator.
2. Click Settings.
3. In the Customize section, click Customize Menu Bars.
4. If you want to edit an existing menu bar, click Edit under the menu bar's title.
5. If you want to add the view to a new menu bar, create the new menu bar, and then complete this procedure for the new menu bar. For additional information, see "Creating New Menu Bars" on page 140.
6. Drag the view from the Available items list into the Selected items list.
7. Click Submit.

Customizing Menu Bars

Menu bars are displayed at the top of every page. As an administrator, you can create different menu bar configurations and assign them to users as needed. Each user has the potential to see a different set of menu bars.

Creating New Menu Bars

Create new menu bars using the drag and drop Menu Bar interface. Complete the following procedure to create a new menu bar.

After you create a new menu bar, assign it to users in the users' settings. For additional information, see "Defining User Settings" on page 121.

To create a new menu bar:

1. Log on to the Patch Manager web console as an administrator.
2. Click Settings.
3. In the Customize section, click Customize Menu Bars.
4. Click New Menu Bar.
5. Type a name for the menu bar at the top of the form.
6. If you want to add a menu item, drag the menu item from the Available items column to the Selected items column.

Note: You cannot drag a menu item by its Edit button.
7. **If you want to change the order of menu items**, drag the menu item to a new location in the Selected items column.

8. **If you want to remove a menu item**, drag the menu item back to the Available items column.

9. **If you want to rename a menu item**, click Edit on the menu item.

10. **If you want to add a custom menu item**, click Add, and then complete the form for the custom menu item.

11. **If you have finished configuring your menu bar**, click Submit.

### Editing Existing Menu Bars

You can configure an existing menu bar by completing the following procedure.

To edit an existing view:

1. Log on to the Patch Manager web console as an administrator.
2. Click Settings.
3. In the Customize section, click Customize Menu Bars.
4. Click Edit under the menu bar's title.
5. Complete the task as if creating a new menu bar. For additional information see "Creating New Menu Bars" on page 140.

### Adding Custom Links to Menu Bars

You can add a custom link to the menu bars in the Patch Manager web console by completing the following procedure.

To add a custom link to a menu bar:

1. Log on to the Patch Manager web console as an administrator.
2. Click Settings.
3. In the Customize section, click Customize Menu Bars.
4. Click Edit under the menu bar's title.
5. Add the custom link to the Available items column:
   a. Click Add.
   b. In the Name field, enter a display name for the link.
   c. In the URL field, enter the address for the link.

Note: To link to an external webpage, include the protocol in the address. For example, to link to www.solarwinds.com, enter http://www.solarwinds.com.
d. **If you do not want the link to open in a new window or tab,** clear the check box, Open in a New Window.

e. Click OK.

6. Drag the custom link to the Selected items column.

7. Click Submit.

**Customizing the Web Console Banner**

The banner at the top of the Patch Manager web console consists of two parts: an image and a background. You can customize this banner to display your logo instead of the default SolarWinds logo at the top of every web console page.

To customize the Web Console banner:

1. Log on to the Patch Manager web console as an administrator.
2. Click Settings.
3. In the Settings section, click Web Console Settings.
4. In the Site Logo URL field, enter a URL for the new logo.

Notes:

- The SolarWinds logo image is 182x50 pixels, though the banner will be automatically resized to accommodate a taller image.
- The default file path for the images folder used to store the default images is %SystemDrive%\IIS\SolarWinds\NetPerfMon\images.
- The SolarWinds.com End User License Agreement prohibits the modification of the SolarWinds logo.

5. **If you want to revert to the default settings,** replace the custom logo URL with the default URL: /NetPerfMon/images/SolarWinds.Logo.png.

6. Click Submit.

**Setting the Web Console Refresh Rate**

The default refresh rate for the Patch Manager web console is 5 minutes. You can customize this interval to make the Patch Manager web console refresh as frequently or infrequently as you would like.

To set a custom refresh rate for the web console:
1. Log on to the Patch Manager web console as an administrator.
2. Click Settings.
3. In the Settings section, click Web Console Settings.
4. Enter a whole number value between 1 and 999 in the Page Refresh field. The refresh rate is measured in minutes.
5. Click Submit.
Maintaining Patch Manager

The sections in this chapter describe on-going administrative tasks to maintain your Patch Manager environment. If you are a Patch Manager administrator, review the following sections:

- Managing Patch Manager Tasks
- Clearing Caches, Layouts, Tasks, and Packages
- Viewing Server Settings and Details

ConfigMgr Note: The tasks discussed in this chapter are available regardless of the Microsoft product you are extending. Although you cannot perform these functions from within the ConfigMgr console, all of the Patch Manager functionality is available in the stand-alone MMC-based console.

Managing Patch Manager Tasks

It is important to be diligent about managing your Patch Manager tasks because the Task History is one of the two components SolarWinds uses to license the Patch Manager software. There are two ways to manage your Patch Manager tasks:

- Managing Scheduled Tasks
- Managing Task History

Managing Scheduled Tasks

Use the Scheduled Tasks node to run, view, or otherwise manage tasks you have scheduled to run at a future and/or recurring time.

When you select a scheduled task, you have the following options in the Actions pane:

**Run Task Now**

Executes the task without modifying the existing schedule settings.

**Enable/Disable Task**

Alternately enables or disables the task, depending on its current state.

**Properties**

Opens the Task Options Wizard for the existing task.

**Delete**

Permanently deletes the task.

To manage a scheduled task:
1. In the left pane of the Patch Manager console, expand Administration and Reporting, and then select Scheduled Tasks.
2. In the center pane, select the task you want to manage.
3. In the Actions pane (right), select one of the options discussed previously.

Managing Task History

Use the Task History node to view and modify the "online" history of tasks in the Patch Manager console. Remember, Task History is one of the two components SolarWinds uses to license Patch Manager. To effectively manage your Patch Manager node count, ensure your Task History items only contain computers you are actively managing.

Deleting Task History Items

From time to time, you may want to manually delete Task History items if they contain computers that you no longer wish to manage with Patch Manager. For example, if you know an Inventory task contains a computer that is no longer enabled, you can delete that Task History item to remove that computer from the pool of Patch Manager nodes.

To delete a Task History item:

1. In the left pane of the Patch Manager console, expand Administration and Reporting, and then select Task History.
2. In the center pane, select the Task History item you want to delete.
3. In the Actions pane (right), click Delete Task.
4. Click Yes to confirm your selection.

Configuring Task History Retention Settings

By default, Patch Manager deletes Task History items after 60 days. Customize the Application Server settings to retain items for a longer or shorter period and define whether you want to archive, rather than delete, Task History items.

To customize Task History retention settings:

1. In the left pane of the Patch Manager console, expand Patch Manager System Configuration > Patch Manager Servers, and then select Application Servers.
2. In the upper-center pane, select the application server.
3. In the lower-center pane, click the Application Server Settings tab.
4. Filter the Category column for General:
a. On the Category column, click ☑.
b. Select General.

5. Select each of the following settings, and then click Modify Setting in the Actions pane (right) to open a dialog for that setting:
   - Automatically archive Task History Enabled
   - Automatically archive Task History Days

6. Modify the settings as appropriate, and then click OK to close the dialog.

Note: When Patch Manager archives Task History items, it stores them in the following folder:
%PROGRAMFILES%\SolarWinds\Patch Manager\Server\archives

**Clearing Caches, Layouts, Tasks, and Packages**

As it operates, the Patch Manager server stores XML files in the ~\Server\Data folder, which eventually grows to consume a notable quantity of disk space. The Clear Caches and View Layouts task in the Patch Manager console provides the following options:

**Clear Caches**

Clears the XML files from the ~\Server\Data folder. Patch Manager generates these files during normal operations, and they consume considerable space over time.

**Delete Old Tasks**

Deletes console-related worker files for old tasks from the server. The Patch Manager stores these files in the local server's ~\EminentWare\Tasks folder.

**Clear View Layouts**

Reverts all custom view layouts in the Patch Manager console to their default configurations. If you want to backup these custom layouts, find them in the ~\EminentWare\gridlayout folder.

**Clear Packages**

Deletes console-related worker files for old packages from the server. The Patch Manager stores these files in the local server's ~\EminentWare\Packages folder.

**Automatic Task Maintenance**

Allows you to specify whether you want Patch Manager to automatically delete old tasks after a period of time you specify.

Note: The default paths for the folders referenced in these definitions are:
Windows XP and earlier

- %PROGRAMFILES%\SolarWinds\Patch Manager\Server\Data
- %USERPROFILE%\Local Settings\Application Data\EminentWare

Windows Vista and later

- %PROGRAMFILES%\SolarWinds\Patch Manager\Server\Data
- %USERPROFILE%\AppData\Local\EminentWare

To clear Patch Manager caches, layouts, tasks, or packages:

1. In the left pane of the Patch Manager console, click Administration and Reporting.
2. In the center pane, click General Settings.
3. Click Clear Caches and View Layouts.
4. In the Cache, Layouts and Tasks Maintenance window, click any of the options described previously.
5. **If you want Patch Manager to automatically delete the console work files for old tasks,** select Delete tasks older than, and then specify the number of days in the active field.
6. Click OK.

**Viewing Server Settings and Details**

Use the Patch Manager System Configuration > Patch Manager Servers node to view Patch Manager server settings and details. The views in this node can help configure, monitor, and troubleshoot the Patch Manager servers in your environment.

The Patch Manager System Configuration > Patch Manager Servers node contains a child node for two of the three Patch Manager server roles:

- Application Servers
- Management Servers

The parent Patch Manager Servers node contains details about the Automation server role on every Patch Manager server.

**The Patch Manager Servers Node**

When you select a Patch Manager server in the Patch Manager Servers node, the console displays the following tabs with information about that server in the lower-center pane.
Summary
Displays details about the server, such as its name, Patch Manager server roles, and management group.

Server File Details
Displays a list of all Patch Manager files on the server. Each line-item contains the attributes of the file, such as its location, modification date, version, and read-only status. For additional information about Patch Manager server files, see "The Patch Manager Server File System" on page 149.

Tasks Diagnostics
Displays details about the tasks currently running on the Automation role server. These details also appear on the Task Diagnostics tab of the Management Servers node, which can contain details for several Automation role servers.

Worker Process Jobs
Displays details about the jobs assigned to each worker process on the Automation role server.

Automation Server Settings
Displays the Patch Manager server settings that are specific to the Automation server role. For additional information about these settings, see "Automation Server Settings" on page 190.

Note: The Logging settings on this tab override the corresponding settings on both the Application Servers and Management Servers nodes.

