Patch Manager

Version 2020.2
Copyright

© 2020 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.
Table of Contents

Introduction ................................................................................................................................................. 9
  Architecture ............................................................................................................................................... 9
  Components ............................................................................................................................................... 10
  Patch Manager licensing ....................................................................................................................... 13
  Upgrade your Evaluation license ........................................................................................................... 13

Patch Manager Administrator Console ...................................................................................................... 17
  Optional extension packs ....................................................................................................................... 17
  Navigation pane ...................................................................................................................................... 18
  Data Grid pane ....................................................................................................................................... 22
  Task Options Wizard .............................................................................................................................. 30
  Patch Manager computer groups ........................................................................................................... 38
  Console status icons ............................................................................................................................... 40

Configure Patch Manager .......................................................................................................................... 42
  Configure the managed resources .......................................................................................................... 42
  Configure credentials and credential ring rules ..................................................................................... 44
  Configure the third party update schedule ............................................................................................ 46
  Configure the publishing servers .......................................................................................................... 49
  Configure the Patch Manager email settings ......................................................................................... 51
  Configure the administrative settings ................................................................................................... 57
  Configure the managed clients .............................................................................................................. 62

Publish third-party updates .......................................................................................................................... 69
  Manage the publishing servers ............................................................................................................. 69
  Import and export catalogs .................................................................................................................... 70
  Create and publish software packages .................................................................................................. 72
  Manage third-party packages ................................................................................................................ 88
  Auto-publish third-party updates to WSUS ............................................................................................ 90
Push, approve, and install third party updates ................................................................. 95
Push the updates ........................................................................................................... 95
Approve the updates .................................................................................................. 100
Install the updates using Update Management ......................................................... 102
Create PowerShell scripts for third-party updates .................................................... 103
Push the updates with PowerShell scripts ................................................................. 114
Schedule the WSUS updates .................................................................................... 122
Stop an update to the managed systems ................................................................... 123
Delete an update to the managed systems ............................................................... 124
Check the task history .............................................................................................. 125
Troubleshoot certificate errors during third-party updates ....................................... 126
Uninstall a program using Patch Manager Computer Explorer .............................. 129

Generate an inventory and create reports .................................................................... 130
Configure the inventory tasks ................................................................................... 130
Generate and view reports .......................................................................................... 142
View the available data sources ................................................................................ 161

Manage WSUS using Patch Manager ......................................................................... 164
Select the Microsoft products on the WSUS server ................................................ 164
Synchronize the WSUS server with Microsoft Update .............................................. 164
Delete expired updates and revisions from the WSUS server ................................ 168
Repair and maintain the Windows Update Agent ..................................................... 170
Update the Windows Update Local Policy on remote systems ............................... 173
Move computers between WSUS groups .................................................................. 174

Advanced configuration options .................................................................................. 176
Patch Manager management groups ......................................................................... 176
Install the Patch Manager Administrator Console on a remote system .................. 186
Configure additional Patch Manager servers ......................................................... 187
Manage users and security ................................................................. 189
  Credentials .................................................................................... 189
  Credential rings ............................................................................. 192
  Security roles .................................................................................. 195
  User preferences .......................................................................... 199
  Server certificates .......................................................................... 201
  Web Console user accounts .......................................................... 202

Manage client WMI connectivity ....................................................... 209
  WMI requirements ......................................................................... 209
  WMI Providers security and permissions ....................................... 209
  Install the SolarWinds WMI Providers ......................................... 210
  Verify WMI connectivity ............................................................... 214
  Troubleshoot the WMI connections ............................................. 215
  Resolve WMI connection issues .................................................... 218

Patch Manager agents .................................................................... 223
  Agent requirements ........................................................................ 223
  Deploy agents .............................................................................. 224
  Approve agents ............................................................................ 228
  Configure agents .......................................................................... 230

Integrate Patch Manager with the Orion Platform ......................... 232
  Patch Manager Orion integration architecture .............................. 233
  Access Patch Manager data in the Orion Web Console ............... 234
  Configure the Patch Manager Web Console settings .................. 235
  Patch Manager Summary view ..................................................... 238
  Generate Patch Manager reports in the Orion Web Console ....... 253
  Install the Patch Manager Orion Web Console on a separate server 265

Administrator functions and settings ........................................... 266
Manage Patch Manager tasks ................................................................. 266
Clear outdated files from the Patch Manager server .............................. 270
View the server settings and details ...................................................... 273
Wake on LAN ...................................................................................... 282
Wake on LAN requirements ................................................................. 282
Set up Wake on LAN ........................................................................ 282
Advanced deployment examples ............................................................. 287
Server roles ....................................................................................... 287
Design Considerations ....................................................................... 288
Set up an Automation Server ............................................................... 290
Set up additional Application and Management Servers .................. 303
Configure a downstream WSUS server ................................................ 307
Add a managed domain or workgroup .................................................. 307
Manage servers in a DMZ outside the local domain ............................. 309
Troubleshoot Patch Manager ............................................................... 310
General issues .................................................................................. 310
Error messages .................................................................................. 311
Downstream WSUS server issues ......................................................... 314
Set up Patch Manager with SCCM ....................................................... 316
Integrate Patch Manager with SCCM ................................................... 316
Publish third-party updates ................................................................ 320
Manage the published third-party updates ............................................. 324
Manage the WSUS servers using the SCCM console ......................... 328
Provision the WMI Providers using the SCCM console ....................... 331
Resolve WMI connectivity issues using the SCCM console ................. 332
Verify WMI connectivity using the SCCM console ............................... 333
Troubleshoot Patch Manager in SCCM ............................................... 334
<table>
<thead>
<tr>
<th>Reference</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patch Manager server settings</td>
<td>335</td>
</tr>
<tr>
<td>Orion Web Console components</td>
<td>345</td>
</tr>
<tr>
<td>Advanced Setup CLI commands</td>
<td>347</td>
</tr>
</tbody>
</table>
Introduction

SolarWinds Patch Manager is a Microsoft Management Console (MMC) that adds additional functionality to Windows Server Update Services (WSUS) and Microsoft System Center Configuration Manager (SCCM). When installed on a WSUS or SCCM server, you can update Windows servers and workstations in your corporate network with Microsoft and third-party software updates.

You can install Patch Manager in a stand-alone deployment or an integrated deployment with an existing Orion Platform.

Architecture

The following diagram illustrates a typical Patch Manager installation.
In this installation:

- Patch Manager is installed on a dedicated server (known as the Primary Application Server).
- Windows Server Update Services (WSUS) is enabled in the Microsoft® Windows Server® operating system.
- No additional SolarWinds Orion Platform products or third-party applications are installed on the server.

> In SCCM environments, the WSUS server corresponds with the SCCM software update point (SUP).

Patch Manager runs the EminentWare Data Grid Server Service. This service starts automatically at system startup and manages all aspects of the Patch Manager server except the Microsoft SQL Server® database resources.

See Advanced Deployment Scenarios for details about alternative deployment scenarios.

**Components**

Patch Manager uses the following components and devices in a deployment:

- WSUS
- SCCM
- SQL Server database
- Administrator console
- Web Console
- Managed computers node
- Patch Manager agents

**WSUS**

WSUS is included in supported Windows Server® operating systems. This software component distributes and manages updates and hotfixes released by Microsoft in a corporate enterprise. WSUS replaces Windows Update and allows system administrators to distribute Windows updates and hotfixes released by Microsoft to systems in a corporate environment. Patch Manager integrates with WSUS to distribute Windows updates, third-party updates, and custom packages to managed systems in your deployment.
SCCM

Microsoft System Center Configuration Manager (SCCM) is a Microsoft systems management software product that manages large groups of computers in a corporate enterprise. Patch Manager integrates with SCCM to distribute Windows updates, non-Microsoft (third-party) updates, and custom packages to managed systems in your deployment.

SQL Server database

Patch Manager supports the following Microsoft SQL Server database software:

- Microsoft SQL Server Express
- Microsoft SQL Server Standard or Enterprise Edition

If you select SQL Server Express during the installation, Patch Manager installs SQL Server Express on the PAS with no user intervention.

💡 SQL Server Express has a 10 GB storage limit. SolarWinds recommends this option for Evaluation deployments only.

If you select SQL Server Standard or Enterprise Edition, be sure the SQL Server software is installed on a separate server and enter the database instance path in the Patch Manager Administrator Console. SolarWinds recommends this option to prevent a single point of failure and maximize database performance.

Administrator Console

The Patch Manager Administrator Console is a Microsoft® Management Console (MMC) 3.0-based snap-in that connects to the Patch Manager Primary Application Server. In SCCM environments, an additional Patch Manager console is integrated with the SCCM console. You can install the administrator console on the Patch Manager server or a remote workstation.

Using the administrator console, you can:

- View and manage Microsoft updates on your WSUS server or SCCM software update point (SUP).
- Publish and manage third-party updates using WSUS functionality in both WSUS and SCCM 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 detailed reports that describe the updates and assets in your publishing environment.
In SCCM environments, an additional Administrator Console integrates with the SCCM console.

Web Console

The Patch Manager Web Console is a read-only console that displays detailed information about your deployment collected from a Patch Manager Application server. You can install the web console on any Windows server that can access the Patch Manager Application Server. When the installation is completed, you can access the console from any computer with access to the host web server's website.

When you integrate Patch Manager with the Orion Platform, the Orion Installer adds Patch Manager to your existing Orion Web Console.

Managed computers node

The Managed Computers node is located in the navigation pane of the Patch Manager Administrator Console. This node includes a list of machines that are targeted with a task (such as Inventory or Update Management) Managed computers can include WSUS servers, SCCM servers, and managed clients in your corporate enterprise.

You can use this node to locate a machine name, right-click the name, and execute a task. Patch Manager also uses this node and the Task History node to calculate the number of computers for your product license.

For optimal inventory and reporting functionality, deploy the Patch Manager Windows Management Interface (WMI) providers to all managed clients. See Manage Client WMI connectivity for details.

Patch Manager agents

Patch Manager agents provide a communications link between the managed computer and the PAS. The agents poll the server at set intervals using asynchronous remote procedure calls.

Use Patch Manager agents when your managed computers are:

- DISconnected from the corporate network
- Cannot be managed with WMI
- Protected by stringent firewall rules or virtual private networks
Patch Manager licensing

SolarWinds licenses Patch Manager based on the number of managed computers. These computers include:

- Microsoft® Windows Server® Update Services (WSUS)
- Microsoft System Center Configuration Manager (SCCM)
- Patch Manager servers (including the Primary Application Server)
- Managed clients

The Primary Application Server (PAS) calculates the number of managed computers using the following sources located in the Patch Manage Admin Console navigation menu:

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

If you discover that you exceeded your product license, see License count exceeded error in Patch Manager for steps to resolve the issue.

Upgrade your Evaluation license

You can purchase a Patch Manager license in the Customer Portal. After you complete the purchase, activate the license using the SolarWinds Licensing application located in the Windows App Panel of your Windows Server operating system.

- The Primary Application Server (PAS) stores the SolarWinds Patch Manager license for the deployment. If you add new SolarWinds Patch Manager servers (such as an Automation Server), these servers do not require a license.

Copy the activation key from the Customer Portal

After you purchase a license, the activation key is available on the Customer Portal.

1. Log in to the Customer Portal using your SolarWinds Customer ID (SWID) and password.
2. Click License > Manage Licenses.
3. Click the All Products drop-down menu and select Patch Manager.
4. Click [+ ] next to Patch Manager.

5. Copy the activation key to a file.

Activate the license

After you copy the activation key, use the SolarWinds Licensing app to apply the activation key and activate the license.

1. Log in to the PAS as an administrator.
2. Verify that the server has Internet access.
   
   If you access the Internet through a proxy server, locate and record the following information for a future step:
   
   - Proxy address and port
   - Proxy user name and password
3. Access Apps in the Windows operating system.
4. In the SolarWinds group, click SolarWinds Licensing.

5. Click Enter Licensing Information.
6. Activate the license online or offline.

Activate the license online

If the PAS server is connected to the Internet, activate the license online.

1. In the Activate Patch Manager window, select I have internet access and an activation key from my customer portal license management page.
2. If you access the Internet through a proxy server, select I access the Internet through a proxy server and complete the fields in the window.

3. Paste the activation key in the Activation Key field, and click Next.

4. Complete the remaining fields, and click Activate.

Activate the license offline

If the PAS is not connected to the internet, activate the license offline.

1. In the Activate Patch Manager window, select This server does not have Internet access. Guide me through offline, manual activation.

2. Click Next.

3. Review the instructions in the window, and click Next.

4. Complete the remaining fields, and click Activate.

View the license

After you active the license, you can view the license in the Patch Manager Admin Console.

1. Log in to the SolarWinds Patch Manager Admin Console as an administrator.

2. Click Patch Manager System Configuration in the navigation menu.

3. Click View Product Licensing in the Patch manager System Tasks window.

4. Verify the license information in the Patch Manager System Licensing window.
When the license expires, a banner displays in the Administration and Reporting > Software Publishing window.
Patch Manager Administrator Console

The Patch Manager Administrator Console is a Microsoft Management Console (MMC) 3.0-based snap-in that integrates with Windows Server Update Services (WSUS)—an optional extension pack that you install in a supported Microsoft® Windows Server® operating system on a dedicated server. Use the console to view, manage, and deploy Microsoft and third-party updates, and perform additional administrative functions.

You cannot perform all administrative functions using the Patch Manager Administrator Console from within the SCCM console. However, all of the Patch Manager functionality is available in the stand-alone Patch Manager Administrator Console.

Optional extension packs

During the initial configuration, Patch Manager provides the option to select and install:

- Windows Server Update Services (WSUS) Extension Pack
- System Center Configuration Manager (SCCM) Extension Pack

The following table lists the features included with each Extension Pack.