The Application Servers Node
When you select a Patch Manager server in the Application Servers node, the console displays the following tabs with information about that server in the lower-center pane.

Summary
Displays details about the server, such as its name, Patch Manager server roles, and management group.

Sessions
Displays a list of active console connections to the selected Patch Manager server.

Task Diagnostics
Displays details about the tasks currently running on the Automation role server. These details also appear on the Task Diagnostics tab of the Management Servers node, which can contain details for several Application role servers.
Management and Application Server Monitoring

Lists all of the Patch Manager servers with the Management and/or Application server role. This view displays detailed information about the status of each server.

Application Server Settings

Displays the Patch Manager server settings that are specific to the Application server role. For additional information about these settings, see "Application Server Settings" on page 192.

The Management Servers Node

When you select a Patch Manager server in the Management Servers node, the console displays the following tabs with information about that server in the lower-center pane.

Summary

Displays details about the server, such as its name, Patch Manager server roles, and management group.

Automation Server Monitoring

Lists all of the Automation role servers assigned to the selected Management role server.

Task Diagnostics

Displays details about the tasks currently running on the Automation role server. These details also appear on the Task Diagnostics tab of the Patch Manager Servers and Application Servers nodes, which contain only details for the selected server role.

Management Server Settings

Displays the Patch Manager server settings that are specific to the Management server role. For additional information about these settings, see "Management Server Settings" on page 197.

The Patch Manager Server File System

The Patch Manager server file system consists of four sub-folders stored in the Patch Manager installation folder:

- Console
- Installers
- Server
- WMI Providers

Note: The default installation folder is %PROGRAMFILES%\SolarWinds\Patch Manager.
The following sub-folders in the Server folder contain useful files for maintaining the Patch Manager server:

- **archives**: Contains XML files for Task History items that Patch Manager has automatically purged from the Patch Manager database.
- **certs**: Contains a CER file for each of the certificates created by the PAS.
- **data**: Contains operational data for the Patch Manager server, including task definitions.
- **database**: Contains the SQL script files used to initialize the Patch Manager database. If Patch Manager installed a local instance of SQL Server Express, this folder also contains the SQL Server MDF and LDF files, which comprise the database.
- **exports**: The default storage location for all task result and scheduled report exports.
- **packages**: Contains the WMI redistributable, the WMI provider installer, and all content related to locally published packages.
- **scheduled**: Contains a repository of work files Patch Manager uses to execute scheduled tasks.
- **templates**: Contains all configuration templates used by the server-resident console sessions. On remote consoles, the templates are stored in %AppData%\Local\SolarWinds\Templates.

Additionally, the root of the Server folder contains all of the log files. These log files are in addition to the EminentWare event log Patch Manager maintains on the host operating system.
Wake on LAN

Wake on LAN (WOL) allows you to remotely power on WOL-enabled computers using a UDP broadcast on the local subnet. Patch Manager provides WOL functionality to use in conjunction with other scheduled tasks to patch computers that are not powered on. By scheduling the WOL, Update Management, and Shutdown or Reboot Computers tasks, you can power on remote computers, apply the updates you specify, and then shut down the computer when the update is finished.

Before you attempt to use this feature, ensure your target systems meet the requirements listed in the following section.

Requirements

Ensure your target systems meet the following requirements to use the WOL feature.

- The target systems must have a network card that supports WOL.
- The target systems must have WOL enabled. This is typically enabled in the BIOS.
- Patch Manager must be able to reach the target systems with a UDP broadcast. By default, many network devices do not forward UDP broadcasts, so a best practice is to perform the WOL function from the local subnet of the target system. You can achieve this by deploying secondary Patch Manager servers with the Automation role to any subnets that contain WOL targets.
- Patch Manager must know the MAC address of the target systems. To get systems' MAC addresses in Patch Manager, execute the Discovery task for each subnet that contains WOL targets.

Procedure

After you have confirmed your systems meet the requirements listed in the previous section, complete the following procedure to execute or schedule the Wake on Lan task in the Patch Manager console.

To complete the Wake on Lan task:

1. In the left pane of the Patch Manager console, select Administration and Reporting.
2. In the center pane, click Wake on Lan. You will specify target systems in a later step.
3. In the Wake on Lan Options window, enter the broadcast address for the subnet that contains the target systems. For example, if the system's IP address is 192.168.1.X, enter 192.168.1.255. If you want to send the broadcast to all subnets, enter 255.255.255.255.
4. If you have configured a non-standard port for WOL, enter the port number in the UDP Port field.
5. **If you have configured a Secure On password for the target systems**, enter the password in the Secure On Password field.

6. Click Wake Up.

7. In the Task Options Wizard window, specify the target system(s).

8. **If you want to schedule the task or specify export or notification options**, click Next and then complete the Scheduling and Notification Options page.

9. Click Finish.

10. On the Summary page, click Finish to schedule or execute the task according to your specifications.

## Advanced Deployment Scenarios

This appendix discusses several scenarios for deploying additional Patch Manager servers to help balance the load on any single server and connect to remote systems across a distributed network. This section addresses the following topics.

- [*Server Role Definitions*](#)
- [*Design Considerations*](#)
- [*Additional Automation Server Scenarios*](#)
- [*Additional Application and Management Server Scenarios*](#)

### Server Role Definitions

Patch Manager consists of three server roles:

- Application
- Management
- Automation

By default, all Patch Manager servers include the Automation role. When you deploy additional Patch Manager servers, you have the option of deploying just an Automation role server, or adding one or both of the other roles. The first Patch Manager server you deploy is the Primary Application Server (PAS), and it contains all three server roles.

**Notes:**

- SolarWinds licenses Patch Manager by the number of computers it manages. As such, there are no additional license costs associated with deploying additional Patch Manager servers.
- All Patch Manager servers, regardless of their role, require their own instance of SQL Server.
Application Server

Interfaces with the MMC-based administration console, Orion Platform web console, and ConfigMgr integrated console. Servers in this role also manage all communication between the console and the rest of the Patch Manager environment. Configure Application role servers to work with one or more servers in the Management role to specify what systems can be managed by what Patch Manager consoles.

Management Server

Maintains all inventory and discovery data for specific systems in the Patch Manager environment. Each Management role server hosts a management group defined by a collection of managed domains, workgroups, or WSUS servers. Deploy additional Management role servers to partition managed systems into defined security or network management boundaries.

Automation Server

Manages the local Patch Manager worker processes on each Patch Manager server. The worker processes perform the inventory and configuration management tasks and interface with the Windows Management Instrumentation (WMI) providers to collect data and supervise remote management capabilities. Deploy additional Automation role servers to support load balancing scenarios, fault tolerance scenarios, or isolated/access-controlled networks, such as a perimeter (DMZ) network.

Design Considerations

There are several things to consider when designing your Patch Manager deployment strategy for a distributed environment. The following sections address these considerations in detail and make recommendations when possible.

- Placing the Patch Manager Servers
- Placing the Patch Manager Consoles
- Configuring the Patch Manager Databases

Placing the Patch Manager Servers

Use multiple Patch Manager servers to facilitate load balancing, fault tolerance, or the needs imposed by geographic distribution or securities boundaries within an enterprise. When you deploy multiple Patch Manager servers, consider the following as you design your deployment strategy.

- Physical Location
- Enterprise Size
- **Wake-on-LAN**
- **Port Considerations and Bandwidth Restrictions**

**Physical Location**

In geographically distributed environments, deploy an additional Automation role server to each remote site. In this way, you enable these additional servers to facilitate client management and configuration processes on the local LAN of the target systems, instead of across the WAN.

Similarly, deploy additional Management role servers to each site to segregate management and data collection tasks as needed. Management role servers can also work in conjunction with the additional Application role servers to support remote system administrators.

**Enterprise Size**

In large environments with multiple subnets or large inventory requirements, deploy additional Application and/or Management role servers to optimize the Patch Manager environment. Use additional Application role servers to support multiple administration consoles. Use additional Management role servers to create smaller management groups for administration and reporting.

**Wake-on-LAN**

In environments that utilize Wake-on-LAN (WOL), deploy additional Automation role servers to facilitate WOL broadcasts for distributed systems. This helps administrators avoid the need to configure routers to support this functionality. It also increases the overall reliability by restricting WOL broadcasts to smaller, LAN-specific network domains.

**Port Considerations and Bandwidth Restrictions**

In environments with open-port or bandwidth concerns, deploy additional Automation and/or Management role servers to limit these requirements. Use additional Application role servers to limit WAN communication to a single port: 4092, the port used for server-to-server communication. With an Automation role server on each LAN, the other ports required in the Patch Manager environment only have to be open on each LAN.

Similarly, use additional Management role servers to limit the amount of traffic travelling across the WAN. With a Management role server on each LAN, inventory data only has to cross the WAN if a Patch Manager administrator runs a report for that LAN from a remote site.

**Placing the Patch Manager Consoles**

Use multiple Patch Manager consoles to connect to a single PAS from multiple locations, or to connect to distinct Secondary Application Servers (SAS) as needed. The following sections address these scenarios in more detail.
Multiple Consoles with a Single PAS

In environments that only require one Application role server, deploy additional Patch Manager consoles to allow console connections from more than one computer. For additional information about how to deploy additional Patch Manager consoles, see "Configuring Remote Administration Consoles" on page 106.

Multiple Consoles with Dedicated Servers

In environments that require multiple Application role servers, the Patch Manager installer installs an administration console on each additional server. If you need to connect to those servers from separate computers, deploy additional Patch Manager consoles and connect them to the appropriate Application role server as needed. For additional information, see "Configuring Remote Administration Consoles" on page 106.

Configuring the Patch Manager Databases

When you install Patch Manager servers, you have several options to configure the database. Patch Manager supports the following configuration options:

- SQL Server Express on the Patch Manager server
- SQL Server on the Patch Manager server
- SQL Server on a remote server

The purpose of the Patch Manager database is to store all consolidated data from WSUS Inventory, Managed Computer inventory, and Discovery tasks. To report on that data, the Patch Manager console pulls the data directly from the database. To ensure optimal performance, SolarWinds recommends the following:

- Use SQL Server 2005 Express Edition SP3 (included with the Patch Manager installer) for Patch Manager servers that require 4GB or less of storage space.
- Use SQL Server 2008 R2 Express Edition (available from Microsoft) for Patch Manager servers that require less than 10GB of storage space.
- Use a licensed version of SQL Server for Patch Manager servers that support multiple console users, inventory multiple WSUS servers, or execute simultaneous WMI-based tasks. These scenarios are all particularly heavy on reporting services.
- Use a remote database server for Patch Manager servers that reside on a WSUS or ConfigMgr server.
Deploy additional Management role Patch Manager servers to split storage requirements between each additional server.

**Additional Automation Server Scenarios**

Scenarios that warrant deploying additional Automation role servers are the most common when implementing Patch Manager in large or distributed networks. Patch Manager uses Automation role servers to initiate RPC/WMI connections to remote systems. When you deploy additional Automation role servers, Patch Manager can target more systems simultaneously. Furthermore, when you deploy Automation role servers closer to the remote systems they manage, the RPC/WMI connection has to travel a lesser distance.

**Automation Server Routing Rules**

Patch Manager uses Automation Server routing rules to manage what tasks go to what Automation role server. Furthermore, Automation Server routing rules define whether or not to assign a task to the default round-robin pool if the assigned server(s) is/are unavailable. In this way, Automation Server routing rules result in one of four general rule definitions:

- An absolute rule for a specific Automation role server
- A rule with a preferred Automation role server that relies on the default pool when needed
- An absolute rule for a specific pool of Automation role servers
- A rule with a pool of preferred Automation role servers that relies on the default pool when needed

In any case, you can define specific Worker Process Settings to limit the capacity of each Automation role server. For additional information, see "Automation Server Settings" on page 190.

To define Automation server routing rules:

1. In the left pane of the Patch Manager console, expand Patch Manager System Configuration > Management Groups.
2. Select the management group for which you want to configure the rule.
3. In the center pane, click the Automation Server Routing Rules tab.
4. In the Actions pane (right), select the action for the type of rule you want to create.
5. In the dialog that opens, specify the system(s) you want to target.
6. Complete the Select Automation Server(s) for routing rule and rule type dialog:
   a. Select one or more Automation role servers to assign to the rule.
   b. **If you want to restrict the rule to only the server(s) you selected**, select Absolute Rule.
   c. Click OK.
The following two scenarios illustrate a use case for additional Automation role servers, and then describe how to create the appropriate Automation server routing rules to address them.

**Scenario 1: Using an Automation Role Server to Manage a Dedicated Target**

A typical example of this scenario is using a dedicated Automation role server to manage tasks on the Patch Manager PAS. A Patch Manager server cannot perform certain actions on itself, such as a pre-execution reboot in an Update Management task. To address this, deploy an additional Automation role server to handle all tasks Patch Manager executes against itself.

Additional Automation Role Server to Manage the PAS

In other scenarios, SolarWinds recommends you deploy additional Automation role servers on dedicated systems. However, since the additional server in this scenario is only responsible for a single system, you have the option to deploy this server to a collocated system. Examples include the desktop system that has your Patch Manager console, or a WSUS server.

**Automation Server Routing Rule for Scenario 1**

In this scenario, create an Automation server routing rule that instructs Patch Manager to direct all tasks against the PAS to the additional Automation role server as long as it is online. If the additional server is offline, Patch Manager should direct the task to the PAS.

To create the rule for this scenario:

1. In the left pane of the Patch Manager console, expand Patch Manager System Configuration > Management Groups.
2. Select the management group for which you want to configure the rule.
3. In the center pane, click the Automation Server Routing Rules tab.
4. In the Actions pane (right), click Add Computer Rule.
5. In the Add Computer dialog, enter the details for the PAS.
6. Click Add.
7. Complete the Select Automation Server(s) for routing rule and rule type dialog:
   a. Select the additional Automation role server.
   b. Clear the Absolute Rule check box.
   c. Click OK.

Scenario 2: Using Additional Automation Role Servers for Geographically Distributed Networks

A typical example of this scenario is placing an additional Automation role server at each remote location in a geographically distributed network. Use this configuration with either a replica WSUS server at each remote location, or an always-on desktop system to host the Automation role server.

Additional Automation Role Servers for Geographically Distributed Networks

Another example is to use a separate Automation role server to offload work from the PAS. Use the following configuration if the PAS cannot complete tasks quickly enough due to the number of managed clients in the local network.
Automation Server Routing Rule for Scenario 2

In this scenario, use the Absolute Rule option to instruct Patch Manager to abandon the task if none of the Automation role servers you explicitly define for a location are online.

To create the rule for this scenario:

1. In the left pane of the Patch Manager console, expand Patch Manager System Configuration > Management Groups.
2. Select the management group for which you want to configure the rule.
3. In the center pane, click the Automation Server Routing Rules tab.
4. In the Actions pane (right), click Add Subnet Rule.
5. Complete the Add TCP/IP Subnets dialog:
   a. In the IP Address field, enter the IP address for the subnet.
   b. In the Subnet Mask menu, select the subnet mask.
   c. Modify the Starting Address or Ending Address fields as necessary.
   d. In the Description field, enter a description for the subnet.
   e. Click Add Subnet.
   f. Repeat these steps for any additional subnets.
6. Click OK.
7. Complete the Select Automation Server(s) for routing rule and rule type dialog:
   a. Select the additional Automation role servers.
   b. Select Absolute Rule.
   c. Click OK.
Additional Application and Management Server Scenarios

Scenarios that warrant deploying additional Application role servers relate directly to managing separate Patch Manager console connections. Use additional Application role servers to provide redundancy or additional load capacity for console connections, or to create isolated sandboxes in which a console user manages an environment. An Application role server has its own credentials, user profiles, and security roles.

Scenarios that warrant deploying additional Management role servers include any in which you want to create additional management groups. Since each Patch Manager server uses its own instance of SQL Server, creating multiple management groups means segregating Patch Manager data into multiple data stores. Examples of when this might be helpful include managing segments of an organization that have data sensitivity or confidentiality concerns, or reporting at a granular level, such as by department or site.

Scenario 3: Using an Application Role Server to Manage Console Connections

A typical example of this scenario is using multiple Application role servers to manage a large number of console connections. This example also serves to address High Availability (HA) requirements. For the HA scenario, deploy at least three Application role servers:

- The PAS, which Patch Manager does not use for console connections.
- At least two Secondary Application Servers (SAS), which can segregate groups of console users and/or back one another up in case of a failure.

Additional Application Role Servers for High Availability (HA)
This HA scenario scales to as many Application role servers as you require. If necessary, each console user could have a dedicated Application role server for their console connection.

**Scenario 4: Using a Management Role Server to Segregate Patch and Asset Data**

A typical example of this scenario is physically segregating patch data collected from the WSUS server from the asset inventory data collected from Managed Computer Inventory tasks. Deploy additional Management role servers to improve performance, or limit database space requirements to avoid the need for a licensed instance of SQL Server.

In the following example, assume the 10 GB database size limitation of SQL Server 2008 R2 Express Edition is not sufficient for both patch and asset data. To stay within that limit, deploy an additional Management role server to house the asset data from a domain inventory. This reserves the PAS for patch data from the WSUS server.

**Additional Management Role Server for Separate Databases**
Since Patch Manager physically segregates the data in this example, each database is significantly smaller than they would be if combined. In addition to limiting space requirements, this example also improves performance and enhances security by keeping unique data sets completely separate.

**Scenario 5: Using an Application and Management role server in a Testing Lab**

A typical example of this scenario is deploying functionally identical Patch Manager servers in a production and testing environment. Deploy an additional Patch Manager server with both the Application and Management roles to test packages before you deploy them. This architecture allows you to isolate the testing environment completely from the production environment.

In this example, define a separate management group for the resources in the test environment. These resources should include the subdomain or workgroup for the environment, along with a dedicated WSUS server.

Additional Application and Management Role Servers for Testing
A similar example would be to use the additional server for a special business or perimeter network (DMZ).
Appendix A

System Center Configuration Manager 2012 and 2012 R2 Procedures

The sections in this appendix address the procedural differences present in the Patch Manager extension of the System Center Configuration Manager (ConfigMgr) consoles. This material supplements the material discussed in the main portion of this guide.

This appendix contains the following sections:

- Integrating Patch Manager and ConfigMgr
- Publishing Third-party Updates
- Managing Published Third-party Updates

Integrating Patch Manager and ConfigMgr

There are two scenarios where you need to integrate Patch Manager and ConfigMgr. The first scenario is where you have ConfigMgr console installed in your server, and you install Patch Manager for the first time. The second scenario is where both ConfigMgr console and Patch Manager are installed in the same server but they are not integrated.

Before integration with Patch Manager, ConfigMgr2012 console looks like:

*ConfigMgr console before integration:*
Upon successful integration of Patch Manager and ConfigMgr, communication between the ConfigMgr console and ConfigMgr server does not change. Patch Manager console communicates with the WSUS servers directly, while ConfigMgr console communicates with the WSUS servers through the ConfigMgr server. Patch Manager does not make any changes to the ConfigMgr server. Patch Manager integrates with the new ribbon-style in the ConfigMgr console to extend its functionality.

**A typical deployment scenario for an integrated Patch Manager and ConfigMgr:**

![Diagram of Patch Manager and ConfigMgr integration](image)

To integrate Patch Manager and ConfigMgr when installing Patch Manager for the first time (scenario 1):

1. Log on as an administrator to the server on which you want to install Patch Manager.
2. Temporarily disable any antivirus software.
3. Run the SolarWinds Patch Manager installer. The installer prompts you to install any missing prerequisites.
4. Select **Patch Manager server components** and **Patch Manager administration console**, and then click **Next**.
5. In the Patch Manager Setup window, click **Next**.
6. Accept the End User License Agreement, and then click **Next**.
7. Click **Next** to use the default installation folder. Click **Browse** to choose a different folder.
8. If you are evaluating Patch Manager, select **Express Install - Recommended**, and then click **Next**. This selection installs WSUS servers and SQL Server Express. Follow the onscreen instructions to finalize your evaluation installation.

**Notes:**
- The Patch Manager Configuration Wizard installs and configures the IIS components, Microsoft Update Services, WMI Providers, Patch Manager Database, and Third-party Catalogs.
- Patch Manager configuration may take a few minutes.

9. Verify that **Run administration console after this wizard is finished** is selected, and then click **Finish**.

10. In the Product Features Selection window, select **WSUS Extension Pack** and **System Configuration Manager Extension Pack**, and then click **Continue**. Patch Manager continues with the post configuration, and then Patch Manager console launches after few minutes.

To integrate Patch Manager and ConfigMgr when both are installed but not integrated (scenario 2):

1. Log on as an administrator to the server on which you want to install Patch Manager
2. Temporarily disable any antivirus software.
4. Run the Patch Manager upgrade package.