<table>
<thead>
<tr>
<th>Extension Pack</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSUS Extension Pack</td>
<td>- WSUS tasks in the Enterprise &gt; Update Services node</td>
</tr>
<tr>
<td></td>
<td>- Update Management and Update Management Wizard tasks</td>
</tr>
<tr>
<td></td>
<td>- Inventory task</td>
</tr>
<tr>
<td></td>
<td>- WSUS Reports in the Administration and Reporting &gt; Reporting node</td>
</tr>
<tr>
<td>SCCM Extension Pack</td>
<td>- Enterprise &gt; Configuration Manager Site Servers node</td>
</tr>
<tr>
<td></td>
<td>- SCCM tasks and tabs in Computer Explorer</td>
</tr>
<tr>
<td></td>
<td>- Client management and health monitoring tasks</td>
</tr>
<tr>
<td></td>
<td>- Configuration Manager agent configuration tasks</td>
</tr>
</tbody>
</table>

See SCCM Extension Pack for Patch Manager for additional details.
You can run both extension packs with a single Patch Manager license, and each pack provides unique features. Select extension packs when you first configure your Patch Manager server, or perform the following steps to add these features:

1. Open the Patch Manager Administrator Console.
2. In the Patch Manager menu, click Patch Manager System Configuration.
3. In the Patch Manager System Tasks pane, click Select Products and Features.
4. Select the extension pack(s), and click Continue.

5. In the Actions pane, click Refresh to refresh your action options.
6. Close the Patch Manager Administrator Console.
7. Restart the Patch Manager Administrator Console to refresh the Patch Manager menu options.

**Navigation pane**

The navigation pane displays the action categories (or nodes) available in Patch Manager. Each category contains a drop-down menu that displays additional resources and tasks you can perform in the Patch Manager Administrator Console.

The navigation pane contains the following nodes:

- **Enterprise**
- **Administration and Reporting**
- **Patch Manager System Configuration**
Enterprise node

Use the Enterprise node to select WSUS servers and computers you want to manage in your enterprise network or a Patch Manager group. If the computer connects to your network using an agent, you can approve or disapprove the agent as required.

Select the Microsoft and third-party updates you want to install on your targeted systems.

You cannot run the Update Management Wizard to select specific updates.

Below is a description of each child node in the Enterprise node.

<table>
<thead>
<tr>
<th>Child Node</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Services</td>
<td>Lists 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.</td>
</tr>
<tr>
<td>Microsoft Windows Network</td>
<td>Lists each domain, workgroup, and Patch Manager computer group available to the Patch Manager Application Server (PAS). This node replicates the Windows network browser in the Application Server.</td>
</tr>
<tr>
<td>Managed Computers</td>
<td>Displays the computers included in one or more Managed Computer inventory events. This node also displays all Patch Manager and WSUS servers.</td>
</tr>
<tr>
<td>Agents</td>
<td>Displays the approved, pre-approved, and disapproved agents running on the managed computers.</td>
</tr>
</tbody>
</table>

Administration and Reporting node

Use the Administration and Reporting node to select third-party updates and schedule tasks that install these updates on your managed systems.
You can schedule tasks immediately or during your non-business hours to minimize bandwidth and impact to your business systems. If you have custom packages (or Java updates with complex installation scenarios) created for your environment that require a specific pre- and post-installation environment, you can automate these patches using built-in Package Boot™ technology.

Check out this video (26:58) for details on how to create custom packages using Package Boot Technology.

SolarWinds supports packages created and provided by SolarWinds or for packages of SolarWinds products. SolarWinds does not provide support for custom code or software packages created by third-party sources. See the Patch Manager Product Forum on THWACK for help with custom packages.

After you complete a task, you can generate a report to demonstrate patch compliance to your auditors and internal stakeholders.

The following table describes each child node in the Administration and Reporting node.

<table>
<thead>
<tr>
<th>Child Node</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Publishing</td>
<td>Contains a child node for each third-party update vendor you are synchronizing. This node displays all updates for the selected vendor. It also contains a Rules node that lists your software publishing rules.</td>
</tr>
<tr>
<td>Task History</td>
<td>Displays a list of past Patch Manager tasks and details about whether the task completed or failed.</td>
</tr>
<tr>
<td>Scheduled Tasks</td>
<td>Displays a list of scheduled Patch Manager tasks. Use this node to view, manage, or run previously-scheduled tasks.</td>
</tr>
<tr>
<td>Active Tasks</td>
<td>Displays the progress of all active Patch Manager tasks.</td>
</tr>
</tbody>
</table>
### Child Node | Description
--- | ---
Reporting | View, run, manage, and create pre-configured and custom reports. This node contains a child node that stores WSUS, configuration management, and task history reports. This node also contains a child node that stores the WSUS, configuration management, and task history reports.

---

**Patch Manager System Configuration node**

Use the Patch Manager System Configuration node to configure the groups, servers, and settings in your Patch Manager deployment.

![Patch Manager (spm-mgom)](patch_manager_tree.png)

Using this node, you can:

- Create a [management group](#) to manage the domains, workgroups, and WSUS servers in a specific location or group
- Configure and manage the Application Server for load balancing, separate business units, or users at different locations
- Configure and manage the Management Server to store inventory data for management resources in secondary management groups
- Set up and manage the security settings (such as credential rings and security roles) in your Patch Manager deployment

Below is a description of each child node in the Patch Manager System Configuration node.

<table>
<thead>
<tr>
<th>Child Node</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Groups</td>
<td>Contains a child node for each Patch Manager management group. By default, this node includes the Managed Enterprise management group.</td>
</tr>
</tbody>
</table>

ℹ️ A management group is a container of computers managed by a single Patch Manager server in the Management role.
<table>
<thead>
<tr>
<th>Child Node</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patch Manager Servers</td>
<td>Contains a child node for the Application Server and Management Server roles in your SolarWinds Patch Manager environment. Each child node displays a list of servers in the selected role.</td>
</tr>
<tr>
<td>Security and User Management</td>
<td>Contains tabs to view and manage the security and user settings in your Patch Manager deployment. These settings include:</td>
</tr>
<tr>
<td></td>
<td>- Credentials</td>
</tr>
<tr>
<td></td>
<td>- Credential rings</td>
</tr>
<tr>
<td></td>
<td>- Server certificates</td>
</tr>
<tr>
<td></td>
<td>- Security roles</td>
</tr>
<tr>
<td></td>
<td>- User preferences</td>
</tr>
</tbody>
</table>

### Data Grid pane

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

The Patch Manager Administrator Console saves your settings in the current user profile.

### Select columns

Use the Column Chooser to choose which columns to show or hide in the Patch Manager Administrator Console. When you are finished, you can save your new layout or allow your previous layout to display when you return to this view. Using this process, you can view data for all resources. After you complete your selections, only the selected columns display in the view.

1. In the navigation pane, select the view you want to customize (for example, Enterprise > Managed Computers).

2. In the center pane, right-click any column header and select Choose Columns to display the Column Chooser window.
3. Select the columns you want to display in the Patch Manager Console.

![Column Chooser](image)

4. Close the Column Chooser window.

   The selected columns display in the view.

<table>
<thead>
<tr>
<th>Name</th>
<th>Domain/Workgroup</th>
<th>Operating System</th>
<th>IP Address</th>
<th>Last Contact Time</th>
<th>Last Inventory Attempt Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLANK-ORION</td>
<td>WORKGROUP</td>
<td>Windows Server</td>
<td>10.199.21.37</td>
<td>10/25/2017 2:00 PM</td>
<td>10/25/2017 2:00 PM</td>
</tr>
<tr>
<td>ORION-MCCM</td>
<td>WORKGROUP</td>
<td>Windows Server</td>
<td>10.199.21.32</td>
<td>10/25/2017 2:00 PM</td>
<td>10/25/2017 2:00 PM</td>
</tr>
<tr>
<td>SPM-MCCM</td>
<td>WORKGROUP</td>
<td>Windows Server</td>
<td>10.199.21.33</td>
<td>10/25/2017 2:00 PM</td>
<td>10/25/2017 2:00 PM</td>
</tr>
</tbody>
</table>

5. (Optional) Click Save View Layout in the Actions pane to save your layout.

Reorganize columns

You can reorganize columns to see the most important information first to help you manage your deployment. When you are finished, you can save your new layout or allow your previous layout to display when you return to this view.

1. In the navigation pane, select the view you want to customize (for example, Enterprise > Managed Computers).
2. In the center pane, drag the targeted column to a new position.

   The Patch Manager Administrator Console displays arrows above and below the header bar to indicate where the column will go.
3. Drop the column into the new location.

4. (Optional) Click Save View Layout in the Actions pane to save your layout.

**Sort column data**

You can sort entries by clicking one or more column headers in the data grid. You can sort each column in either ascending or descending order. When you are finished, you can save your new layout or allow your previous layout to display when you return to this view.

1. In the navigation pane, select the view you want to customize (for example, Enterprise > Managed Computers).

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.
To sort a data grid by values in more than one column, hold <Shift> while clicking the consecutive sorting columns.

4. (Optional) Click Save View Layout in the Actions pane to save your layout.

Filter column data

You can filter entries in the data grid by the values in one or more column headers. Use this process to view specific data for a specific value. When you are finished, you can save your new layout or allow your previous layout to display when you return to this view.

Filter by specific values

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

1. In the navigation pane, select the view you want to customize.

   For example, Enterprise > Managed Computers.

   The window displays all managed computers.

<table>
<thead>
<tr>
<th>Name</th>
<th>Domain/Workgroup</th>
<th>Operating System</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>APOLLO</td>
<td>OLYMPUS.LAB</td>
<td>Microsoft Windows Server 2019 Standard</td>
<td>10.199.25.108</td>
</tr>
<tr>
<td>ARES</td>
<td>OLYMPUS.LAB</td>
<td>Microsoft Windows Server 2019 Standard</td>
<td>10.199.25.53</td>
</tr>
<tr>
<td>ARTEMIS</td>
<td>olympus.lab</td>
<td>Microsoft Windows Server 2012 R2 Datacenter</td>
<td>10.199.25.41</td>
</tr>
<tr>
<td>ATHENA</td>
<td>OLYMPUS.LAB</td>
<td>Microsoft Windows Server 2016 Datacenter</td>
<td>10.199.25.92</td>
</tr>
<tr>
<td>CHAOS</td>
<td>OLYMPUS.LAB</td>
<td>Microsoft Windows Server 2019 Standard</td>
<td>10.199.25.44</td>
</tr>
<tr>
<td>CRONUS</td>
<td>OLYMPUS.LAB</td>
<td>Microsoft Windows Server 2019 Standard</td>
<td>10.199.25.107</td>
</tr>
<tr>
<td>DIONYSUS</td>
<td>OLYMPUS.LAB</td>
<td>Microsoft Windows Server 2019 Standard</td>
<td>10.199.25.68</td>
</tr>
</tbody>
</table>

2. In the center pane, locate a column header that contains a value you want to filter.

   For example, you want to locate all computer that are running a specific Microsoft Windows Server version. For this filter, you can use the Operating System column.

3. In the Operating System column, click ✓ and select an operating system as your filter value.

   For example, select Microsoft Window Server 2019 Standard. This will display all computers running this operating system.
The Operating System filter icon changes to ▼ and the corresponding values for the selected operating system display in the window.

4. (Optional) In the Actions pane, click Save to save your layout. When completed, the window pane only displays computers based on your selected operating system.

   To redisplay all computers, click ▼ and select All.

Create custom filters

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

1. In the navigation pane, select the view you want to customize.

   For example, Enterprise > Managed Computers.

   The window displays all managed computers.

2. In the center pane, select a column header to filter.
For example, you want to search for computers that were last inventoried before December 18, 2019. For this example, you can filter the Last Inventory Attempt Time column.

3. In the Last Inventory Attempt Time column, click 📊 and select Custom.

![Custom Filter](image)

4. In the Custom Filter window, enter your custom filter as a search string.

   In this example, you want to search all computers that were last inventoried before December 18, 2019.

   ![Custom Filter](image)

   You can click Add to add additional filters and narrow your search.

5. Click OK.

   The Last Inventory Attempt Time filter icon changes to 📊, and the window displays all computers that were inventoried prior to December 18, 2019.

   ![Computers List](image)

6. (Optional) In the Actions pane, click Save to save your layout. When completed, the window pane only displays computers based on your custom filter.

   To redisplay all computers, click 📊 and select All.
Group column data

You can group entries in a data grid by dragging the column to the grouping bar directly above the column headers. Then expand or collapse the entries in each group to view your targeted data. You can temporarily group the entries in a data grid or save the layout.

Add a column header to the grouping bar

Complete the following procedure 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.
   
   For example: Administration and Reporting > Reporting > WSUS Reports > Windows Server Update Services Analytics.
   
2. In the center pane, drag the column header into the grouping bar. To group entries by more than one column, drag the additional column header(s) into the grouping bar.
   
   The console displays arrows above and below the existing column header(s) in the grouping bar to indicate where the header is placed.

![Grouping Bar Example]

The header serves as the parent node for the grouped data. Subsequent headers serve as child nodes to the header.

To group the entries by two or more columns, drag the additional column headers into the grouping bar. The console displays arrows above and below the existing column headers in the grouping bar to indicate where the new header is placed.

3. Release the mouse button.

   The Type column categories (for example, System and User Defined) are grouped together in...
separate drop-down views.

Remove a column header from the grouping bar

To remove a header from the grouping bar, drag the header out of the grouping bar.

When you release the mouse button, the column header is restored to its previous display in the data grid.

To save the current layout, click Save View Layout in the Actions pane.
Task Options Wizard

The Task Options Wizard is integrated into several actions and procedures you perform in Patch Manager, such as configuring a managed computer inventory task and installing updates from a WSUS report. Use the wizard to select additional options to complete a task. These options may include computers in your network, configuration information (such as IP addresses), and the date, time, and frequency when the task runs.

The wizard implements three primary dialog boxes:

- Computer Selection
- Scheduling and Notification Options
- Summary

Depending on your options, these dialog boxes open secondary pages for more advanced settings. The following sections describe how to complete the dialog boxes that display in the Task Options Wizard:

- Computer Selection page
- Scheduling and Notification Options page
- Summary page

Computer Selection page

Depending on the task, the Task Options Wizard opens a dialog box that prompts you to select the computers you want to include in a task. This dialog box can be populated or blank, depending on your method for launching the task.