**Notes:**
- The upgrade package may be the same version as your currently installed Patch Manager version.
- Patch Manager does not support direct upgrade from versions earlier than 1.80. For versions earlier than 1.80, upgrade to Patch Manager 2.0 first and then upgrade to the latest version of Patch Manager.
5. Accept the End User License Agreement, and then click **Next**. Patch Manager upgrade installation begins.

**Note:** In the Patch Manager Updates Installation Wizard window, make sure that you can see **Found the SCCM Console Director**.

6. Click **Next** and then click **Finish**.

**Verifying that Patch Manager is Integrated with ConfigMgr**

Before publishing third-party updates, you need to verify that Patch Manager is integrated with ConfigMgr successfully.

To verify that Patch Manager is integrated with ConfigMgr:
1. Open ConfigMgr console.

2. In the left pane, click **Software Library**.

3. In the Overview pane, check if 3rd Party Updates is available. If 3rd Party Updates is available, then integration is successful.

4. Expand **3rd Party Updates > Updates Overview**, and then select **All Updates**. The available updates for a time frame appear.

**Notes:**
- If you are not connected to the Patch Manager server, the Connect to Application Server window appears. Fill in with hostname, IP address, and port information. Click **Connect**.
- Retrieving of updates may take a long time, depending on the number of packages in the server.
Publishing Third-party Updates

If you configured third-party updates when you configured Patch Manager, the next step is to publish some packages to the WSUS server serving as your ConfigMgr software update point (SUP). For evaluation purposes, select one of the following procedures:

- Verifying SUP is Configured to Synchronize Locally Published Updates
- Publishing Third-party Updates without Direct Download URL
- Publishing Third-party Updates with Direct Download URL
- Deploying Third-party Updates
- Installing Third-party Updates in Client Machine

Verifying SUP is Configured to Synchronize Locally Published Updates

Complete this procedure to initially show the available third-party updates in WSUS/SUP servers. Also, complete this procedure after each time you publish third-party updates.

To verify that SUP is configured to synchronize locally published updates:

1. In the left pane of the ConfigMgr console, click the Administration heading.
2. Expand Site Configuration > Sites.
3. Click Configure Site Components in the ribbon, and select Software Update Point.
4. Make sure the Local Publisher with Locally published packages option is selected under the Products tab. You can also select Vendors of already published packages. Click OK.

Publishing Third-party Updates without Direct Download URL

Use the Package Download Assistant to download third-party update files. Then use the Publishing Wizard to copy the installation file and update definition to the WSUS/SUP server.

To publish third-party updates without direct download URL:

1. In the left pane of the ConfigMgr console, click Software Library.
2. Expand 3rd Party Updates > Updates Overview, and then select All Updates.
3. In the center pane, select the third-party update you want to publish.
4. In the ribbon, click **Publish**.

![Image of ribbon with Publish button highlighted]

5. In the Patch Manager Publishing wizard window, check the box next to the third-party update you want to publish. Click Next.

6. Download the source from the vendor website.

7. Return to the Package Download Assistant window, and then click Import Source.

8. Browse to the folder that contains the file you want to import, and then click Open.

**Note:** The file you select must match the update you selected in Step 3. The Package Download Assistant provides the correct filename by default, so you do not need to select the file after you browse to the appropriate folder.

9. Click **OK**.

10. Back in the Patch Manager Publishing Wizard window, select the package you want to publish, and click Next.

11. Click **Finish**. The package is now published in your SUP server.

After publishing third-party updates, you need to verify that updates are synchronized locally. For additional information, see "[Verifying SUP is Configured to Synchronize Locally Published Updates](#)" on page 168.

**Publishing Third-party Updates with Direct Download URL**

Use the Publishing Wizard to download third-party updates and copy the update definition to the SUP server.

To publish third-party updates with direct download URL:
1. In the left pane of the ConfigMgr console, click the **Software Library** heading.
2. Expand **3rd Party Updates > Updates Overview**, and then select **All Updates**.
3. In the center pane, select the third-party update you want to publish.
4. In the ribbon, click **Publish**.
5. Click **Next**.
6. After the publishing wizard downloads the package, select it, and then click **Next**.
7. Click **Finish**. The package is now published in your SUP server.

After publishing third-party updates, you need to verify that updates are synchronized locally. For additional information, see "[Verifying SUP is Configured to Synchronize Locally Published Updates](#)" on page 168.

**Deploying Third-party Updates**

Complete this procedure to deploy third-party updates.

To deploy updates:

1. In the left pane of the ConfigMgr console, click the **Software Library** heading.
2. Expand **Software Updates > All Software Updates**.
3. Click **Synchronize Software Updates**. This operation usually takes a couple of minutes depending on the number of updates. You can track progress using the **Wsyncmgr.log** file in CMTrace.
4. On the right side of the search bar click **Add Criteria**, then select **Vendor**. Confirm your choice by clicking the **Add** button.
5. In the search criteria, click the link following the search condition - **AND Vendor**. The list of available vendors is automatically populated.

![Image of search results with AND Vendor and Local Publisher selected](image)

6. Choose the vendor of the third-party update you have previously published and click the **Search** button.

**Note:** You can save the search criteria by clicking save Current Search under the Search tab in the ribbon.

7. Select previously published updates and click the **Deploy** button under the Home tab in the ribbon.

![Image of Deploy Software Updates Wizard](image)

8. On the first screen of **Deploy Software Updates Wizard**, complete the following fields:

   - **Deployment Name**
   - **Software Update Group**
   - **Collection**

![Image of specification for this deployment](image)

9. Click **Next**.
10. Keep the default Deployment Settings unless you are sure of the settings you want to change. Click Next.

11. In the Scheduling window of the wizard, set the Time based on to UTC and choose an Installation Deadline. Click Next.

12. In the User Experience window, define the user experience for your deployment and click Next. For example, the scenario in the screenshot below forces the installation if deadline is met and suppresses the restart on Servers.

13. In the Alerts window, set alert thresholds so you can monitor if compliance is below a defined percentage of machines when the deadline is met. If you do not need alert thresholds, keep the default settings and click Next.
14. In the Download Settings window under Deployment Option, choose Download software updates from distribution point and install and click Next.

15. On Deployment Package setting, choose Create a new deployment package and set Package source to your shared source folder on the SCCM server. Be sure the target folder exists otherwise the download will fail. Click Next.

16. Select Distribution Point and click Next.

17. In the Download Location window, choose Download software updates from a location on my network. Point to your WSUS Content folder on WSUS/SUP. Click Next.

18. In the Language Selection window, select the English language and click Next.

19. In the Summary window, review the settings and save the deployment as a template for later reuse. Click Next.

20. If the updates successfully download to the SCCM source folder and deploy to the distribution point, you will receive the message, The Deploy Software Update Wizard completed successfully. Click Close.

Installing Third-party Updates in Client Machine

Complete this procedure to check and install third-party updates in your client machine through Software Center.

To install third-party updates:
1. In your client machine, click **Start > Software Center**.

2. In the Available Software tab, select the third-party updates to install.

3. Click **Install Selected**.

   **Note:** When installation is successful, the **STATUS** in the Software Center window becomes **Installed**.

   ![Software Center with Installed status](image)

### Managing Published Third-party Updates

This section provides general instructions for managing third-party updates from the ConfigMgr console. For detailed examples of how to publish specific updates, see "Publishing Trial Updates" on page 51.

This chapter addresses the following procedures:

- **Creating a Third Party Updates View**
- **Managing Publishing Servers**
- **Importing and Exporting Catalogs**
- **Creating and Publishing Software Packages**
- **Managing Third-party Packages**

#### Creating a Third-party Updates View

One extension Patch Manager offers is the ability to publish, manage, and deploy third party updates from the Patch Manager server. In ConfigMgr, view your third-party updates by vendor using saved searches. Saved searches make it easy to differentiate between third-party update vendors.

To create a saved search in ConfigMgr for third-party updates:

1. In the left pane of the ConfigMgr console, click the Software Library heading.
2. Expand Overview > Software Updates > Update Repository, and then click All Software Updates.
3. In the ribbon, click the Search tab.
4. Click Add Criteria, and then select Vendor.
5. Click the hyperlink under the search bar, and then enter the vendor's name.
6. Click Search.
7. In the ribbon, click Save Current Search.
8. Enter the vendor's name as the name for the saved search.
9. Click OK.

Access saved searches in the Saved Searches menu on the Search tab.

**Managing Publishing Servers**

Use the Server Publishing Verification Wizard to determine whether a WSUS server (the ConfigMgr SUP) has a publishing certificate. If it does, the wizard also determines the status of the publishing certificate with respect to the other server resources associated with that WSUS server.

Note: The Server Publishing Verification Wizard is not currently available in the ConfigMgr console. If needed, complete the wizard in the MMC-based Patch Manager console. For additional information, see "Managing Publishing Servers" on page 69.

**Importing and Exporting Catalogs**

Import and export package catalogs to move catalogs amongst Patch Manager servers. This section addresses the following procedures:

- **Importing Catalogs**
- **Exporting Catalogs**

**Importing Catalogs**

Use the Import Catalog Wizard to import selected packages or an entire catalog from a portable catalog (.cab) file created by another Patch Manager server, System Center Updates Publisher, or any other product that complies with the Microsoft package and catalog specifications.

To import packages from a portable catalog file:

1. In the left pane of the ConfigMgr console, click the Software Library heading.
2. Expand 3rd Party Updates > Updates Overview, and then select All Updates.
3. In the ribbon, click Import Catalog.
4. On the Select Catalog File screen, browse to or enter the complete path for the catalog (.cab) file you want to import.
5. Click Next.
6. On the Import Details screen, select the package(s) you want to import.
7. Click Next.
8. Review the import results, and then click Finish.
Exporting Catalogs

Use the Export Catalog Wizard to export one or more packages into a portable catalog (.cab) file that can be imported into another Patch Manager server, System Center Updates Publisher, or any other product that complies with the Microsoft package and catalog specifications.

Use the Export Catalog Wizard to do either of the following:

- Export the entire library of packages into a catalog file.
- Export one or more selected packages into a catalog file.

The following define the export options in this wizard.

**Include downloaded package content when exporting**

Select this check box if you want to export all installers and other files you have downloaded for the packages you are exporting. If you select this option, use the Additional Files dialog to select files on a per-file basis.

**Export the selected software packages to a cabinet file that can be imported by other publishers**

Select this option if you selected one or more packages to export prior to launching the wizard.

**Export all software packages to a cabinet file that can be imported by other publishers**

Select this option if you want to export all packages in your library.