The primary selections in this dialog box include:

- Add computers
- Browse computers
Select computers using rules
Additional options

After you complete the Computer Selection options, click Next to configure the Scheduling and Notification Options.

Add computers

Click Add computers in the Task Options Wizard to open the Add Computer dialog box. This dialog box prompts you to enter information about your targeted computer.

1. In the Computer Name field, enter the computer name and click Resolve to auto-fill the remaining fields. If your DNS is set up correctly, clicking Resolve populates the remaining fields.
2. In the Domain/Workgroup field, enter the domain or workgroup for the selected computer.
3. In the Hostname or FQDN field, enter the hostname or Fully Qualified Domain Name (FDQN) for the selected computer.
4. (Active Directory computers) In the Canonical Name field, enter the canonical name used in Active Directory.
5. In the IP address field, enter the IP address of the selected computer.
6. Click the Operating System Version drop-down menu and select the version number.
7. Click Add to continue.
Browse computers

Click Browse computers in the Task Options Wizard to display the Select Computer dialog box. Use this dialog box to select computers from the WSUS Server groups, Active Directory domains and organizational units, workgroups, and Patch Manager computer groups.

1. In the navigation pane, select the container with the computers you want to add.

2. Select the individual computers you want to add. Press <Ctrl> to select multiple computers.

3. Add one or more computers 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 box and manually enter objects to add.

4. Click OK.
   The computers are added to the bottom right pane.

Select computers using rules

Click Select computers using rules in the Task Options Wizard to open the Computer Select Rule Management dialog box. Use this dialog box to select or define a computer selection rule to apply when the task runs.
The computer selection rules are based on 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 a computer filter option.
Additional options

The following table lists the additional options included on the Computer Selection page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove</td>
<td>Removes the selected computers.</td>
</tr>
<tr>
<td>Remove All</td>
<td>Removes all computers from the Computer Selection dialog box.</td>
</tr>
<tr>
<td>Change Domain / Workgroup</td>
<td>Changes the Domain/Workgroup value for the computers highlighted in the Computer Selection dialog box.</td>
</tr>
<tr>
<td>Change canonical path</td>
<td>Changes the absolute unique path (canonical path) for the computers highlighted in the Computer Selection dialog box.</td>
</tr>
<tr>
<td>New Patch Manager Computer Group</td>
<td>Opens the Patch Manager Computer Group Management window. Use this option to define a new Patch Manager Computer Group that contains the selected computers.</td>
</tr>
</tbody>
</table>

Scheduling and Notification Options page

After you complete a Patch Manager task, the Scheduling and Notification Options page prompts you to publish a software package to the WSUS server. You can:

- Schedule the day, time, and frequency of when the task runs
- Export the task results to a file format, such as a Microsoft Excel spreadsheet or text file
- Set up an email notification that notifies you when the task is completed

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

Schedule settings

Use the Schedule Settings box to schedule several Patch Manager tasks to run immediately or on a scheduled day, week, or month.

Select Run Task Now to run the task immediately. To run the task at a scheduled time:
1. Select Schedule the task to run daily, weekly, or monthly, and click Edit.

2. In the Schedule window, enter a start time and date for the scheduled task. To convert the scheduled time to Greenwich Mean Time (GMT), select the Universal Time check box.

![Scheduled Time](image)

- The scheduled time corresponds to the local time on the Patch Manager Automation Server where you created the task. If the targeted computers are located in a different time zone, incorporate the time difference in your Schedule Time settings. If you select Universal Time, calculate the time difference between Universal Time and the time zone of your targeted computers.

3. In the Recurrence pattern box, select an hourly, daily, weekly, or monthly task schedule.

![Recurrence pattern](image)

4. In the Range of recurrence box, select the end date for the task, and click OK.
Export options

When the task is completed, you can export the task results to a variety of formats, including a Microsoft® Excel® spreadsheet or a CSV file. Select an option in the Export Options box.

1. In the Export Options box, select Export results of the task to one of several formats and click Edit.

2. Complete the options in the Export Options window.
   a. Select an export file format for the exported results.
   b. Select a file name for the export. Select Append date and time to file name to add the date and time to the file name.
   c. Select Export record filter if you want to export all records or only records that include
successful or failed operations.

3. Click OK.

Email options

You can configure the task to notify one or more email recipients when the task is completed. If you configured the task to export the results to a file, you can include the file in the email.

1. In the Email Options box, select Send an email notification on completion to, and click Edit.
2. Complete the options in the Email Notification Options window.
a. Select Include task results as attachment to include the exported results with the email notification.

> Attachments are automatically zipped and cannot exceed 10MB.

b. Select Only send notification email if export contains records if you want to suppress task notifications that do not yield results.

> This option is only available if you decide to attach the exported results to the email.

c. Enter one or more email recipients. Separate multiple entries with commas.

d. Click OK.

**Summary page**

After you complete the Task Options Wizard, Patch Manager displays a summary page.

Review the settings on this page. When you are finished, 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**

Computer groups are located on the WSUS server. These groups are used to logically separate machines targeted for patching. Sometimes referred to as WSUS groups or WSUS target groups, these groups display in the navigation pane under Computers and Groups > All Groups.

A default WSUS installation uses Server Side Targeting. When you point a client machine to a WSUS server through Group Policy, the computer displays under Unassigned computers until you move it to another specific group. You can create WSUS groups using various logical grouping based on your needs, such as Servers, Workstations, Operating System, or a name that represents a physical location. After you create the group, move each computer client into the group.

Client Side Targeting is another option. Normally enabled through Group Policy, each machine places itself in a group. Using this method, each machine receive Group Policy from their organizational unit (OU), and each OU can be configured to automatically drop the client machines into the correct WSUS group.

> Beginning in 2020.2, scheduled tasks now support Patch Manager dynamic computer groups. When you add or remove a client computer from a Patch Manager group, the computer is automatically added or removed from the scheduled task. See Schedule the updates to schedule a task.
See Managing Computer Groups on the Microsoft Docs website for more details about managing computer groups.

To create a Patch Manager computer group:

1. Log in to the Patch Manager Administrator Console as an administrator.
2. In the navigation pane, expand Enterprise and select Microsoft Windows Network.

   ![Navigation Pane](image)

3. In the Actions pane, click Add Patch Manager Computer Group.

   ![Actions Pane](image)

4. In the Patch Manager Computer Group Management window, enter or select a name for the computer group.

   ![Computer Group Management Window](image)

5. (Optional) Enter a description for the group.
6. Select the computers to add to the group. See Computer selection for details.

   ![Computer Selection](image)

7. Click Save.

   ![Save Computer Group](image)
The Patch Manager computer groups display in the navigation pane under Microsoft Windows Network.

## Console status icons

The following table lists the status icons that display in the Patch Manager Administrator Console.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Object</th>
<th>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>Scheduled Task</td>
<td>Occurs monthly</td>
</tr>
<tr>
<td>🕒</td>
<td>Scheduled Task</td>
<td>Occurs weekly</td>
</tr>
<tr>
<td>🕒</td>
<td>Scheduled Task</td>
<td>Disabled task</td>
</tr>
<tr>
<td>🕒</td>
<td>Scheduled/Saved Task</td>
<td>Saved task or task that occurs daily or weekly</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>Synchronization</td>
<td>Warning</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 PackageBoo</td>
</tr>
<tr>
<td>Icon</td>
<td>Object</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------</td>
<td>---------------------------------</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>⏰</td>
<td>3rd party/WSUS package</td>
<td>Is superseded</td>
</tr>
<tr>
<td>⏰</td>
<td>3rd party/WSUS package</td>
<td>Is superseding and superseded</td>
</tr>
</tbody>
</table>
Configure Patch Manager

The Primary Application Server (PAS) is a dedicated server that hosts the Primary Application Server (PAS) role. This server provides the default management group, certificate configuration authority, and communications hub for your Patch Manager deployment. This server role is installed on a Microsoft® Windows®-based host system with the Patch Manager Administrator Console.

The Primary Application Server is also referred to as the Patch Manager server.

After you install your first updates, configure the following resources on the Primary Application Server:

- **Managed resources**—the servers and workstations updated by Patch Manager.
- **Credential and credential ring rules** that map user credentials to managed resources (such as computers and servers).
- **Third party update schedules** for your non-Microsoft software updates.
- **Publishing servers** to enable the WSUS server to publish third-party updates and custom packages to the managed systems.
- **Administrative settings**, such as the email and proxy settings.
- **Managed clients**, such as Group Policy settings and configuring clients using the Patch Manager Administrator Console.

Configure the managed resources

Managed resources are servers and workstations updated by Patch Manager. If you have a collection of resources (such as WSUS servers domains and workgroups) located in a specific location, you can group them together into a logical collection called a management group.

Management groups are assigned to a single, unique management server that resides on a Primary Application Server (PAS), Secondary Application Server (SAS), or its own dedicated server. Use the Managed Resource Enterprise Configuration Wizard to configure these devices into a management group you can manage with Patch Manager.

1. Log in to the Patch Manager Administrator Console as an administrator.
2. In the navigation menu, select Patch Manager System Configuration.
3. In the Patch Manager System Tasks pane, double-click Configure Managed Resources in your Enterprise.


5. Select the domains and workgroups that contain the computers you want to manage, and click Next.

6. In the Step 1 panel, enter the required WSUS server information.

   a. Enter the server name.

   b. Click Resolve to populate the remaining fields.

   c. Select a port number. The default port is 80.

   d. Select the Use Secure Sockets Layer (SSL) to connect check box to enable an SSL connection to the management group.

   e. Click the Operating System Version drop-down menu and select the operating system running on the WSUS server.

7. In the Step 2 panel, click Add and add and select the WSUS server.
8. Click Next.

Patch Manager automatically creates the Managed Enterprise management group on the PAS.

9. Click Next.

10. Enter a name and description of the management group, and click Next.

11. Review the summary screen, and click Finish.

Configure credentials and credential ring rules

Check out this video (2:50) on how to use the default credential ring to map end user credentials to managed resources.

A credential ring maps user credentials to managed resources (such as computers and servers). Patch Manager uses a credential ring to identify which credentials to pull from the database before performing tasks on the managed computers in your corporate enterprise.

When you set up Patch Manager for the first time, the installer creates a default credential ring for you. Run the Credential and Credential Rings Rules Wizard to set up the default credential ring and specify the credentials for each group or system.

Use the default credential ring to map user credentials to your managed resources. If you require additional security, you can add additional credential rings and adjust the user preferences.

See Managing Patch Manager Users and Security for details about managing access to Patch Manager resources.

1. In the navigation menu, select Patch Manager System Configuration.

2. In the Patch Manager System Tasks pane, click Configure Security and User Management to start the Credential and Credential Rings Rules Wizard.
3. Click the Credential Ring drop-down menu and select the default credential ring or add a new credential ring.

4. Select an existing credential or add a new credential.
   
a. Click the User Name drop-down menu and select an existing or new credential with a fully-qualified user name in UPN or flat format (for example, useradmin@example.com or COMPANY\useradmin).

   To add a common local computer account, enter .\ before the username. For example, enter or select .\administrator to specify the local Administrator account for several computers.

   b. Enter and confirm the password for the selected account.

5. Add the credential to the credential ring.
   
a. In the User Name column, select a credential.

   b. Click Add to add the credential to the credential ring.

6. Repeat step 4 through step 5 for each additional credential.
7. In the credential ring, select <Default>.

![Credential Ring](image)

8. Click Change Assigned Credential.

9. Select the credential to assign to the resource.

10. Click OK.

11. Repeat step 7 though step 10 for any additional resources you want to add.

12. Click Finish.

**Configure the third party update schedule**

The SolarWinds Third Party Update Library contains third party update catalogs with software updates you can download to Patch Manager. To synchronize the library with Patch Manager, run the Third Party Updates Configuration Wizard. After you complete the wizard, Patch Manager contains the latest third-party updates you can upload to the WSUS server and apply to your managed systems.

![Configuration Wizard](image)

The Evaluation version includes access to a limited selection of third party updates. When you purchase a Patch Manager license, the license includes access to all available catalogs.

1. In the Patch Manager menu, expand Administration and Reporting and select Software Publishing.
2. In the Actions pane, click Patch Manager Update Configuration Wizard.

3. Verify that the Patch Manager server meets the requirements listed in the wizard, and click Next.

Patch Manager retrieves the list of available vendors and product catalogs.

> This process may require several minutes to complete.

When the synchronization process is completed, a list of available catalogs displays.
4. Click Next.

5. Select the vendors and specific products you want to synchronize with the Patch Manager server, and click Next.
6. Select the synchronization schedule settings that describe how often Patch Manager synchronizes your selected vendor catalogs and products.

![Synchronization Schedule](image.png)

7. Click Finish.
   Patch Manager updates the third party catalogs based on your synchronization settings.

**Configure the publishing servers**

To prevent errors when you publish software updates, run the Server Publishing Setup Wizard and generate the WSUS self-signed publishing certificate for the Patch Manager server certificate store. This process enables the WSUS server to publish third-party updates and custom packages to the managed systems.

If you installed SolarWinds Patch Manager on a dedicated server and chose not to allow the application to automatically deploy the SolarWinds WMI Providers, the Server Publishing Setup Wizard is disabled. Manually deploy the WMI Providers to the WSUS server or distribute the publishing certificate using the Group Policy. See [Configure the group policy to enable third-party updates](#) in the Patch Manager Getting Started Guide for details.

See [Manage Client WMI connectivity](#) for details about WMI connections.

See [Using Group Policy to Configure Managed Clients](#) if you need to use Group Policy to configure your publishing server. The Group Policy procedure is the same whether you are configuring publishing servers or managed clients.
Configure the WSUS upstream server

The upstream WSUS server publishes software updates to the managed systems. Perform the following procedure to create a signing certificate that establishes a chain of trust between the WSUS server and the managed systems.

1. Log in to the Patch Manager Administrator Console as an administrator.

2. In the navigation menu, expand Administration and Reporting and select Software Publishing.

3. In the Actions pane, click Server Publishing Setup Wizard.

4. In the wizard, click the WSUS Server drop-down menu and select the upstream WSUS server that requires a certificate.

   In this example, SPM-MGOM is the WSUS server added to Patch Manager.

5. Select Create self-signed certificate, and click Next.

   If the WSUS server is provisioned with a certificate, the wizard completes the remaining fields. Select Distribute existing WSUS signing certificate to required servers to distribute the certificate or click Close to end this procedure.

6. Select the WSUS server, and click Next.


8. In the Summary window, click Finish.

9. Review the information in the WSUS Client Certificate and GPO Management window, and click OK.

   The certificate is signed and distributed to the SolarWinds Patch Manager server and all managed servers in your deployment.

10. In the navigation menu, expand Enterprise > Update Services and select the WSUS server.
11. Click Refresh Update Server in the Actions pane.

   The certificate is signed and distributed to the SolarWinds Patch Manager server and all managed servers in the deployment.

12. Click Software Publishing Certificate in the Actions column to view the certificate.

Troubleshooting

If the Server Publishing Setup Wizard fails to create the self-signed certificate, see the following KB articles:

- [How to create a self-signed WSUS certificate when the Server Publishing Setup Wizard fails](#) (for WSUS 2012 and 2016)
- [Unable to create self-signed certificates on Windows 2012 R2 for remote WSUS](#) (for WSUS with Windows 2012 R2)

Set up and configure a WSUS downstream server

See [Add a downstream WSUS server to Patch Manager](#) for details about installing and configuring one or more downstream servers. After you configure the server, [push a publishing certificate to the server](#).

**Configure the Patch Manager email settings**

When you create tasks in Patch Manager, you can set up email notifications that notify you when the task is finished. To enable this option, configure the Application Server settings on the Patch Manager server. These settings define the email and Simple Mail Transfer Protocol (SMTP) server settings for email notifications sent from the Application Server.

When you are finished, [send a test email](#) to verify that the configuration settings are correct.

💡 If you configured an IBM Domino server as an SMTP server in your network, you can enable Patch Manager to email you when a task or synchronization is completed. See [Configure Domino Lotus Notes for SMTP](#) for details.

ℹ️ See [Application Server Settings](#) for additional details.

1. Gather the following information:
   - Name and email address of the user who receives task notifications
   - SMTP server hostname, port number, and password

2. In the navigation pane, expand Patch Manager System Configuration > Patch Manager Servers
and select Application Servers.

3. Select the Application Server in the top center pane.

4. Click the Application Server Settings tab.

5. In the Category column, click ☑ and select Email Configuration to filter the list.

6. Double-click Email Configuration: Sender e-mail Address.

7. Enter the sender e-mail address included in email notifications from the Application Server, and then click OK.

For example: danny.walker@example.com.
8. Double-click Email Configuration: Sender e-mail Name.

9. Enter the sender name included in the email notifications from the Application Server, and then click OK. 
   For example: Danny Walker.

10. Double-click Email Configuration: SMTP Server Name (Outgoing).

11. Enter the SMTP server host name used when sending email notifications from the Application Server, and then click OK.
   For example, outlook.office365.com.

12. Double-click Email Configuration: SMTP Server Port Number.
13. Enter the SMTP port number used when sending email notifications from the Application Server, and then click OK.

The default setting is port 25.


15. Select Enabled if the SMTP server requires authentication to send email. Otherwise, select Disabled, and then click OK.


17. Enter a user password for sending email notifications from the Application Server using an authenticated mail server, and then click OK.
18. Double-click Email Configuration: SMTP Server uses encrypted SSL connection.

19. Select Enabled if the SMTP server uses an encrypted Secure Socket Layer (SSL) connection. Otherwise, select Disabled, and then click OK.

20. Click Enable Configuration: SMTP Server uses encrypted TLS connection.

21. Select Enabled if the SMTP server uses an encrypted Transport Layer Security (TLS) connection. Otherwise, select Disabled, and then click OK.

22. Double-click Email Configuration: SMTP Server logon user name.

23. Enter the logon user name for sending email notifications from the Application Server using an
authenticated mail server, and then click OK.

For example, danny.walker@example.com.

24. Double-click Email Configuration: SMTP Server user logon domain.

25. Enter the user domain used when sending email notifications from the Application role server using an authenticated mail server, and then click OK.

26. In the lower center console, verify that your settings are correct.

Send a test email

After you set up your email configuration settings, send a test email to verify that Patch Manager can send notification email to your recipients.

1. In the Actions pane under Application Server Settings, click Email Configuration Test.

2. In the Recipient field, enter the email address of a notification recipient, and click Add.
3. Repeat step 2 for each additional email recipient.

4. Click OK.

If the email settings were not set up correctly, an error message displays on your screen. Read the message and make the appropriate changes.

5. Verify that these individuals received the notification email.

**Configure the administrative settings**

Depending on your environment and how you plan to use Patch Manager, you can:

- **Configure your proxy settings** if your organization uses a proxy server to connect to the Internet.
- **Create a third party updates view** to separate third party updates from the Microsoft updates you normally see in your WSUS console.

These procedures are optional.

**Configure the proxy settings**

Both the Patch Manager Administrator Console and Application 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 dialog boxes.
Configure the console proxy settings

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

1. In the navigation menu, select Administration and Reporting.
2. In the center pane, click General Settings > Proxy Configuration.
3. In the Console Proxy Settings window, select Use a proxy server while synchronizing.

4. Complete the remaining options based on your environment.
5. Click OK.
Configure the server proxy settings

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

💡 You can use an Active Directory account for the EminentWare Data Grid Server Service. If you change the server proxy settings for this configuration, you may need to update the GPOs applied to the Active Directory service account, stop the service, and clear the user’s Windows profile.

1. In the navigation menu, expand Administration and Reporting and select Software Publishing.
2. In the Actions pane, click Synchronization Settings.
3. In the Third Party Update Options window, click the Proxy Settings tab.
4. Select Use a proxy server when synchronizing.
5. Complete the remaining selections for your environment.
6. Click OK.
Create a third party updates view

You can use Patch Manager to publish, manage, and deploy third party updates from the Patch Manager server. Create a third party updates view in the Patch Manager Administrator Console to separate these types of updates from the Microsoft updates you normally see in your WSUS console.

If you installed Patch Manager on SCCM, see Create a third-party updates view for SCCM.

1. In the navigation menu, expand Enterprise > Update Services, and then expand your WSUS server.
2. Select Updates and click New Update View in the Actions menu.
3. In the Step 1 panel, select one or both of the following options:
   - Updates have a specific approval and installation status
   - Updates are from Microsoft Update, Third Parties, or both

4. In the Step 2 panel, define the properties.
   a. Select any update source.

b. In the Updated Sources dialog box, click Only updates from a third party, and click OK.
c. In the step 2 panel, click approved and needed.

d. In the Updates View Filter, click the Approved State drop-down menu and select All.

e. In the Update Status menu, select Any, and click OK.

5. In the step 3 panel, enter a name and description for the new view, and click OK.
Configure the managed clients

You can provision the WSUS publishing certificate to all clients you want to manage by configuring clients using:

- **Group Policy** (recommended)
- **Patch Manager Console**

When you are finished, configure the clients to accept updates from the Patch Manager server.

Configure clients using Group Policy

To avoid using WMI connections required by the Client Publishing Setup Wizard, configure the clients using your Group Policy by exporting the WSUS certificate to a file. When you are finished, configure the Group Policy object, and then push the file to your managed clients. You can also deploy certificates using the Group Policy.

Export the WSUS certificate

Perform the following procedure to export the WSUS publishing certificate to a file from the Patch Manager Administrator Console.

1. Open the Patch Manager Admin Console.
2. In the navigation menu, expand Enterprise > Update Services.
3. Select the WSUS server to export the certificate.
4. In the Actions pane, click Software Publishing Certificate to display the Publishing Certificate Information window.

If the window does not display the WSUS server certificate information:
   a. Click Close.
   b. Click Refresh Update Server in the Actions pane.
   c. Click Software Publishing Certificate in the Actions pane.

5. Click [...].

6. In the Certificate window, click the Details tab.
7. Click Copy to File, and click Next.

8. In the Certificate Export Wizard, click Next.

9. Select DER encoded binary X.509 (.CER), and click Next.

10. Enter a file name, and click Next.

11. Click Finish, and then click OK.

Configure the Group Policy Object

Use the following procedure to configure the Group Policy Object (GPO) and push to your managed clients in your Microsoft® Windows® domain.

The GPO stores the WSUS certificate in the certificate stores and configures the managed clients to accept third-party updates from non-Microsoft sources.

1. Using an account with administrator privileges, open Administrative Tools and click Edit group policy.

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 the Success dialog box.
   i. Repeat these steps for the Trusted Publishers certificate store.


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.

Deploy certificates using Group Policy

You can deploy a certificate to multiple computers using Active Directory Domain Services and the GPO. Use this method each time you need to push a certificate to your client computers.

For example, you can push a WSUS self-signed or CA-signed certificate to all clients before they can trust a publish third-party package.

1. Verify that you are a member of the local administrator group (or equivalent).
2. Open the Group Policy Management Console.
3. Locate an existing GPO or create a GPO that contains the certificate settings. Ensure that the GPO is associated with the domain, site, or organizational unit that includes the users you want to include in the policy.

4. Right-click the GPO and select Edit.

   The Group Policy Management Editor opens and display the current policy object contents.


6. Click the Action menu and select Import.

7. Complete the Certificate Import Wizard to locate and import the certificate.

8. If the certificate is signed and cannot be tracked back to a certificate in the Trusted Root Certification Authorities certificate store, copy the certificate to the store.
   a. In the navigation pane, click Trusted Root Certification Authorities.
   b. Complete step 6 through step 7 to install a copy of the certificate to the store.

**Configure clients using the Patch Manager Administrator Console**

SolarWinds WMI Providers provide additional management and inventory tools that interface with Windows Server Update Services (WSUS) and your managed clients. If you provisioned your managed clients with the SolarWinds WMI Providers, run Client Certificate Management in the Patch Manager Administrator Console to enable your clients to receive third-party updates from Patch Manager.

When you are finished, Patch Manager prompts you to configure the Windows Update Group Policy on your managed clients to enable each client to allow third-party updates from Patch Manager. Based on your corporate IT policy, enable the requisite policy in Group Policy.

**Run Client Certificate Management**

Run the Client Certificate Management task to distribute and install the WSUS self-signed publishing certificate to your managed clients.

1. In the navigation pane, select Administration and Reporting.

2. In the Administrative Tasks pane, click Client Certificate Management.
3. In the Client Certificate Management window, select the WSUS publishing certificate you want to distribute to the managed clients.

   a. Select the Distribute and install Update Services Signing Certificate check box.

   b. Choose whether to distribute the certificate directly from the WSUS server or a CER file. To distribute the certificate directly from the WSUS server, choose Select certificate from WSUS server, and then select the WSUS server from the drop-down menu.

   To distribute the certificate from a CER file, choose 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 check box.

      b. Next to the File Name field, browse to the file location.

4. Click Distribute.

5. Complete the Task Options Wizard to specify the target systems and schedule or execute the task. See Task Options Wizard for additional information.
Configure the Windows Update Local Policy on systems not managed by a GPO

Use this procedure to configure the Windows Update local policy on your managed systems so they can access the WSUS server and download updates. This procedure applies to systems that are not managed by a group policy (GPO).

1. Log in to Patch Manager as an administrator.
2. In the navigation pane, locate and select a system that needs access to the WSUS server and third party updates.
3. In the Actions pane, click Windows Update Local Policy Management.
4. In the window, enable the following settings:
   - Specify intranet Microsoft update service location
     This option indicates the targeted WSUS server.
   - Allow signed content from intranet Microsoft update service location
     This option enabled third-party updates.
   - (Optional) Configure Automatic updates.
     This option enables the system to update automatically by policy.
5. Click Save to save the template.
6. Click OK.
7. Schedule the task or run it now.
Publish third-party updates

Patch Manager leverages WSUS to deploy and manage Microsoft® and third-party applications to workstations and servers in a corporate network.

See Publishing Trial Updates to publish specific updates.

See Set up Patch Manager with SCCM to publish third-party updates using SCCM.

Manage the publishing servers

Use the Server Publishing Setup Wizard to view the current WSUS certificate and create a self-signed certificate, or use an existing certificate to enable custom package publishing. If the certificate is installed on the server, the wizard determines the publishing certificate status with server resources associated with that WSUS server.

1. In the navigation menu, expand Administration and Reporting and select Software Publishing.

2. In the Actions pane, click Server Publishing Setup Wizard.

3. In the Configure dialog box, click the WSUS Server drop-down menu and select a WSUS server.

   If the WSUS server does not have a publishing certificate, the Configure box generates an error message.

   If the WSUS server has a publishing certificate, the Configure dialog box displays the certificate information.
4. Select a certificate option, and click Next.

5. Complete the Server Publishing Setup Wizard to create or deploy publishing certificates as required.

**Import and export catalogs**

You can import and export package catalogs to move software publishing catalogs between Patch Manager servers.

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.
Use the Export Catalog Wizard to export one or more packages into a portable catalog (CAB) file you can import into a Patch Manager server, System Center Updates Publisher, or any other product that complies with the Microsoft package and catalog specifications. You can export the entire library of packages or selected packages into a catalog file.

**Import catalogs**

Perform the following steps to import packages from a portable catalog (.cab) file.

1. Log in to the Patch Manager Administrator Console.
2. In the navigation pane, expand Administration and Reporting and select Software Publishing.
3. In the Actions pane click Import Catalog.
4. In the Import Catalog Wizard, click [...] select the catalog file (.cab) you want to import, and click Next.
5. Select the package you want to import, and click Next.
6. Review the import results, and click Finish.

**Export catalogs**

Perform the following steps to export selected packages or the entire package library to a catalog (.cab) file.

1. Log in to the Patch Manager Administrator Console.
2. In the navigation pane, expand Administration and Reporting > Software Publishing.
3. Select a publishing container (such as Adobe Packages) in the Software Publishing node.
4. Select one or more packages in the center pane.

You can export specific packages based on your selection, or all packages regardless of your selection. Press <Ctrl> to select multiple packages.