**Export File Name**

Enter or browse to the file you want to use for the export. This field requires a fully qualified file path.

To export packages to a portable catalog file:

1. In the left pane of the ConfigMgr console, click the Software Library heading.
2. Expand 3rd Party Updates > Updates Overview, and then select All Updates.
3. Select one or more packages in the center pane. The wizard lets you export specific packages based on your selection, or all packages regardless of your selection. Use Ctrl+click to select multiple packages.
4. In the ribbon, click Export Catalog.
5. Complete the Export Options screen as described previously.
6. Click Next.
7. Review the export results, and then click Finish.
Creating and Publishing Software Packages

Use Patch Manager to create custom software packages to publish to WSUS. Publish custom packages or packages from the SolarWinds third-party updates library so WSUS can deploy them to the applicable clients. This section addresses the following procedures:

- [Creating Software Packages](#)
- [Managing Software Package Rule sets](#)
- [Publishing Custom Software Packages](#)

Creating Software Packages

The Package Wizard is a guided interface for creating or editing a package definition. A package definition is an XML file that defines the attributes and behavior of an update package. Use the Package Wizard to view or define the following:

- Package metadata
- Prerequisite rules
- Update source
- Applicability rules
- Installed rules

To open the Package Wizard:

1. In the left pane of the ConfigMgr console, click the Software Library heading, and then expand 3rd Party Updates > Updates Overview.
   **If you want to create a new package:**
   a. Select All Updates.
   b. In the ribbon, click New.
   **If you want to view a package's details:**
   a. Select the container that contains the package you want to view.
   b. In the center pane, select the package you want to view.
   c. In the ribbon, click Edit.

4. Complete the Patch Manager Package Wizard as described in "Completing the Package Wizard" on page 72.
Managing Software Package Rulesets

WSUS uses software publishing rulesets to determine whether or not to evaluate a client for the packages it deploys, and then determine whether applicable clients need the update. The following sections describe each type of software publishing ruleset and provide a corresponding example.

For additional information about these rulesets, see the Microsoft article, "Updates Publisher Rules," http://technet.microsoft.com/en-us/library/bb531100.aspx.

Note: The Rule Editor is the same regardless of the type of rule. Furthermore, it is the same whether you launch it from the Package Wizard or elsewhere in the ConfigMgr console.

To open the Rule Editor from the ConfigMgr console:

1. In the left pane of the ConfigMgr console, click the Software Library heading, and then expand 3rd Party Updates.
2. Select Rules.
3. If you want to create a new rule, click New Rule in the ribbon.
4. If you want to edit an existing rule, select the rule you want to edit, and then click Properties in the ribbon.

For additional information about software package rulesets, see the following sections in the main portion of this guide:

- Prerequisite Ruleset
- Applicability Ruleset
- Installed Ruleset

Publishing Software Packages

Use the Patch Manager Publishing Wizard to publish one or more packages to your ConfigMgr SUP. When publishing packages, you have the option to publish any of the following:

- Entire packages, which include all metadata and installers.
- Metadata-only packages, which you can use to determine whether or not a package is installed or needed on target computers.
- Revision-only packages, which update an existing package's metadata, but not its installation file.

Complete the following procedure to publish packages to the SUP/WSUS server to be deployed to applicable clients.

The wizard in this procedure provides the following additional options:
Verify WSUS version compatibility and required signing certificate is distributed

Checks the versions and certificates throughout the publishing environment to verify publishing will be successful. WSUS requires that all components in the publishing environment are running the same WSUS version and have the same publishing certificate installed. We recommend you use this option to verify these requirements prior to large publishing jobs to avoid wasted publishing time.

Re-sign existing selected packages

Re-signs the selected packages with the current publishing certificate. Use this option when republishing packages that were previously signed with an earlier publishing certificate.

Delete package if it exists (select this if binaries have changed)

Replaces the existing binary files for the selected packages with new ones. Most often, you will accomplish this goal by publishing an entirely new package, but this option allows you to reuse an existing package definition.

Re-download packages that have already been downloaded

Downloads the binary content for all packages, even if the content is already on the SolarWinds Patch Manager server. Use this option to ensure the content you publish to the WSUS server is exactly the same as the content available from the vendor's update publishing site.

To publish packages to a SUP/WSUS server:

1. In the left pane of the ConfigMgr console, click the Software Library heading.
2. Expand 3rd Party Updates > Updates Overview, and then select All Updates.
3. In the center pane, select a single update or update container.
4. In the ribbon, click Publish.
5. On the Packages to Publish screen, select the WSUS server to which you want to publish the packages.

Note: This wizard cannot publish packages to replica servers.

6. Select one of the following options as your initial selection method:
   - Publish selected packages to the WSUS server: Select this option to start with only the packages you selected before launching the wizard.
   - Publish all packages to the WSUS server: Select this option to start with all available packages selected. You can clear or modify these selections in the following step.

7. In the pane that lists the available packages, select the check box next to the packages you want to publish. Clear the check box next to the packages you do not want to publish.
8. In the Content column for each package you selected, specify whether you want to publish the Full, Metadata Only, or Revision Only version.

9. Above the package selection pane, select any of the additional options described previously.

10. Click Next.

If you need to download any additional content:

   a. **If any packages do not include direct download links**, use Package Download Assistant to download and import the content. For additional information, see "Using Package Download Assistant" on page 81.

   b. After the wizard finishes downloading the required content, select each of the packages you want to publish.

   c. Click Next.

12. Review the publishing results, and then click Finish.

Managing Third-party Packages

After you have created a package in Patch Manager, select it in the Patch Manager console to view useful information about it in the details pane. The topics in this section address the following procedures.

- Viewing Package Details
- Verifying Package Integrity
- Checking a Package's Publication Status

Viewing Package Details

When you select a package in the All Updates node of the ConfigMgr console, Patch Manager displays detailed information about the package in the following tabs.
Package Details
Similar to the Update Details tab for WSUS updates. Displays the package description and metadata.

Prerequisite Rules
Displays the prerequisite rules for the package just as they appear in the Package Wizard.

Applicability Rules
Displays the applicability rules for the package just as they appear in the Package Wizard.

Installed Rules
Displays the installed rules for the package just as they appear in the Package Wizard.

Verifying Package Integrity
Use the Package Integrity Verification task to verify the content of a package before you publish it. This package compares the contents you have previously downloaded for the package to what is currently available from the vendor.

This task does the following:

- It calculates the SHA-1 hash of the downloaded file and compares it to the SHA-1 hash that was calculated when the package was created.
- It identifies the quantity of any extra files that should be included as defined by the Include Additional Files option, and the quantity of any files that are missing based on the number of files that are defined.
- It provides a Repair option to remediate any repairable conditions.

To check the integrity of one or more downloaded packages:

1. Select one or more packages that have already been downloaded.
2. In the ribbon, click Integrity Check.
3. If the wizard displays a package without a green check mark in the left column, click Repair to repair the package.
4. Click Close to exit the window.

Checking a Package's Publication Status
Use the Check Publication Status task to determine whether or not a package has been published to a WSUS server.

To check the publication status of one or more packages:
1. Select the packages you wish to check.
2. In the ribbon, click Publication Status.
3. On the Package Publication Status Wizard, select the update servers you want to check against.
4. Click Next.
5. Review the results of the check, and then click Close to exit the wizard.

**Administrating WSUS Using Patch Manager**

Use the 3rd Party Updates > Administration > Update Servers node in the ConfigMgr console to manage your SUP/WSUS server just like you would in the native WSUS console. This node lists each WSUS server you have registered with Patch Manager in the center pane. Select a WSUS server to expose WSUS management options in the ribbon.

The following sections discuss common WSUS administration tasks and how to execute them from the ConfigMgr console.

- [Synchronizing WSUS Servers](#)
- [Cleaning Up WSUS Servers](#)
- [Repairing and Maintaining the Windows Update Agent](#)
- [Administrating Windows Update Agent Local Policy](#)

**Synchronizing WSUS Servers**

Use the Synchronize Server task to synchronize the selected WSUS server with its upstream server. Review a server's synchronization information on the Server Settings tab of the 3rd Party Updates > Administration > Update Servers > yourWsusServer view.

SolarWinds recommends that you schedule regular synchronization tasks for your WSUS servers to ensure they have the latest updates at all times. Complete the following procedure to schedule or execute a synchronization task from the ConfigMgr console.

To schedule or execute a synchronization task:

1. In the left pane of the ConfigMgr console, expand 3rd Party Updates > Administration, and then select Update Servers.
2. In the center pane, select the WSUS server you want to synchronize.
3. In the ribbon, click Synchronize Server.
4. Complete the Task Options Wizard to schedule and/or execute the synchronization task for the selected WSUS server. For additional information, see "[The Task Options Wizard](#)" on page 62.
Cleaning Up WSUS Servers

Use the Server Cleanup Wizard task to clean up the selected WSUS server. It deletes expired updates and old revisions of updates from the server. This task in the Patch Manager console has two advantages over the native cleanup task in the WSUS console:

- The Patch Manager task allows you to configure a threshold for the number of days WSUS keeps non-reporting computers in the console.
- You can schedule the Patch Manager task to run regularly, which SolarWinds recommends.

The Server Cleanup Wizard task consists of five distinct actions, which you can run simultaneously or individually on the selected WSUS server:

**Unused updates and update revisions**

The system deletes expired updates that have remained unapproved for three months or longer. Also deletes unapproved, old revisions of updates. The system deletes revisions that have remained unapproved for 30 days or longer.

**Computers not contacting the server**

Deletes computers that have not contacted the Update Server within the computer deletion threshold.

**Configure the computer deletion threshold**

Number of days that the computer must remain out of contact with the server before the system deletes it.

**Unneeded update files**

Deletes update files that other update files and downstream servers do not require to perform their duties. Generally, these updates have been declined.

**Expired Updates**

Declines unapproved, expired updates from Microsoft.

**Superceded Updates**

Declines unapproved updates that have been superseded with approved updates. The system declines superseded updates that have remained unapproved for 30 days or longer.

To schedule or execute a WSUS server cleanup task:

1. In the left pane of the ConfigMgr console, expand 3rd Party Updates > Administration, and then select Update Servers.
2. In the center pane, select the WSUS server you want to clean up.
3. In the ribbon, click Server Cleanup Wizard.
4. Select one or more of cleanup options, as described previously.
5. Click OK.
6. Complete the Task Options Wizard to schedule and/or execute the cleanup task for the selected WSUS server. For additional information, see "The Task Options Wizard" on page 62.