5. Click Export Catalog in the Actions pane.

6. In the Export Catalog Wizard, select the export options, and click Next.

   ![Export Catalog Wizard](image)

   - To export all installers and other files you downloaded for the packages you are exporting, select Include download package content when exporting.
   - If you selected one or more packages to export, select Export the selected software packages to a cabinet file that can be imported by other publishers.
   - To export all packages in your library, select Export all software packages to a cabinet file that can be imported by other publishers.

7. Review the export results, and click Finish.

Create and publish software packages

Use Patch Manager to create and publish custom software packages to the SolarWinds third-party updates library on your WSUS server. These packages can be distributed to your managed computers in your Patch Manager deployment.
Create software packages

Use the Package Wizard to create and edit a package definition—an XML file that defines the attributes and behavior of an update package. Use the Package Wizard to view or define:

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

SolarWinds does not provide support for custom code or software packages created by third-party sources. See the Patch Manager Product Forum on THWACK for help with custom packages.

Open the Package Wizard

1. Log in to the Patch Manager Administrator Console.
2. In the navigation pane, expand Administration and Reporting > Software Publishing.
3. Complete the Patch Manager Package Wizard.

Create a package

1. Select any container in the Software Publishing node.
2. In the Actions pane, click New Package.

View the package details

1. Select the container that contains the package you want to view.
2. In the center pane, select the package.
3. In the Actions pane, click Edit.
4. When you are finished, complete the Patch Manager Package Wizard.
Complete the Package Wizard

This section describes how to complete the Patch Manager Package Wizard. See Manage software package rule sets for details about adding prerequisite, applicability, and installed rules in the wizard.

1. On the Enter or modify the package information page, enter the package metadata, and click Next.

See Define the package metadata for field descriptions.

2. On the Prerequisite Rules screen, add or modify rules to define whether a target computer should evaluate the update based on the hardware or software attributes, and click Next.

See Prerequisite rule set for details.
3. On the Select Package page, specify the source of the package contents, and then click Next.

See [Define the package source](#) for details.

4. On the Applicability Rules page, add or modify rules to indicate if the update applies to the target computers, and then click Next.

See [Applicability rule set](#) for details.

5. On the Installed Rules page, add or modify rules to determine if the update is installed on the target computer, and then click Next.
See Installed rule set for details.

6. On the Summary page, verify your package settings, and click Save.

Define the package metadata

The following table describes the fields on the Enter or modify the package information page located in the Package Wizard.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package Title (required)</td>
<td>The text string displayed in the update listing of the administrative console and the header of the update details. Enter a text string using up to 80 characters.</td>
</tr>
<tr>
<td>Description (required)</td>
<td>Provides an update description.</td>
</tr>
<tr>
<td>Classification (required)</td>
<td>A pre-defined value that describes the update type. Microsoft defines these options.</td>
</tr>
<tr>
<td>Bulletin ID</td>
<td>The ID assigned to a Microsoft Security Response Center Security Bulletin. This field can also store a bulletin ID published by other vendors. For non-security updates, this field is blank.</td>
</tr>
<tr>
<td>Vendor (required)</td>
<td>The vendor who created the update.</td>
</tr>
<tr>
<td>Product (required)</td>
<td>The product name that applies to the update.</td>
</tr>
<tr>
<td>Article ID</td>
<td>The Microsoft Knowledge Base article ID number. This field can store a similar value for updates published by other vendors.</td>
</tr>
<tr>
<td>CVE ID</td>
<td>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.</td>
</tr>
<tr>
<td>Severity</td>
<td>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.</td>
</tr>
<tr>
<td>Support URL</td>
<td>The URL that links to the vendor support site for this update.</td>
</tr>
<tr>
<td>More Info URL</td>
<td>The URL for additional information about the update.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Impact (required)</td>
<td>Designates the impact on the target computer. Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Normal. An update that does not require user intervention.</td>
</tr>
<tr>
<td></td>
<td>• Minor. An update that does not require a system restart. Minor updates use the Allow automatic updates immediate installation setting in the Windows Update Agent to determine if the update can be installed immediately or after a scheduled event.</td>
</tr>
<tr>
<td></td>
<td>• Requires exclusive handling. An update that must be installed by itself, outside of a batch of other updates. This update includes operating system service packs, .NET Framework service packs, redistributables, and updates to the Component-Based Servicing Stack.</td>
</tr>
<tr>
<td></td>
<td>• Reboot Behavior. Describes how the target computer should behave after the update. Select Can request reboot if a reboot is required, but not necessary. Otherwise, select Never reboots or Always requires reboot based on vendor requirements.</td>
</tr>
</tbody>
</table>

Define the package source

The following table describes the fields in on the Select Package page of the Package Wizard.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The package file extension. Select EXE, MSI, or MSP.</td>
</tr>
<tr>
<td></td>
<td>EXE is a file extension for files that contains a program you can execute on a computer. You can run an executable file in Microsoft DOS or Windows using a command or double-clicking the file.</td>
</tr>
<tr>
<td></td>
<td>MSI files install computer code, whereas EXE files can be any file that runs on a Windows computer.</td>
</tr>
<tr>
<td></td>
<td>MSP is a file extension for a Windows Installer patch file used by Windows and Microsoft programs. Files with this extension usually install a bug fix, security update, or hotfix. Most Windows patches are sent as .MSP files. This extension is also used for Microsoft Paint bitmap files.</td>
</tr>
<tr>
<td>I do not have the package content</td>
<td>Specifies the URL to a web-based or FTP-based download location. Enter the URL for the installer in the Download URL field. This field does not accept forwarding links.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>I already have the content for the package locally on my network</td>
<td>Specifies the name and location of downloaded content. Enter the package filename in the Package field and the web-based, FTP-based, or UNC file path in the Download URL field.</td>
</tr>
<tr>
<td>Use the Package Boot Helper program when performing installation of the software</td>
<td>Activates the Package Boot Editor so you can define additional files and behavior for the installer. See <a href="#">Using PackageBoot</a> for details.</td>
</tr>
<tr>
<td>Include additional files with the package</td>
<td>Activates the Package Content Editor so you can define additional files to accompany the installer.</td>
</tr>
<tr>
<td>Binary Language</td>
<td>The language required by the update. If the update is not language-specific, select None.</td>
</tr>
<tr>
<td>Success Return Codes</td>
<td>The package return codes. Separate multiple codes with commas.</td>
</tr>
<tr>
<td>Success Pending Reboot Codes</td>
<td>The package reboot codes. Separate multiple codes with commas.</td>
</tr>
<tr>
<td>Command Line (silent install)</td>
<td>Additional arguments to support the unattended installation.</td>
</tr>
</tbody>
</table>

**Using PackageBoot**

PackageBoot is a utility that adds specific actions before and after an update. For example, a locked file can generate issues with a silent installation and require a reboot.

**Use PackageBoot to:**

- Verify that files overwritten during the installation procedure are unlocked
- Stop and start services before and after the installation
- Execute programs (MSI or EXE) before or after the installation
- Terminate processes before the installation

The Package Boot Editor creates two files to include in the update package:

- PackageBoot.EXE
- PackageBoot.XML

Both files are published with the installer to the WSUS server and downloaded to the target computer. The **PackageBoot.XML** file provides the specifications for activities and tasks executed by the Windows Update Agent.
Complete the Package Boot Editor

1. In the Select Package screen, open the Package Boot Editor.

2. In the Before applying package screen, select the actions to run prior to installing the update. For example, stop a service, run a program, or terminate a process.

3. In the After applying package screen, select the actions to run after installing the update. For example, run a program or start a service.

4. In the right pane, enter the action details.

5. Click Save to save the PackageBoot.XML configuration file.

The following table describes additional options in the Package Boot Editor screen.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td>Import a PackageBoot.XML file from a local or network location.</td>
</tr>
<tr>
<td>View XML</td>
<td>Display the PackageBoot.XML configuration file generated by the Package Boot Editor.</td>
</tr>
<tr>
<td>Add Action</td>
<td>Select an action to add to the active section of the editor.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the selected action.</td>
</tr>
<tr>
<td>Duplicate</td>
<td>Duplicate the selected action.</td>
</tr>
<tr>
<td>Move Up</td>
<td>Move the selected action one position higher.</td>
</tr>
<tr>
<td>Move Down</td>
<td>Move the selected action one position lower.</td>
</tr>
</tbody>
</table>

Manage software package rule sets

WSUS uses software publishing rules to evaluate if a package is installed and can be deployed to a specific client. This section describes each type of software publishing rule set and provides a corresponding example.

For additional information about these rule sets, see the following articles on THWACK:

- [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](#)
The Rule Editor is the same regardless of the rule type or 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 Administrator Console.

Prerequisite rule set

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

See the Microsoft TechNet website to identify the specific version for your Windows Server operating system.

For example, to add a rule to include only workstations running Windows Server 2008:

1. Expand Administration and Reporting > Software Publishing and select Rules.
2. In the center pane, double-click a rule.
3. In the Rule Editor dialog box, select Create Basic Rule.
4. Click the Rule Type drop-down menu and select Windows Version.
5. Complete the Windows Version tab options.
a. Click the Rule Type drop-down menu and select Windows Version.

b. In the Comparison field, select Greater Than or Equal To.

c. In the Major Version field, select 6.

d. In the Minor Version field, select 0.

e. In the SP Major Version field, select 1.

f. In the SP Minor Version field, select 0.

g. In the Product Type field, select Server.

6. Click OK.

Applicability rule set

Common applicability rules check to see whether certain registry keys or values exist on the target computer. Generally, applicability ruleset works together with the installed rule set to define whether or not a target computer requires the update.

The 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 version, and the installed rule is checking for the existence of the same version. As a result, the two rule sets combined determine whether the update is required.

For example, to add a rule to check whether the Firefox version is 10.0 or earlier.

1. Expand Administration and Reporting > Software Publishing and select Rules.

2. In the Rule Editor window, select Create Basic Rule.
3. Click the Rule Type drop-down menu and select File Version with Registry Value.


   a. In the Registry Key field, enter:
      
      `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\firefox.exe`

   b. In the Registry Value field, enter Path, and then select Use 32-bit registry.

   c. In the Sub-path field, enter `firefox.exe`.

   d. In the Comparison field, select Less Than.

   e. In the Version field, enter `10.0.0.441`. 
5. Click OK.

Installed rule set

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 rule set to define whether or not a target computer requires the update.

For example, to add a rule to check whether the Firefox version is 10.0 or earlier.

1. In the Rule Editor window, select Create Basic Rule.

2. In the center pane, double-click a rule.

3. In the Rule Type field, select File Version with Registry Value.


   - **Registry Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion
   - **Registry Value:** Path, Use 32-bit registry
   - **Sub-path:** firefox.exe
   - **Comparison:** Equal To
   - **Version:** 10.0.0.441
a. In the Registry Key field, enter:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\firefox.exe
```

b. In the Registry Value field, enter Path, and then select Use 32-bit registry.

c. In the Sub-path field, enter `firefox.exe`.

d. In the Comparison field, select Equal To.

e. In the Version field, enter `10.0.0.441`.

5. Click OK.

### Publish custom software packages

The Patch Manager Publishing Wizard allows you to publish software packages to the WSUS server. Using the wizard, you can publish:

- Entire packages (including all metadata and installers)
- Metadata-only packages used to determine if a package is installed or required on target computers
- Revision-only packages that update an existing package metadata and not the installation file

Below is an example of the Patch Manager Publishing Wizard dialog box.
The following table describes the options in the wizard.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSUS Server</td>
<td>WSUS Server that stores the published packages.</td>
</tr>
<tr>
<td>Verify WSUS version compatibility and required signing certificate is distributed</td>
<td>Checks the versions and certificates in the publishing environment to ensure the publishing process is successful. WSUS requires all publishing environment components to run the same operating system, WSUS version, and publishing certificate to prevent API Mismatch errors.</td>
</tr>
<tr>
<td>Re-sign existing selected packages</td>
<td>Re-signs the selected packages with the current publishing certificate. Use this option when republishing packages that were previously signed by an earlier publishing certificate.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Delete package if it exists (select this if binaries have</td>
<td>Installs new binary files in the selected packages. This option allows you to reuse an existing package definition.</td>
</tr>
<tr>
<td>changed)</td>
<td></td>
</tr>
<tr>
<td>Re-download packages that have already been downloaded</td>
<td>Downloads the binary content for all packages, even if the content is already on the Patch Manager server. Use this option to ensure the content you publish to the WSUS server is the same as the content available from the vendor update publishing site.</td>
</tr>
</tbody>
</table>

### Publish the packages to a WSUS server

After you publish the software packages, you can download and install the packages on your managed systems.

1. Log in to Patch Manager as an administrator.
2. In the navigation pane, expand Administration and Reporting > Software Publishing and select the container that contains one or more packages you want to publish. For example, SolarWinds, Inc. Packages
3. In the Actions pane, click Publish Packages.
   a. Select the WSUS Server drop-down menu and select the WSUS server that will publish the packages.
   
   The wizard cannot publish packages to replica servers.
   b. Select an option as your initial selection method.
      - Select Publish selected packages to the WSUS server to start with only the packages you selected before launching the wizard.
      - Select Publish all packages to the WSUS Server to start with all available and selected packages. You can clear or modify these selections in the following step.
   c. Review the available packages and select the check box next to each package you want to publish. Clear the check box next to each package you do not want to publish.
   d. In the Content column for each selected package, select the Full, Metadata Only, or Revision Only version for publishing.
   e. Above the package selection pane, select any additional options, and click Next.
The selected package is downloaded to the WSUS server.

5. If you do not need to download any additional content, go to step 6.

If you need to download any additional content, use the Package Download Assistant to download and import the content for packages that do not include the download links.

After the Wizard completes the download, select each package you want to publish, and click Next.

See Complete the Package Download Assistant Wizard.

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

Complete the Package Download Assistant Wizard

Some software vendors (such as Oracle and Adobe) require you to accept a License Agreement before you can download and distribute a software package to your managed computers. When this occurs, the Patch Manager Publishing Wizard opens the Package Download Assistant Wizard and directs you to the vendor website. Here, you can accept the License Agreement, download the software package, and complete the options in the Patch Manager Publishing Wizard.

1. In the Package Download Assistant window, select a package.

2. Double-click the link below the package list.

3. In the vendor download page, review the License Agreement. If you agree, accept the License Agreement.

4. Download the file or archive for your selected package.

5. In 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.

6. Click Import Source.
7. Navigate to the folder that contains the downloaded file and click Open.

   The wizard pre-populates the Select the download file package dialog box with the required file name. You do not need to select or specify a file during this step, except for the folder.

8. Repeat step 2 through step 6 for any other packages listed in the wizard.

9. Click OK.


**Manage third-party packages**

After you create a package, select the package in the Patch Manager Administrator Console to view detailed information about the package. After you select a package, you can:

- View the package details
- Verify the package integrity
- Check the package publication status

View the package details

When you expand Administration and Reporting > Software Publishing, you can select the vendor package group (such as Adobe Packages) and then select the specific package in the center console.

<table>
<thead>
<tr>
<th>Name</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flash Player 22.0.0.192 Plugin MSI (metadataonly)</td>
<td>Adobe</td>
</tr>
<tr>
<td>Flash Player 27.0.0.187 PPAPI MSI (Upgrade)</td>
<td>Adobe</td>
</tr>
<tr>
<td>Flash Player 27.0.0.187 PPAPI MSI</td>
<td>Adobe</td>
</tr>
<tr>
<td>Flash Player 27.0.0.187 PPAPI EXE (Upgrade)</td>
<td>Adobe</td>
</tr>
<tr>
<td>Flash Player 27.0.0.187 PPAPI EXE</td>
<td>Adobe</td>
</tr>
<tr>
<td>Flash Player 27.0.0.187 Plugin MSI (Upgrade)</td>
<td>Adobe</td>
</tr>
<tr>
<td>Flash Player 27.0.0.187 Plugin MSI</td>
<td>Adobe</td>
</tr>
</tbody>
</table>

When you select a package, tabs display at the bottom of the console that provides details about the package.

The following table describes each tab.
<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package Details</td>
<td>Displays the package description and metadata. Similar to the Update Details tab for WSUS updates.</td>
</tr>
<tr>
<td>Prerequisite Rules</td>
<td>Displays the package prerequisite rules. These rules typically apply to the machine and the operating system.</td>
</tr>
<tr>
<td>Applicability Rules</td>
<td>Displays the package applicability rules. If the package is new, these rules determine if the package is currently installed. If the package is an upgrade, these rules check for a previous version.</td>
</tr>
<tr>
<td>Installed Rules</td>
<td>Displays the package installed rules. When the machine checks in with WSUS for the latest updates, these rules verify if the software is currently installed.</td>
</tr>
<tr>
<td>Content</td>
<td>Displays the package contents.</td>
</tr>
<tr>
<td>Version History</td>
<td>Displays the dates and changes to the package.</td>
</tr>
</tbody>
</table>

**Verify the package integrity**

The Package Integrity Verification action allows you to verify the package contents prior to publishing. The action compares the contents in the current package to what is currently available from the vendor.

This action allows you to:

- Calculate the Secure Hash Algorithm 1 (SHA-1) hash of the downloaded file and compare it to the calculated SHA-1 obtained when the package was created.
- Identify 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 defined files.
- Provide a repair option to correct any repairable conditions.

To check the integrity of one or more downloaded packages:

1. In the navigation pane, expand Administration and Reporting > Software Publishing.
2. Select a package group (such as Adobe Packages).
3. Select a package in the center console.
4. In the Actions pane, click Package Integrity Verification.

   If the wizard displays a package without a green checkmark in the left column, click Repair to repair the package.
5. Click Close to exit the window.

Check the package publication status

The Run Check Publication Status action allows you to determine if a package was published to the WSUS server.

1. In the navigation pane, expand Administration and Reporting > Software Publishing.
2. Select a package group (such as Adobe Packages).
3. Select a package in the center console.
4. In the Actions pane, click Check Publication Status.
5. On the Package Publication Status Wizard, select the WSUS servers to check the publication status of your selected packages, and click Next.

6. Review the results of the check, and click Close.

Auto-publish third party updates to WSUS

The Auto-Publishing of Third Party Updates to WSUS action displays in the Actions menu when you expand Administration and Reporting > Software Publishing and select a software package. This action allows you to automatically publish non-Microsoft updates to the WSUS server based on a daily, weekly, or monthly schedule.

When the task is completed, you can enable the task to export the results to a supported file format and email the file to one or more recipients.
1. In the navigation pane, expand Administration and Reporting and select Software Publishing.

![Diagram showing navigation pane with Software Publishing selected]

2. In the Actions pane, click Auto-Publishing of 3rd Party Updates to WSUS.

3. Select the WSUS servers that will host the third party updates.

![Image showing Set Scope of Auto-Publishing window with SPM-MGOM selected]

---

Page 91
4. Select the products you want to publish to the WSUS server, and click Next.

For safety reasons, license conditions, and efficiency, auto-publishing skips driver-based packages and updates without a direct link to an executable file, marked as metadata only, marked as expired, and created by a user.

5. Click Next. Patch Manager verifies the WSUS server.

6. Enter a task name and description.
7. Select the auto-publishing schedule options.

To disable this option, select Disable auto-publishing and go to the next step.

To enable auto publishing and publish now, select Auto-publish now and go to the next step.

To enable auto publishing and set up a schedule:

a. Select Schedule the task to run daily, weekly, monthly and click Configure.

b. In the Scheduled Time panel, enter a start time and date.

c. In Recurrence Pattern, select an hourly, daily, weekly, or monthly value.

d. In Range of recurrence, select whether you want the task to continue without end or end
at a specific time.

![Range of recurrence](image)
e. Click OK.

8. Choose whether to export the task results to a file (such as a Microsoft® Excel®, XML, or CSV file).

![Export Results](image)

9. Choose whether to culminate the task results into an output file (such as Microsoft Excel) and send the file to one or more recipients. Click Configure to set up the notifications and file format.

![Email Notifications](image)

10. Click Next.

11. Review the information in the Task Summary window, and click Finish.

**Update the scheduled auto-publish task**

Repeat the steps in the previous section to update your task settings.

**Delete the scheduled auto-publish task**

1. Expand Administration and Reporting and select Scheduled Tasks.

2. In the center pane, select the task you want to delete.

3. In the Actions pane, click Delete.
Push, approve, and install third party updates

Patch Manager provides automated patching (or updates) for third-party applications and Microsoft® servers and workstations. Using the Patch Manager Administrator Console, you can push the updates to the managed systems, approve the updates, and then install the updates on the managed systems.

The Approve updates and Install the updates sections do not apply to SCCM (or ConfigMgr) environments. If you use SCCM to manage your updates, use the SCCM methods to deploy the updates you publish using Patch Manager. See Set up Patch Manager with SCCM for details.

Push the updates

Besides operating system updates for your Microsoft systems, you can push third-party update packages from the WSUS server to the client systems. These packages include updates for Adobe Reader, Java Runtime, and Adobe Flash.

This section provides examples on how to push, approve, and install these third-party update packages to your managed systems.

See Set up Patch Manager with SCCM for SCCM instructions.

Push Adobe Reader updates

Use the Publishing Wizard to download Adobe® Reader update packages and publish the installation file and update definition to the WSUS server.

1. Log in to the Patch Manager Administrator Console as an administrator.
2. In the navigation pane, expand Administration and Reporting > Software Publishing.

4. In the center pane, select the update package you want to publish.

   The Package Details tab displays important information about the update. The remaining tabs provide additional information, including prerequisite rules and version history.

5. In the Actions pane, click Publish Packages.

6. Review the selections in the Patch Manager Publishing Wizard.

7. Click Next.

   The Patch Manager Publishing Wizard downloads the selected packages.

   This process may take several minutes to complete.

8. When the download is completed, click Next.

   This process may take several minutes to complete.

9. In the Patch Manager Summary window, click Finish.

   The selected software packages are published to the WSUS server.
Push Java Runtime environment updates

Check out this video (4:06) for an introduction on Patching Java and preventing failed updates.

Use the Package Download Assistant to download the Java Runtime Environment update files from the Oracle® Java® Downloads website. When you are finished, copy the installation file and update definition to the WSUS server.

If you need to update the Java software on your managed systems, see How to uninstall previous Java 8 versions using Patch Manager before you apply the new package on the target systems.

1. In the Patch Manager menu, 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.

The Package Details tab displays important information about the update. The remaining tabs provide additional information, including prerequisite rules and version history.

4. In the Actions pane, click Download Content.

5. Click OK in the Download Assistant dialog box.

6. In the Package Download Assistant window, double-click the download link to access the Oracle Java download site.

Patch Manager opens a web browser and navigates to the Oracle website.

7. If you accept the License Agreement, select Accept License Agreement.
8. Locate the following product files:
   - Windows x86 Offline
   - Windows x64

9. Download the files.

   🔄 This process may take several minutes.

10. When the download is completed, close the browser window.

11. Return to the Package Download Assistant window.

12. Click Import Source.

13. Browse to the folder that contains the imported file.

14. Select the file, and click Open to import the file.

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

   Patch Manager imports the file.

   ![Import Source Table]

   When the import is finished, the Status column displays **Completed**.

15. Click OK.

16. In the Actions pane, click Refresh to view the imported files.

17. Repeat step 3 through step 16 for any additional updates.

18. In the Actions pane, click Publish Packages.

19. Click Next.

20. Click Finish.
Push Adobe Flash updates

Use the Package Download Assistant to download the Adobe Flash update files. When you are finished, use the Publishing Wizard to copy the installation file and update definition to the WSUS server.

See [Download archived versions of Adobe Flash](#) if you need a previous version.

1. In the Patch Manager menu, expand Administration and Reporting > Software Publishing.

2. Select Adobe Packages.

3. In the center pane, select the Flash Player package you want to publish.

   The Package Details tab displays important information about the update. The remaining tabs provide additional information, including prerequisite rules and version history.

4. In the Actions pane, click Download Content.

5. Click OK in the Download Assistant dialog box.

6. In the Package Download Assistant window, double-click the download link to access the Adobe Flash Player distribution site.


   Patch Manager opens a web browser and navigates to the Adobe website.

7. Apply for a license to distribute Flash Player.

8. Download the archive for the version you want to publish.

9. When the download is completed, close the browser window.

10. Return to the Package Download Assistant window.
11. Click Import Source.

12. Browse to the folder that contains the imported file.

13. Select the file, and click Open to import the file.

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

14. Extract the contents of the archive to your local computer.

15. Return to the Package Download Assistant window, and then click Import Source.

16. Browse to the folder that contains the file you want to import, and then click Open.

   - 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.

17. Click OK.

18. In the Actions pane, click Refresh to view the imported files.

19. Repeat step 3 through step 18 for any additional updates.

20. In the Actions pane, click Publish Packages.

21. Click Next.

22. Click Finish.

**Approve the updates**

- This section does not apply to SCCM environments. If you use SCCM to manage your updates, use the SCCM console to deploy the updates you publish using Patch Manager. See [Set up Patch Manager with SCCM](#) for details.

When you approve an update, WSUS pushes the update to the targeted group—for example, the Finance Department in your organization. When each computer in the group checks in with the WSUS server, the server installs the update on the computer.

Before you approve the updates for the targeted group, be sure to:
Avoid changing the Applicability and Prerequisite rules in the update packages. This ensures that the targeted group receives the updates.

Approve and test the update packages on a test system. This ensures that the software operates as expected and does not conflict with any other installed software application.

Avoid enabling automatic approvals on the WSUS server. This helps you maintain approval control using Patch Manager.

After you push the updates you want to evaluate, approve the update for the appropriate WSUS target groups.

1. In the Patch Manager menu, expand Enterprise > Update Services > Your WSUS Server > Updates.

2. Select Third Party Updates.

3. In the center pane, select one or more update packages.

   The Update Details tab displays additional information about the update, including installation status.

4. In the Actions pane, click Approve.

   If the console generates an error when you approve the updates, see this KB article.

5. In the Approve Updates window, select the targeted WSUS computer group. Press <Ctrl> to select multiple groups.

6. Click Approved for Install.

7. Click OK to push the approval to the WSUS server database or click Schedule to create a
schedule for the update.

8. In the Approval Progress window, click Close.

Install the updates using Update Management

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

Use the Update Management task to push updates on a WSUS server to 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.

An exclusive update is an update that must be installed individually, outside of a batch of other updates. This typically includes updates such as operating system service packs, .NET Framework service packs and redistributables, and updates to the Component-based Servicing Stack.

1. Use the Patch Manager Publishing Wizard to publish one or more packages to a WSUS server.

2. In the navigation pane, expand Enterprise > Update Services > Your WSUS Server > Updates.

3. Select Third Party Updates.

   If you have not created this view, see Creating a third-party updates view.

4. In the center pane, select an update.

5. In the Actions pane, click Update Management.

6. In the Update Management window, select any additional options, and then click OK.
For example, you can create PowerShell scripts for your third-party updates and push the scripts with your updates.

7. In the Task Options Wizard, select your targeted systems.
   a. Click Browse Computers.
   b. Locate and select the targeted systems or groups.
   c. Click Next.

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

9. Click Finish.

Create PowerShell scripts for third-party updates

Beginning in Patch Manager 2.1.6, you can create PowerShell scripts that execute as part of an Update Management task—both before and after the task completes. Using Update Management or the Update Management Wizard, you can push updates with PowerShell scripts to your managed systems that perform the following tasks:

- Create a VM snapshot prior to an update task
- Revert to a snapshot if an issue occurs
- Stop services in a specific order
- Fail over machines
- Mute alerts from Orion Platform nodes during update tasks

See the Microsoft Docs website at https://docs.microsoft.com for details about how to write and run scripts in the Windows PowerShell ISE.

⚠️ The PowerShell script functionality applies to devices connected to WMI and does not apply to Patch Manager Agents. If a managed client is included in the target scope, the task for that agent will fail.

⚠️ Review and evaluate how Windows PowerShell scripts are incorporated in your environment. This includes importing scripts from third parties, including content posted by customers in the THWACK online community. To prevent unauthorized access to computers in your network, SolarWinds recommends using a dedicated Windows account with low-level privileges to create and review PowerShell scripts.

About Windows PowerShell

Microsoft Windows PowerShell is a task automation and configuration management framework that consists of a command-line shell and associated scripting language.
PowerShell is built on top of the .NET Framework Common Language Runtime (CLR) and the .NET Framework, and accepts and returns .NET Framework objects. This means you can get the information you need almost instantly using PowerShell—if you know how to ask for it. PowerShell is included with .NET Framework 4.0 and later and can be accessed from within the Windows Server operating system.

PowerShell includes built-in commands with a consistent interface (as shown below), plus an Integrated Scripting Environment (ISE) host application.

![PowerShell interface](image)

To access the interface or the ISE host application, search for PowerShell in the Windows Server operating system.

PowerShell also includes default cmdlets — simple commands you can use to manipulate objects. Cmdlets have a unique format — a verb and noun separated by a dash (-), such as Get-Help. You can use them separately or combine them in scripts that perform complex tasks. You can also write your own cmdlets.

SolarWinds provides customer support for PowerShell scripts, but not for scripting languages or custom scripts. Visit THWACK for scripting support from the SolarWind online IT community.

**Security considerations**

Depending on how you configure PowerShell in your environment, it can make any system vulnerable to unauthorized access. Be sure to review and assess how you incorporate PowerShell scripts into your environment. This includes importing scripts from third parties and the THWACK online community.

While PowerShell enhances Patch Manager functionality, be sure to consider the security risks inherent in using PowerShell scripts. To prevent unauthorized access to computers in your network, SolarWinds recommends using a dedicated Windows account with low-level privileges to create and review PowerShell scripts.
To avoid security risks such as malicious OS command injections, consider implementing the PowerShell built-in security. See the Microsoft PowerShell documentation located on the Microsoft Docs website at https://docs.microsoft.com for details.

Requirements

Below are the PowerShell requirements for a typical Patch Manager environment.

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerShell version</td>
<td>PowerShell 2.0 or later is required on the Patch Manager server to execute remote scripts on your managed computers. PowerShell is installed by default with Microsoft Windows Server operating systems. See the Microsoft Docs website at <a href="http://docs.microsoft.com">http://docs.microsoft.com</a> for the PowerShell system requirements.</td>
</tr>
<tr>
<td>Accounts and permissions</td>
<td>Local Admin rights are required to run scripts on the Patch Manager server. To execute scripts on your managed systems, select a Windows credential with rights to log in to the Patch Manager server plus sufficient rights on the managed systems to execute tasks in the script. For example, if a script executes a task with WMI, the credentials also require WMI rights on the target system.</td>
</tr>
<tr>
<td>Microsoft .NET Framework</td>
<td>Many PowerShell scripts require .NET 3.5.x, but the latest Patch Manager software includes a later version. If required, use the Add Roles and Features Wizard in Server Manager to add .NET Framework 3.5.x.</td>
</tr>
</tbody>
</table>

Push scripts using the Update Management Wizard

You can create PowerShell scripts using Windows PowerShell Integrated Scripting Environment (ISE) or a text editor (such as Notepad). After you create your remote and local scripts, you can load them in Update Management or the Update Management Wizard by clicking Load remote script or Load local script—based on the type of script you create.

You can create remote or local scripts for your managed systems. Remote scripts are executed on each client machine using PowerShell Remoting (PSRemoting). These scripts use the client machine credentials stored in the Credential Ring to authenticate and execute the script. Local scripts are executed on the Application Server.
When you are ready to upload a script, click the appropriate button in the interface to load the remote or local script (for example, Load remote script). When completed, Patch Manager validates the script for syntax errors. If an error is detected, a dialog box displays with the error.

After Patch Manager validates the script, a Valid message displays under the script load button. If the script contains errors, Not Valid displays under the load button. If the script is validated, Valid displays under the load button.

If Not Valid displays, the Next button is deactivated in the wizard. When this occurs, rewrite the script and then reload. After the script is validated, the Next button is activated, and you can proceed.

Remote PowerShell scripts

Remote PowerShell scripts are executed on client machines that access your corporate network from a remote location. When an employee logs in and connects to the WSUS server, Patch Manager pushes the updates to their systems.

To access the remote systems, Patch Manager uses PowerShell Remoting and the client machine credentials stored in the Credential Ring to authenticate and execute the PowerShell script on each client machine listed in the target scope.

On each client machine targeted with PowerShell scripts, ensure that:

- PowerShell Remoting (PSRemoting) is enabled. This allows your Patch Manager server and your managed clients to communicate with each other.
- Windows Remote Management (WinRM) is configured. This enables the managed system to receive PowerShell remote commands.

See the Microsoft Docs website at https://docs.microsoft.com for details on how to enable and configure these settings.

Script limitations

Remote PowerShell scripts have the following limitations:

- They do not support Patch Manager PowerShell variables.
- They only execute on client machines running WMI Providers and not a Patch Manager agent. If a Patch Manager agent is included in your target scope, the task for that agent will fail.
Pre-update remote script example

Pre-update scripts are executed on the targeted client machines listed in the target scope before the patch update runs. To run this script, locate the Patch Manager Pre-Update Script box in the Update Management Wizard and select the Run remote script checkbox. Click Load remote script to load the script and validate for errors.

If you want to execute the update task in the event that the script fails, select the Continue if script failed checkbox. If Patch Manager cannot access the targeted computer, the script will not be executed.

If the script includes PowerShell commands that can temporarily break the connection between the Patch Manager server and the client machine, select Wait if connection lost and select an appropriate wait time.

The following script example creates a new folder on the client system at c:\Result, where the folder name is the current date and time. This script is executed before the patches are installed on the system.