**Repairing and Maintaining the Windows Update Agent**

Use the Windows Update Agent Maintenance and Repair task to execute diagnostic and remediation functions on remote Windows Update Agents. In a standard WSUS environment, these functions are only available at the command line, and can only be executed on one system at a time.

To launch the Windows Update Agent Maintenance and Repair task from the ConfigMgr console:

1. In the Assets and Compliance workspace, select the computer you want to repair.
2. In the ribbon, click RealTime Computer Info.
3. In the Computer Explorer window, click Repair Windows Update Agent on the Actions tab.
4. Select the applicable options as defined in "Repairing and Maintaining the Windows Update Agent" on page 100.
5. Click OK.
6. Complete the Task Options Wizard to schedule and/or execute the task for one or more remote systems. For additional information, see "The Task Options Wizard" on page 62.

**Administrating Windows Update Agent Local Policy**

Use the Windows Update Local Policy Management task to manage the Windows Update Agent policy using Local Policy on one or more remote systems. This is particularly useful for non-Active-Directory environments, or when you prefer not to use Group Policy.


Note: This task requires WMI connectivity with the remote system(s). For additional information about enabling WMI connectivity between the Patch Manager server and remote systems, see "Managing Client WMI Connectivity" on page 122.

To manage Windows Update Agent policy on a remote system:

1. In the Assets and Compliance workspace, select the computer you want to update.
2. In the ribbon, click RealTime Computer Info.
4. In the Windows Update Local Policy Settings window, click the checkbox next to each setting to toggle between Not Configured, Disabled, and Enabled states.

5. After you have configured the desired settings, click Save.

6. In the Windows Update Local Policy Settings Template window, enter a name for the new template, and then click Save.

7. If you want to load an existing template, click Load, and then browse to the template you want to load.

8. Click OK.

9. Complete the Task Options Wizard to schedule and/or execute the task for one or more remote systems. For additional information, see "The Task Options Wizard" on page 62.

**Provisioning the WMI Providers**

During the initial configuration steps, the Patch Manager installer provides the option to automatically provision WMI Providers to all managed clients as they are needed. If you opted out of automatic provisioning or otherwise want to deploy WMI Providers manually, complete the following procedure.

To create a task to deploy WMI Providers to managed computers:

1. In the Assets and Compliance workspace, select the computer you want to update.
2. In the ribbon, click RealTime Computer Info.
3. In the Computer Explorer window, click Check Computer Access on the Actions tab.
4. In the Computer Access Management window, select Install the WMI Providers if not already installed, and then click OK.
5. Complete the Task Options Wizard to specify the target systems and schedule and/or execute the task. For additional information, see "The Task Options Wizard" on page 62.

**Fixing WMI Connectivity Issues**

If you recognize an issue with WMI connectivity to a remote system, use the Check Computer Access task to help resolve the issue. This launches the same dialog you use to provision the WMI providers to remote systems.

To complete the Check and Manage Computer Access task:

1. In the Assets and Compliance workspace, select the computer you want to update.
2. In the ribbon, click RealTime Computer Info.
3. In the Computer Explorer window, click Check Computer Access on the Actions tab.
4. In the Computer Access Management window, select the appropriate options as described in the following sections.

5. Click OK.

6. Complete the Task Options Wizard to specify the target systems and schedule and/or execute the task. For additional information, see "The Task Options Wizard" on page 62.

The following sections provide additional information related to this task:

- SolarWinds WMI Providers Actions
- Additional Options
- Additional Requirement for Windows XP

**SolarWinds WMI Providers Actions**

The first section of the Computer Access Management window addresses options to install, reinstall, or uninstall the SolarWinds WMI Providers. Choose one of the following:

**Check if WMI Providers are installed**

Checks for the WMI Providers on the remote system. View results from this check in the Patch Manager Task History, or configure the task to email you the results.

**Install the WMI Providers if not already installed**

Installs the WMI Providers if needed. This option also allows you to reinstall the WMI Providers if necessary.

**Uninstall the WMI Providers**

Uninstalls the WMI Providers from the remote system.

**Additional Options**

The remainder of the Computer Access Management window addresses options to configure remote systems to allow WMI connections. Select any combination of the following:

**Enable DCOM if disabled**

Enables Distributed COM (DCOM) on the remote system. This is a requirement for Patch Manager to use WMI to connect to remote systems.

**Configure DCOM permissions to include 'Administrators' group if needed**

Modifies DCOM permissions to allow users from the Administrators group in Windows. Patch Manager requires local Administrator permissions on remote systems to run the WMI Providers.
Enable the 'Remote Administration' firewall rule (Windows Firewall/Advanced Firewall only)

Enables the Remote Administration firewall ruleset in Windows Firewall. If you are using a third party firewall solution, administer the necessary rules in your firewall through other means.

Create ADMIN$ share if missing

Creates the ADMIN$ share on Windows 2000 systems. Systems running Windows XP and later create the ADMIN$ share automatically on startup. However, it is possible to delete this share in Windows 2000.

Enable Windows Installer service if disabled

Re-enables the Windows Installer service on the remote system. Patch Manager requires this service to install the WMI Providers.

Enable MSI Logging

Enables MSI logging on the remote system. This option is selected by default, but you can clear it if you do not want MSI logging turned on.

Additional Requirement for Windows XP

If the systems you are troubleshooting are running Windows XP, note the following additional requirement when those systems are members of a workgroup.

To configure Windows XP Workgroup clients to allow WMI connections:

1. On the affected system, open Registry Editor (regedit.exe).
2. Expand HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control.
3. Select Lsa.
4. Change the value for the forceguest DWORD to 0:
   a. In the right pane, select forceguest.
   b. Click the Edit menu, and then select Modify.
   c. Enter 0 into the text box.
   d. Click OK.

For additional information about this requirement, see the Microsoft knowledge base article, "How to Set Security in Windows XP Professional That Is Installed in a Workgroup," http://support.microsoft.com/?kbid=290403.

Verifying WMI Connectivity

After you have WMI connectivity configured for your environment, use the Inventory – verify access only Managed Computer Inventory option to verify WMI connectivity with your remote systems.
Note: For ConfigMgr instructions see Appendix A: "System Center Configuration Manager 2012 and 2012 R2 Procedures" on page 164.

To verify WMI connectivity with your remote systems:

1. In the Assets and Compliance workspace, select the computer you want to update.
2. In the ribbon, click RealTime Computer Info.
3. In the Computer Explorer window, click Quick Inventory on the Actions tab.
4. On the Inventory Options window, select Inventory – verify access only.
5. Click OK.
6. Complete the Task Options Wizard to specify the target systems and schedule and/or execute the task. For additional information, see "The Task Options Wizard" on page 62.

View results from this check in the Patch Manager Task History, or configure the task to email you the results.
Appendix B

Patch Manager Server Settings

Configure Patch Manager server settings on the following tabs in the Patch Manager System Configuration > Patch Manager Servers node in the Patch Manager console:

- Automation Server Settings
- Application Server Settings
- Management Server Settings

Automation Server Settings

Since every Patch Manager server includes the Automation server role, this settings tab is at the root of the Patch Manager Servers node. The following settings are available, sorted by category.

Event Logging

Settings in this category control how the Automation role server logs to the Windows Event Log on the Patch Manager server. Enable or disable the following settings to define what the Automation role server logs.

- Automation Server Security Audit Failure Event Logging Enabled
- Automation Server Security Audit Success Event Logging Enabled
- Automation Server Error Event Logging Enabled
- Automation Server Information Event Logging Enabled
- Automation Server Warning Event Logging Enabled

Note: Settings in this category on the Automation Server Settings tab overwrite the corresponding settings on both the Application Server Settings and Management Server Settings tabs.

General

Settings in this category define general options for the Application server role.

Automation Server Enabled

 Enables the Automation server role on the selected Patch Manager server.

Logging

Settings in this category define how Patch Manager generates detailed debug logging. By default, logging is turned on. SolarWinds recommends you only enable this level of logging when engaging in advanced troubleshooting and/or working with SolarWinds Technical Support.
Logging

Enables debug logging. Patch Manager writes these logs to the %programdata%\Solarwinds\PM\Log folder. Logging affects server performance and has potential to consume significant disk space if you leave it enabled for an extended period.

Logging Level

Defines the logging level when logging is enabled. Select one of the following levels:

**Note:** The default logging level is "Error."

Level 1

Normal logging: Enables logging for any program code object that is configured to provide normal logging.

Level 2

Verbose logging only: Enables logging for any program code object that is configured to provide verbose logging.

Level 3

Normal and verbose logging: Enables both normal and verbose logging for all applicable program code objects.

Logging Output

Defines the output type when logging is enabled. Select one of the following output types:

Output 1

Output file: Writes debug logs to the logging folder with a log.txt extension.

Output 2

Debug stream: Writes debug logs to a debug stream. Use this option when using a debugger, such as Microsoft's DebugView utility.

Output 3

Hybrid output: Writes debug logs to both an output file and debug stream.

Worker Process Settings

Settings in this category define how Patch Manager servers in the Automation role execute their worker processes. Worker processes manage tasks assigned to an Automation role server. Whenever possible, they execute immediately on demand. The following settings define when to queue worker processes if Patch Manager requests several tasks at the same time.
**Maximum Worker Processes**

Specifies the maximum number of worker processes the Automation role server can run at once. Select a value from 1 to 8.

**Maximum Thread Pool Size per Worker Process**

Specifies the maximum number of threads each worker process can execute at once. Select a value from 2 to 128.

**Enable Worker Process Memory Usage Quota**

Enables a memory usage quota for the worker processes.

**Shutdown Worker Process after being idle for (in minutes)**

Defines the "idle-out" time for the worker processes. Specify the number of minutes Patch Manager should wait before shutting down an idle worker process. Select a value from 1 to 60.

**Worker Process Memory Usage Quota**

Defines the memory usage limit, or quota, for the worker processes. Specify the number of megabytes (MB) you want to allocate to the worker processes. Select a value from 1 to 500.

**Maximum retry count for Worker Process Job**

Defines the maximum number of times a worker process will retry a failed job. Select a value from 1 to 10.

**Worker Process startup time limit (in seconds)**

Defines the maximum startup time for the worker processes. Specify the number of seconds Patch Manager should wait before terminating a worker process that does not start immediately. Select a value from 10 to 120.

**Application Server Settings**

This settings tab only appears for Patch Manager servers in the Application server role. It appears in the Application Servers child node under Patch Manager System Configuration > Patch Manager Servers.