```powershell
function createFolder ($fname)
{
    New-Item -ItemType directory -Path C:\Result\beforeClientFolder-$fname
}
$time = $((Get-Date).ToString('yyyy-MM-dd hh-mm-ss'))
createFolder $time
```

Post-update remote script example

Pre-update scripts execute on the targeted client machines listed in the target scope after the patch updates run. To run this script, locate the Patch Manager Post-Update Script box in the Update Management Wizard and select the Run remote script checkbox. Click Load remote script and navigate to the script. If the script syntax is good, Valid displays in the box.
Optionally, you can select whether to execute the script if the Patch Manager update fails for any reason. If the script includes PowerShell commands that can temporarily break the connection between the Patch Manager server and the client machine, select Wait if connection lost and select an appropriate wait time.

The following script example creates a new folder on the client system at \c:\Result, where the folder name is the current date and time. This script is executed after the patches are installed on the system.

```powershell
function createFolder ($fname)
{
    New-Item -ItemType directory -Path C:\Result\afterClientFolder-$fname
}
$ime = $((Get-Date).ToString('yyyy-MM-dd-hh-mm-ss'))
createFolder $ime
```

**Local PowerShell scripts**

Local PowerShell scripts are executed on client machines that access your corporate network locally—for example, from within your corporate headquarters. These scripts are executed on the Application Server from the Patch Manager Administrator Console. Users can access the Patch Manager PowerShell Variables from within the scripts. All local PowerShell scripts support PowerShell variables.

**Pre-update local script example**

Pre-update local scripts are executed by the Application Server on the targeted client machines before the patch update runs. To run this script, locate the Patch Manager Pre-Update Script box in the Update Management Wizard and select the Run local script checkbox. Click Load remote script and navigate to the script. If the script syntax is good, Valid displays in the box. Select the Continue if script failed checkbox if you want the update to continue in this situation.
The following script example creates a folder in the Patch Manager server with the first client machine name. This script will also set the registry key on each client machine with the current date and time and the user name.

```powershell
function createFolder ($fname) {
    $path = "C:\Result\beforeFolderOnLocal-" + $fname
    $time = $((Get-Date).ToString('yyyy-MM-dd-hh-mm-ss'))
    New-Item -ItemType directory -Path $path+stime
}
createFolder $TargetMachineList.Values[0].NetbiosName

function Set-RemoteRegistryValue {
    $null = Invoke-Command -ComputerName $ComputerName -ScriptBlock {
        Set-ItemProperty -Patch $using:Path -Name $using:Name -Value $using:Value
    } -Credential $Credential
}

$m32 = $TargetMachinesList['mentonw7x32']
$m64 = $TargetMachinesList.Values[1]
```
```powershell
$remoteKeyParams32 = @{
    ComputerName = $m32.NetBiosName
    Path = 'HELM:\SOFTWARE\Test'
    Name = 'Cred'
    Value = $m32.Credential.UserName + ' ' + $(Get-Date.ToString('yyyy-MM-dd-hh-mm-ss'))
}

$remoteKeyParams64 = @{
    ComputerName = $m64.NetBiosName
    Path = 'HELM:\SOFTWARE\Test'
    Name = 'Cred'
    Value = $m64.Credential.UserName + ' ' + $(Get-Date.ToString('yyyy-MM-dd-hh-mm-ss'))
}

Set-RemoteRegistryValue @remoteKeyParams32 -Credential $sm32.Credential
Set-RemoteRegistryValue @remoteKeyParams64 -Credential $sm64.Credential
```

Warning: SolarWinds strongly recommends that you back up the client registry before making any edits to their system registry. You should only edit the registry if you are experienced and confident in doing so. Editing the register incorrectly can cause serious issues with the client operating system, which could require you to reinstall their operating system to correct them. SolarWinds cannot guarantee resolutions to any damage resulting from making registry edits.

Post-update local script example

Post-update local scripts run on the client machines by the Application Server after the patch updates are installed. To run this script, locate the Patch Manager Post-Update Script box in the Update Management Wizard and select the Run local script checkbox. Click Load remote script and navigate to the script. If the script syntax is good, Valid displays in the box. Select the Execute if others failed checkbox if you want the script to execute if the update fails.
The following script example creates a new folder on the client system at `c:\Result`, where the folder name is the current date and time. This script is executed after the patches are installed on the system.