**Application Server Communication Settings**

Settings in this category control how the Application role server handles communication failures with remote systems.

**Number of retries to attempt on communication failure**

Specifies the number of times the Application role server will attempt to communicate with a remote system if a task is unable to connect. Select a value from 0 to 10.
Retry delay on communications failure (in seconds)

Defines the retry interval handling communication failures. Specify the number of seconds Patch Manager should wait between retry attempts. Select a value from 0 to 60.

Application Server Job Pool Settings

Settings in this category control the number of concurrent jobs Patch Manager allows.

Maximun Concurrent Jobs

Specifies the total number of jobs that can run at the same time across all Management role servers. Each Management role server also has this setting to limit concurrent jobs by server. Select a value from 4 to 16.

Email Configuration

Settings in this category define the email and Simple Mail Transfer Protocol (SMTP) server settings for email notifications Patch Manager sends from the Application role server.

Email Configuration: Sender e-mail Address

Defines the sender e-mail address Patch Manager should use when sending email notifications from the Application role server.

Email Configuration: Sender e-mail Name

Defines the sender e-mail name Patch Manager should use when sending email notifications from the Application role server.

Email Configuration: SMTP Server Name (Outgoing)

Defines the SMTP server Patch Manager should use when sending email notifications from the Application role server.

Email Configuration: SMTP Server Port Number

Defines the SMTP port number Patch Manager should use when sending email notifications from the Application role server.

Email Configuration: SMTP Server requires authentication

Defines whether the SMTP server requires authentication to send email. Select Enabled or Disabled.

Email Configuration: SMTP Server logon user password

Defines the user password Patch Manager should use when sending email notifications from the Application role server using an authenticated mail server.
**Email Configuration: SMTP Server uses encrypted SSL connection**

Defines whether the SMTP server uses an encrypted Secure Socket Layer (SSL) connection. Select Enabled or Disabled.

**Email Configuration: SMTP Server uses encrypted TLS connection**

Defines whether the SMTP server uses an encrypted Transport Layer Security (TLS) connection. Select Enabled or Disabled.

**Email Configuration: SMTP Server logon user name**

Defines the user logon name Patch Manager should use when sending email notifications from the Application role server using an authenticated mail server.

**Email Configuration: SMTP Server user logon domain**

Defines the user domain Patch Manager should use when sending email notifications from the Application role server using an authenticated mail server.

**Event Logging**

Settings in this category control how the Application role server logs to the Windows Event Log on the Patch Manager server. Enable or disable the following settings to define what the Application role server logs.

- Application Server Security Audit Failure Event Logging Enabled
- Application Server Security Audit Success Event Logging Enabled
- Application Server Error Event Logging Enabled
- Application Server Information Event Logging Enabled
- Application Server Warning Event Logging Enabled

Note: Settings in this category on the Automation Server Settings tab overwrite the corresponding settings on both the Application Server Settings and Management Server Settings tabs.

**General**

Settings in this category define general options for the Application server role.

**Automatically archive Task History Days**

Defines the retention period for old Task History items. Specify the number of days Patch Manager should wait before deleting old Task History items. Select an integer value.

**Automatically archive Task History Enabled**

Enables Patch Manager to delete old Task History items after a specific period of time.
Patch Manager Update

Settings in this category define when and how the Application role server connects to and synchronizes with the SolarWinds third party updates library.

Automatically Purge Synchronization History

 Enables Patch Manager to automatically delete synchronization history items after a specific period of time.

Automatically Purge Synchronization History Threshold in Days

 Defines the purge threshold for synchronization history items. Specify the number of days Patch Manager should wait before deleting synchronization history items. Select an integer value.

Catalog Settings

 Specifies the third party updates library with which the Application role server should synchronize. This setting consists of a complex XML value. To modify this setting, use the Synchronization Settings action in the Software Publishing node.

Enabled Patch Manager Update Notification emails

 Enables the Application role server to send email notifications when it synchronizes new, expired, or revised updates.

Patch Manager Update Notification recipients

 Defines the recipients for synchronization email notifications. Specify email addresses for the recipient(s). Separate multiple email addresses with a comma. Do not use spaces.

Frequency in hours of how often to synchronize

 Defines the synchronization frequency for the Application role server. Specify the frequency, in hours, with which the server should synchronize with the SolarWinds third party updates library. Select an integer value.

Proxy Port Number

 Defines the port number the Application role server should use when connecting to the Internet using a proxy server.

Proxy Domain

 Defines the user logon domain the Application role server should use when connecting to the Internet using an authenticated proxy.
**Proxy User Name**

Defines the user logon name the Application role server should use when connecting to the Internet using an authenticated proxy.

**Proxy Server Name**

Defines the proxy server the Application role server should use when connecting to the Internet.

**Subscription**

Specifies the third party updates catalogs to which the Application role server is subscribed. This setting consists of a complex XML value. To modify this setting, use the Synchronization Settings action in the Software Publishing node.

**Synchronization Start Time**

Defines the time at which the Application role server first synchronizes with the SolarWinds third party updates library. Specify the time for the first update by selecting the number of minutes after midnight you want it to start.

**Synchronization Type**

Enables the Application role server to automatically synchronize with the SolarWinds third party updates library.

**Use Credentials for Proxy**

Defines whether the proxy server requires authentication to connect to the Internet. Select Enabled or Disabled.

**Use Proxy**

Defines whether the Application role server uses a proxy to access the Internet. Select Enabled or Disabled.

**Username**

Deprecated. This setting only applies to version 1.71 and earlier.

**Scheduled Task Scheduler**

Settings in this category define how the Application role server handles scheduled tasks.

**Maximum concurrent executing schedule tasks**

Specifies the total number of scheduled tasks the Application role server can execute at once. Select a value from 1 and 50.
Management Server Settings

This settings tab only appears for Patch Manager servers in the Management server role. It appears in the Management Servers child node under Patch Manager System Configuration > Patch Manager Servers.

Note: The settings on this tab mimic the corresponding settings on the Application Server Settings tab. Management server settings always override settings on the Application role server.

Event Logging

Settings in this category control how the Management role server logs to the Windows Event Log on the Patch Manager server. Enable or disable the following settings to define what the Management role server logs.

- Management Server Security Audit Failure Event Logging Enabled
- Management Server Security Audit Success Event Logging Enabled
- Management Server Error Event Logging Enabled
- Management Server Information Event Logging Enabled
- Management Server Warning Event Logging Enabled

Note: Settings in this category on the Automation Server Settings tab overwrite the corresponding settings on both the Application Server Settings and Management Server Settings tabs.

Application Server Communication Settings

Settings in this category control how the Management role server handles communication failures with remote systems.

Number of retries on communication failure

Specifies the number of times Patch Manager will attempt to communicate with a remote system if a task is unable to connect. Select a value from 0 to 10.

Retry delay on communications failure (in seconds)

Defines the retry interval handling communication failures. Specify the number of seconds Patch Manager should wait between retry attempts. Select a value from 0 to 60.

Management Server Job Pool Settings

Settings in this category control the number of concurrent jobs the Management role server allows.
**Maximum Concurrent Jobs**

Specifies the total number of jobs that can run at the same time across the Management role server. Each Application role server also has this setting to limit concurrent jobs across all Management role servers. Select a value from 4 to 16.
Appendix C

Patch Manager Web Console User Settings

The following define each user setting in the Patch Manager web console.

**Account Enabled**

Enables the user to log into the Patch Manager web console. Select Yes or No.

**Account Expires**

Specifies the date after which the user cannot log into the Patch Manager web console. Enter or select an expiry date, or enter Never if the account should not expire.

**Disable Session Timeout**

Allows the user to stay logged into the Patch Manager web console indefinitely. Select Yes or No.

**Allow Administrator Rights**

Allows the user to add or edit other user accounts and reset passwords. Select Yes or No.

**Allow Node Management Rights**

Allows the user to manage Orion nodes. In Orion web consoles with only the Patch Manager module, this setting is irrelevant. If applicable, select Yes or No.

**Allow Account to Customize Views**

Allows the user to customize the views they see when they log into the Patch Manager web console. When a user customizes a view, the changes are global. That is, all users with the same view see the changes. Select Yes or No.

**Allow Account to Clear Events, Acknowledge Alerts and Syslogs**

Allows the user to clear and acknowledge Orion-generated events, alerts, and syslogs in the web console. In Orion web consoles with only the Patch Manager module, this setting is negligible. If applicable, select Yes or No.

**Allow Browser Integration**

Allows the user to use client browser tools with information provided in the web console. Select Yes or No.
Alert Sound

Enables audible alerts in the Orion web console. In Orion web consoles with only the Patch Manager module, this setting is negligible. If applicable, select a .wav file to use for alerts. The web console populates this list from the folder, %SystemDrive%\Inetpub\SolarWinds\NetPerfMon\Sounds.

Number of items in the breadcrumb list

Specifies the number of items the web console displays in the breadcrumb drop-down lists. If set to 0, the web console displays all items. Enter the number of items to display.

Account Limitations

Specifies the network devices the user can view. For example, limit the user to see only devices in a single location. In Orion web consoles with only the Patch Manager module, this setting is irrelevant. Refer to the Administrator Guide for your Orion Platform product for additional information.

HomeTab Menu Bar

Specifies the menu bar the user sees on the Home tab. Select the menu bar from the list. For additional information about menu bars, see "Customizing Menu Bars" on page 140.

PatchesTab Menu Bar

Specifies the menu bar the user sees on the Home tab. Select the menu bar from the list. For additional information about menu bars, see "Customizing Menu Bars" on page 140.

Tabs ordering

Specifies the order of the tabs in the Patch Manager web console. Use the directional arrows to move tabs up or down in the list. The Patch Manager web console displays the tab at the top of the list on the far left of the tab row.

Home Page View

Specifies the view the user sees immediately upon logging into the Patch Manager web console. Select the home page from the list. For additional information about views, see "Creating and Managing Views" on page 138.

Default Network Device

Specifies the network device the user sees on the corresponding details page upon logging into the Patch Manager web console. This setting only applies if the user's home page is set to a details page, such as WSUS Server Details or WSUS Node Details. Click Edit to specify the default network device.
**Default Summary View**

Specifies the view associated with the Summary link on the default Home menu bar. The Patch Manager web console also displays this view when the user clicks the Home tab. Select a view from the list.

**Report Folder**

Specifies the folder from which the Orion web console pulls reports for the selected user. To assign a specific set of reports to a user, create a sub-folder in the Reports folder, and then put the specific reports in that folder. Select the user's folder for this setting. The default location of the Reports folder is %PROGRAMFILES%\SolarWinds\Orion\Reports.

**Orion General Settings**

Specifies the views the user sees after clicking on the respective element in the web console. Select a view from the list, or select None to hide details from the user. The following settings are available:

- Node Details View
- Volume Details View
- Group Details View

**Patch Manager Settings**

Specifies the views the user sees after clicking on the respective element in the web console. Select a view from the list, or select None to hide details from the user. The following settings are available:

- PM Summary View
- WSUS Node Details View
- WSUS Server Details View
- Update Details View
Appendix D

SolarWinds Orion Web Console Components

The tables in this section list the SolarWinds Orion Platform services and programs the Patch Manager web console installer installs. If you are running the Patch Manager web console on a server that does not serve any other Orion Platform products, you can remove any items that are not required to run the web console.

**SolarWinds Orion Services**

The following table describes the services installed with the Patch Manager web console. The Required column indicates whether the service is required to run the Patch Manager web console.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>SolarWinds Alerting Engine</td>
<td>Processes Advanced Alerts for the Orion Platform products</td>
<td></td>
</tr>
<tr>
<td>SolarWinds Collector Data</td>
<td>Polls data from network devices</td>
<td></td>
</tr>
<tr>
<td>Processor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SolarWinds Collector Management Agent</td>
<td>Polls data from network devices</td>
<td></td>
</tr>
<tr>
<td>SolarWinds Collector Polling Controller</td>
<td>Polls data from network devices</td>
<td></td>
</tr>
<tr>
<td>SolarWinds Information Service</td>
<td>Facilities data exchange and the web console Application Programing Interface (API); also known as SWIS</td>
<td>Yes</td>
</tr>
<tr>
<td>SolarWinds Information Service V3</td>
<td>Facilities data exchange and the web console Application Programing Interface (API); also known as SWIS</td>
<td>Yes</td>
</tr>
<tr>
<td>SolarWinds Job Engine</td>
<td>Polls data from network devices and executes some management tasks</td>
<td></td>
</tr>
<tr>
<td>SolarWinds Job Engine V2</td>
<td>Polls data from network devices and executes some management tasks</td>
<td></td>
</tr>
<tr>
<td>SolarWinds Job Scheduler</td>
<td>Polls data from network devices and executes some management tasks</td>
<td></td>
</tr>
</tbody>
</table>
SolarWinds Orion Programs

The following table describes the programs installed with the Patch Manager web console. The Required column indicates whether the program is required to run the Patch Manager web console.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>SolarWinds Collector</td>
<td>A collection of the three &quot;Collector&quot; services</td>
<td></td>
</tr>
<tr>
<td>SolarWinds Information Service</td>
<td>A collection of the two &quot;SWIS&quot; services</td>
<td>Yes</td>
</tr>
<tr>
<td>SolarWinds Job Engine</td>
<td>Polls data from network devices and executes some management tasks</td>
<td></td>
</tr>
<tr>
<td>SolarWinds Orion Core Services</td>
<td>A collection of the Orion website and the following services:</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>• SolarWinds Job Scheduler</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SolarWinds Orion Module Engine</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SolarWinds Syslog Service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SolarWinds Trap Service</td>
<td></td>
</tr>
<tr>
<td>SolarWinds Orion Improvement Program</td>
<td>An optional service to collect and report usage statistics to SolarWinds, Inc.</td>
<td></td>
</tr>
<tr>
<td>SolarWinds Orion Network Atlas</td>
<td>Allows users to create network maps based on Orion nodes and locations</td>
<td></td>
</tr>
</tbody>
</table>

SolarWinds Orion Shortcuts

The following table describes the Start menu shortcuts the Patch Manager web console installer creates. The Supported column indicates whether the Patch Manager web console supports one or more features in the group.

These shortcuts can be found in Start > All Programs > SolarWinds Orion.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advance Features</td>
<td>Contains advance Orion Platform management features</td>
<td>Yes</td>
</tr>
<tr>
<td>Alerting, Reporting, and Mapping</td>
<td>Contains programs to create and manage Orion alerts, reports, and maps</td>
<td></td>
</tr>
<tr>
<td>Configuration and Auto-Discovery</td>
<td>Contains the Configuration Wizard and Network Discovery programs</td>
<td>Yes</td>
</tr>
<tr>
<td>Documentation and Support</td>
<td>Contains links to common support resources</td>
<td>Yes</td>
</tr>
<tr>
<td>Grouping and Access Control</td>
<td>Contains programs to apply Orion user account limitations and manage Orion Platform custom properties</td>
<td></td>
</tr>
<tr>
<td>Syslog and SNMP Traps</td>
<td>Contains syslog and SNMP trap viewers</td>
<td></td>
</tr>
<tr>
<td>Orion Improvement Program Settings</td>
<td>Allows you to specify whether or not to send usage statistics to SolarWinds, Inc.</td>
<td>Yes</td>
</tr>
<tr>
<td>Orion Web Console</td>
<td>Opens the Orion web console in the default Internet browser.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Appendix E

Advanced Setup CLI Commands

Use SetupHelper.exe from the command line of any additional Patch Manager server on which the standard setup wizards have failed. The default location for this program is:

```
%PROGRAMFILES%\SolarWinds\Patch Manager\Server\SetupHelper.exe
```

For onscreen instructions, run the program from the command line with the argument, `/?`:

```
setuphelper /?
```

To add a Patch Manager server to the environment and automatically register with the PAS (that is, obtain and install the required server certificates):

```
setuphelper /provisionserver /type primary
```

To add a Patch Manager server to the environment and locally install the required server certificates:

```
setuphelper /provisionserver /type local
```

To add the service account to the environment:

```
setuphelper /provisionserviceaccount <fullname of service account>
```

To create the first management group:

```
setuphelper /createmgmtgroup "Managed Enterprise" /description "The Managed Enterprise Management Group" /addserver <deviceID>
```

Note: The deviceID for the Patch Manager PAS can be found in the registry:
HKLM\Software\EminentWare\Data Grid Server, in the value, DeviceID

To assign a server to a specific management group:

```
setuphelper /assignservertomgmtgroup <managementGroupID> addserver <deviceID>
```

To remove the local server from the environment:

```
setuphelper /unregisterserver
```
To reset the ACLs on a server:

```
setuphelper /secureserver /rootdirectory "C:\Program Files\EminentWare"
/serviceaccountname <fullname of service account> /sqlinstance
THISMACHINE\EMINENTWARE
```

To reset the ACLs on a console-only installation:

```
setuphelper /secureconsole /rootdirectory "C:\Program Files\EminentWare"
```

To re-provision the Patch Manager certificate:

```
setuphelper /reprovisioncertificates
```

To uninstall Patch Manager:

```
setuphelper /uninstall
```

To create a custom event log:

```
setuphelper /createcustomeventlog
```

To remove the custom event log:

```
setuphelper /deletecustomeventlog
```
# Appendix F

## Table of Status Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Object</th>
<th>Status Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Task</td>
<td>Completed</td>
</tr>
<tr>
<td>☐</td>
<td>Task</td>
<td>Running</td>
</tr>
<tr>
<td>⬇️</td>
<td>Operation</td>
<td>Failed</td>
</tr>
<tr>
<td>✓</td>
<td>Operation</td>
<td>Succeeded</td>
</tr>
<tr>
<td>✓</td>
<td>Synchronization</td>
<td>Succeeded</td>
</tr>
<tr>
<td>⬶️</td>
<td>Synchronization</td>
<td>Running</td>
</tr>
<tr>
<td>⬇️</td>
<td>Synchronization</td>
<td>Failed</td>
</tr>
<tr>
<td>🍀</td>
<td>Managed Workstation</td>
<td>No issues</td>
</tr>
<tr>
<td>🍀</td>
<td>Managed Workstation</td>
<td>Connectivity failure</td>
</tr>
<tr>
<td>🍀</td>
<td>Managed Workstation</td>
<td>Connected, but some operation failed</td>
</tr>
<tr>
<td>🍀</td>
<td>Managed Server</td>
<td>No issues</td>
</tr>
<tr>
<td>🍀</td>
<td>Managed Server</td>
<td>Connectivity failure</td>
</tr>
<tr>
<td>🍀</td>
<td>Managed Server</td>
<td>Connected, but some operation failed</td>
</tr>
<tr>
<td>🛠️</td>
<td>3rd party package</td>
<td>Package</td>
</tr>
<tr>
<td>🛠️</td>
<td>3rd party package</td>
<td>Using PackageBoot</td>
</tr>
<tr>
<td>✍️</td>
<td>3rd party package</td>
<td>Editable</td>
</tr>
<tr>
<td>✍️</td>
<td>3rd party package</td>
<td>Read only</td>
</tr>
<tr>
<td>🕵️</td>
<td>3rd party/WSUS package</td>
<td>Content downloaded</td>
</tr>
<tr>
<td>🕵️</td>
<td>3rd party/WSUS package</td>
<td>Missing content</td>
</tr>
<tr>
<td>🕵️</td>
<td>3rd party/WSUS package</td>
<td>Is superseding</td>
</tr>
<tr>
<td>Package Type</td>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>3rd party/WSUS package</td>
<td>Is superseded</td>
<td></td>
</tr>
<tr>
<td>3rd party/WSUS package</td>
<td>Is superseding and superseded</td>
<td></td>
</tr>
</tbody>
</table>
Appendix G

First Time Usage Wizard FAQ

This section addresses some of the most common questions about the First Time Usage Wizard.

Why does it take so much time to install an update?

When the First Time Usage Wizard installs patches, it takes some time to complete. The wizard must first download the package from the vendor site and then push the package to the client computer. The size of the package and your network speed can negatively impact the length of time you spend waiting for the patch to install. Additionally, the wizard performs some checks on the client computer(s) to ensure that the package can be installed.

What is the First Time Usage Wizard doing when it is installing packages?

After the First Time Usage Wizard has downloaded and pushed a package to a client computer, the wizard checks the package revision against the software installed on the computer to ensure that the downloaded package is compatible with the software already installed on the computer. If the package is compatible, the wizard precedes to install the package. If the package is not compatible or otherwise unable to be installed, the wizard will return an error message with the most likely failure cause.

How can I decrease the amount of time the wizard takes?

To decrease the amount of time it takes for the First Time Usage Wizard to download or push the packages, try running the wizard during non-peak networking hours or only updating one or two computers at a time.

Can I mass add computers?

While you can add multiple computers to the wizard, you cannot add all computers from a domain or workgroup to the wizard. You must add managed resources outside of the First Time Usage Wizard.