```powershell
function createFolder ($fname)
{
    $path = 'C:\Result\afterFolderOnLocal-' + $fname
    $time = $((Get-Date).ToString('yyyy-MM-dd-hh-mm-ss'))
}
createFolder $TargetMachinesList.Values[0].NetbiosName
```

Customize local scripts using Patch Manager PowerShell variables

To create more efficient local scripts, you can implement the Patch Manager PowerShell variables. You can use these variables in the same way as PowerShell variables by using the `$` sign.

> These variables cannot be used for remote scripts.

The following table lists the variables you can use in a Patch Manager PowerShell script.

<table>
<thead>
<tr>
<th>Class</th>
<th>Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class TargetMachine</td>
<td><code>string</code> Hostname</td>
</tr>
<tr>
<td></td>
<td><code>string</code> FQDN</td>
</tr>
<tr>
<td></td>
<td><code>string</code> NetbiosName</td>
</tr>
<tr>
<td></td>
<td><code>string</code> IPAddress</td>
</tr>
<tr>
<td></td>
<td><code>PSCredential</code> Credential</td>
</tr>
<tr>
<td>Class TaskOperationsResult</td>
<td><code>Guid</code> TaskID</td>
</tr>
<tr>
<td></td>
<td><code>string</code> Device</td>
</tr>
<tr>
<td></td>
<td><code>string</code> OperationName commonconstants.eOperationResultStatus OperationResult</td>
</tr>
<tr>
<td></td>
<td><code>string</code> OperationResultMessage</td>
</tr>
<tr>
<td></td>
<td><code>DateTime</code> OperationCompletionTime</td>
</tr>
</tbody>
</table>
### Class

<table>
<thead>
<tr>
<th>Enum commonconstants. eOperationResultStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>• None = 0x0</td>
</tr>
<tr>
<td>• Success=0x01</td>
</tr>
<tr>
<td>• Failure = 0x02</td>
</tr>
<tr>
<td>• Aborted = 0x04</td>
</tr>
<tr>
<td>• Running = 0x8</td>
</tr>
<tr>
<td>• PartialSuccess = 0x10</td>
</tr>
<tr>
<td>• SuccessSynthetic=0x20</td>
</tr>
<tr>
<td>• FailureSynthetic=0x40</td>
</tr>
<tr>
<td>• PartialSuccessSynthetic=0x80</td>
</tr>
<tr>
<td>• EffectiveSuccess=0x100</td>
</tr>
<tr>
<td>• EffectiveSuccessSynthetic=0x200</td>
</tr>
<tr>
<td>• NotApplicable=0x400</td>
</tr>
<tr>
<td>• All = 0xff</td>
</tr>
</tbody>
</table>

### Class Rule

<table>
<thead>
<tr>
<th>Rule Type</th>
<th>RuleOperator</th>
<th>RuleExpression</th>
</tr>
</thead>
<tbody>
<tr>
<td>string</td>
<td>string</td>
<td>string</td>
</tr>
</tbody>
</table>

### PowerShell script output examples

The following table lists examples of output you can generate using Patch Manager PowerShell variables.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>SortedList&lt;String, TargetMachine&gt; TargetMachinesList</td>
<td>Contains a list of clients machines that is targeted by update task.</td>
</tr>
<tr>
<td>SortedList&lt;String, TargetMachine&gt; UpdateServicesServerList</td>
<td>Contains a list of available WSUS servers.</td>
</tr>
<tr>
<td>List&lt;TaskOperationsResult&gt; TaskResultsList</td>
<td>Contains executed task’s operations results list. Available only for Post-Task local scripts.</td>
</tr>
<tr>
<td>List&lt;Rule&gt; RulesList</td>
<td>Contains list of rules used for task.</td>
</tr>
<tr>
<td>Sting ApplicationServerName</td>
<td>Represents the name of Application server where the script is executing.</td>
</tr>
</tbody>
</table>
PowerShell script execution and failures

The following table lists examples of script execution and the corresponding results.

<table>
<thead>
<tr>
<th>Script Execution</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-Update remote local script is pushed to each end client listed in the target scope</td>
<td>When the script fails, the update task is executed only if “Continue if script failed” is checked. If the client is not accessible, the script is not executed. Patch Manager PowerShell variables are not accessible in these scripts.</td>
</tr>
<tr>
<td>Pre-Update local script is pushed to the Application Server</td>
<td>When the script fails, the update task is executed only if “Continue if script failed” is checked. Patch Manager PowerShell variables are accessible in these scripts.</td>
</tr>
<tr>
<td>Post-Update remote local script is pushed to each end client listed in the target scope</td>
<td>When each client operation fails, the script is executed only if “Continue if update failed” is checked. If client is not accessible, the script is not executed. Patch Manager PowerShell variables are not accessible in these scripts.</td>
</tr>
<tr>
<td>Post-Update local script is pushed to the Application Server.</td>
<td>When the update fails, the script is executed only if &quot;Execute if others failed&quot; is checked. The script is not executed if any of the task operations fail, unless the checkbox is checked. Patch Manager PowerShell variables are accessible in these scripts.</td>
</tr>
</tbody>
</table>

View the PowerShell script output

Patch Manager keeps track of the script output in Active Tasks, including the computer name, status, and details. Below is an example of the script output in the Patch Manager Administrator Console. To access this window, select

<table>
<thead>
<tr>
<th>Computer</th>
<th>Object</th>
<th>Operation</th>
<th>Status</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>mentonw7x32.pivdval...</td>
<td>PowerShell script</td>
<td>Pre-Task Remote Script Execute</td>
<td>Success</td>
<td>15:07:02:605. C:\Res\BeforeClientFolder-2018-11-09-07-02...</td>
</tr>
<tr>
<td>MNServer</td>
<td>PowerShell script</td>
<td>Post-Task Local Script Execute</td>
<td>Failed</td>
<td>19:07:45:040. The term ‘NewItem’ is not recognized as the name.</td>
</tr>
<tr>
<td>MNServer</td>
<td>PowerShell script</td>
<td>Pre-Task Local Script Execute</td>
<td>Success</td>
<td>15:06:05:957. C:\Res\BeforeFolderOnLocal\MENTONW7\x\02&gt;...</td>
</tr>
</tbody>
</table>
Access the script output

1. Log in to Patch Manager as an administrator.
2. In the Patch Manager menu, maximize Administration and Reporting and select Active Tasks.
3. In the lower center menu, click the Output tab.

Check the script task history

1. In the Patch Manager menu, maximize Administration and Reporting and select Task History.
2. In the top center console, select a script task.
3. In the bottom center console, click the Details tab.

Push the updates with PowerShell scripts

After you create your PowerShell scripts, you can push the scripts to your managed systems using one of the following methods:

- Push PowerShell scripts with updates using Update Management
- Push PowerShell scripts without updates using Update Management Wizard
- Push PowerShell scripts with updates using the Update Management Wizard

Push PowerShell scripts with updates using Update Management Wizard

Use this installation method to push PowerShell scripts with specific updates to your managed systems.

1. Create a new Windows PowerShell script and save the file in PS1 format.
2. Log in to the Patch Manager Administrator Console as an administrator.
3. In the navigation pane, select an installation method.
   - To install the script with your software updates, expand Enterprise > Update Services > your_WSUS_server > Updates and select the updates in the center pane that you want to include with the script.
   - To install the script without your software updates, select one or more computers or computer groups in Microsoft Windows Network or Managed Computers that require the script.
4. In the Actions pane, click Update Management.
5. In the Pre-Update Management Reboot Options box, select the options you want to execute
before the updates are installed on the managed computers.

You can select remote or local scripts. Remote scripts are executed on each client machine listed in the target scope using PowerShell Remote. These scripts use the client machine credentials from the Credential Ring. Local scripts are executed on the Application Server.

To run a PowerShell script before Patch Manager installs the updates:

a. Select a remote or local script to run.

   For example, select Run remote script.

   ![Patch Manager Pre-Update Script]

   - Run remote script
   - Run local script
   - Load remote script

   Not Validated
   - Continue if script failed
   - Wait if connection lost
     - Maximum time to wait
       - 10 minutes

b. Click Load remote script, select the targeted PowerShell script, and then click Validate.

   Patch Manager checks and validates the script. If the script code is correct, Valid displays in the window. If the script code is not valid, Not Valid displays in the window.

   ![Patch Manager Pre-Update Script]

   - Run remote script
   - Run local script
   - Load remote script
   - Valid
   - Continue if script failed
   - Wait if connection lost
     - Maximum time to wait
       - 10 minutes

   (Optional) Select Continue if script failed to continue the update procedure if the PowerShell script fails.
d. (Optional) Select Wait if connect lost if PowerShell commands exist in the script that can temporarily break the connect between Patch Manager and the client. If you select this option, select a maximum time to wait before Patch Manager reconnects to the client.

For example, if you select Always reboot in the Pre-Update Management Options, select Wait if connection lost and select an appropriate wait time just in case the reboot requires an extended amount of time.

If you do not select this option and a reboot command exists, the task may fail.

This option assists with executing a script and a reboot command. For example, if you select Always reboot and select Wait if connection lost, the reboot may require an extended amount of time to execute.

e. (Optional) Select any advanced options.

6. Select the options you want to execute before the updates are installed on the managed computers.

To run a PowerShell script after Patch Manager installs the updates:
a. Select Run remote script or Run local script.

For example, select Run remote script.

![Patch Manager Post-Update Script]

b. Click Load remote script, select the targeted PowerShell script, and then click Validate.

Patch Manager checks and validates the script. If the script code is correct, Validate displays in the window. If the script code is not valid, Not Valid displays in the window.

![Patch Manager Post-Update Script]

c. (Optional) Select Execute if update failed.

7. Click OK.

8. In the Task Options Wizard, locate and add the targeted computers, and click Next.

9. Complete the wizard to push the scripts and updates to the managed computers.

**Push PowerShell scripts without updates using the Update Management Wizard**

Use this installation method when you want to push your PowerShell scripts without a fixed list of updates to your managed systems.

1. Create a new script using Windows PowerScript ISE and save the file in PS1 format.

2. Log in to the Patch Manager Administrator Console as an administrator.

3. In the navigation pane, select an installation method.

   To install the script without your software updates, select one or more computers or computer groups in Microsoft Windows Network or Managed Computers that require the script.

4. In the Actions pane, click Update Management Wizard.

5. Select Create custom dynamic update management rules, and click Next.
6. In the Update Management Wizard, click Add Rule > Update Title Rule.

7. In the field, enter PowerShell and select Include update when title equals, and then click OK.

8. Click Add Rule.

   The rule is added to the window.

9. Click Save Template.

10. Add a descriptive template name, and then click Save.

    The template is saved for future use.
11. Click Next in the Update Management Wizard window.

12. Complete the wizard to push the script to the managed computers.

When you need to push another PowerShell script to a managed computer, open the Update Management Wizard, select Load existing update management rules, and complete the wizard.

---

**Push PowerShell scripts with updates using the Update Management Wizard**

Use this installation method when you want to push PowerShell scripts with a fixed list of updates based on specific criteria. For example, downloading and installing all needed and approved security and critical updates.

1. Create a new script using Windows PowerScript ISE and save the file in PS1 format.

2. Log in to the Patch Manager Administrator Console as an administrator.

3. In the navigation pane, select an installation method.

   To install the script with your software updates, expand Enterprise > Update Services > `your_WSUS_server` > Updates and select the updates in the center pane that you want to include with the script.

4. In the Actions pane, click Update Management Wizard.
5. Select a fixed list of updates or a dynamic list of updates based on specific criteria, and click Next.

6. Add a custom dynamic rule that includes updates based on selected criteria. Otherwise, accept the selected rules, and click Next.

7. Select the options you want to execute before the updates are installed on the managed computers.

You can select remote or local scripts. Remote scripts are executed on each client machine listed in the target scope using PowerShell Remote. These scripts use the client machine credentials from the Credential Ring. Local scripts are executed on the Application Server.

To run a PowerShell script before Patch Manager installs the updates:

a. Select Run remote script or Run local script.

   For example, select Run remote script.

   ![Patch Manager Pre-Update Script]

b. Click Load remote script, select the targeted PowerShell script, and then click Validate.

   Patch Manager checks and validates the script. If the script code is correct, Valid displays in the window. If the script code is not valid, Not Valid displays in the window.

   ![Patch Manager Pre-Update Script]

c. (Optional) Select Execute if update failed.

d. Select the approval options as required.

   ![Approval Options]
e. Select any advanced options as required. The option shown below is selected by default.

<table>
<thead>
<tr>
<th>Advanced Options</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Microsoft Update online catalog when scanning</td>
<td>✗</td>
</tr>
<tr>
<td>Do not include superseded updates when scanning</td>
<td>☑</td>
</tr>
<tr>
<td>Only download the updates, do not install the updates</td>
<td>☑</td>
</tr>
<tr>
<td>Run in planning mode</td>
<td>☑</td>
</tr>
<tr>
<td>Ignore exclusive updates when matched and install updates</td>
<td></td>
</tr>
<tr>
<td>If an exclusive update is matched, only install the exclusive update</td>
<td></td>
</tr>
<tr>
<td>If an exclusive update is matched, fail the installation process</td>
<td></td>
</tr>
</tbody>
</table>

An exclusive update is an update that must be installed individually, outside of a batch of other updates. This typically includes updates such as operating system service packs, .NET Framework service packs and redistributables, and updates to the Component-based Servicing Stack. See the table below for option details.

<table>
<thead>
<tr>
<th>Exclusive update option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore exclusive updates when matched and install updates</td>
<td>Installs all updates and ignores the exclusive update.</td>
</tr>
<tr>
<td>If an exclusive update is matched, only install the exclusive update</td>
<td>Installs only the exclusive update and ignores all other applicable updates.</td>
</tr>
<tr>
<td>If an exclusive update is matched, fail the installation process</td>
<td>Fails the installation process if an older update (based on its KB article number) supersedes the latest update. For example, decline KB4088825 if it is superseded by KB4093432.</td>
</tr>
</tbody>
</table>

8. Select the options you want to execute after the updates are installed on the managed computers.

To run a PowerShell script after Patch Manager installs the updates:

a. Select Run remote script or Run local script.

For example, select Run remote script.

b. Click Load remote script, select the targeted PowerShell script, and then click Validate.

Patch Manager checks and validates the script. If the script code is correct, Validate
displays in the window. If the script code is not valid, Not Valid displays in the window.

![Patch Manager Post-Update Script]

- (Optional) Select Execute if update failed.

9. Click Next.

10. Complete the wizard to push the scripts and updates to the managed computers.

**Schedule the WSUS updates**

All managed systems access the WSUS server to receive the pushed updates. If a targeted system belongs to one or more traveling employees, the systems will not receive the updates.

After you push the updates to the managed systems, schedule the pushed updates to run each day or week for up to 30 days based on your corporate IT policy. When the employees log in and reconnect to the WSUS server, the scheduled task pushes the updates to their systems.

- This process will not affect systems that received and installed the updates.

**Beginning in 2020.2, scheduled tasks now support Patch Manager dynamic computer groups.** When you add or remove a client computer from a Patch Manager group, the computer is automatically added or removed from the scheduled task.

1. Enter a name and description for the task.

![General Information]

- Apply the Mozilla Firefox 47 security update
- Description: Applies the Mozilla Firefox 47 security update to the WORKGROUP computers.

2. Select Schedule the task to run daily, weekly, or monthly, and then click Edit.
3. Select a start time and date. Select Universal Time to select Greenwich Mean Time.

In this example, the Start Time is 9AM. This allows the update to begin when most employees are in the corporate office.

4. Select how often the task should run in the assigned department or group (hour, day, week, or month). For example, run the task for at least three weeks to ensure that all users who are on vacation receive the update when they return to the office.

5. Select how often the task should occur, and click OK.

The selected settings display in the wizard.

6. Complete the Task Options Wizard, and click Finish.

The update task is scheduled.

Stop an update to the managed systems

If you need to stop an update to your managed systems, perform the following steps:

1. Log in to Patch Manager as an administrator.

2. In the Patch Manager menu, expand Enterprise > Update Services > your_WSUS_server > Updates and select All Updates.

3. In the center pane, locate and select the update you want to stop.

4. Right-click the update and select Decline.
5. Click Yes to confirm the action.

The update is stopped.

Delete an update to the managed systems

If you need to delete an update assigned to your managed systems, perform the following steps:

1. Log in to Patch Manager as an administrator.

2. In the Patch Manager menu, expand Enterprise > Update Services > *your_WSUS_server* > Updates and select All Updates.

3. In the center pane, locate and select the update you want to delete.

4. In the Actions menu, click Delete.

5. When prompted, click Yes.
6. In the navigation pane, expand Enterprise and select Update Services.

![Navigation Pane]

7. In the Actions pane, click Synchronize Server.

![Actions Pane]

8. Complete the Task Options Wizard to synchronize the WSUS server.

### Check the task history

After you apply or schedule the third-party updates, check the Task History to verify that the update task completed.

1. In the navigation pane, expand Administration and Reporting and select Task History. Patch Manager may require several minutes to populate the Task History pane.

![Navigation Pane]

2. Locate the Update Management task in the Task History pane and verify that the Status is
Troubleshoot certificate errors during third-party updates

When you download or install third-party updates to clients of software distribution points, the targeted managed system may display certificate errors. These errors may include:

- Certificate chain process terminated
- Invalid signature
- Failed to download

These errors may be caused by:

- WSUS self-signed certificate not installed in the Trusted Root CA and Trusted Publishers
- Allowed signed updates from an intranet Microsoft update services location setting is not enabled in the computer policy

To resolve these errors, verify that the WSUS certificate is installed on the client computers, WSUS server, SCCM server, and any other Windows-based system that generates errors when you download and install your software updates.

Check the Windows Update Policy

Verify that the WSUS self-signed certificate is located in the Trusted Root Certification Authorities. This certificate authorizes the installation of the signed content. Also, ensure that the policy on the computer has "Allow signed updates from an intranet Microsoft update services location" enabled.

1. Locate and open the Resultant Set of Policy (RSOP) on the target computer. This policy reflects the current policy for the local and GPO applied to the system.

   Open a Search box and type:

   RSOP.msc
Generating the policy may require several minutes to complete.


3. Verify that the following policy setting is enabled:

   Allow signed updates from an intranet Microsoft update services location

   If the setting is not configured, update the setting from your Group Policy Management Console on the Domain Controller. See Configure clients using Group Policy for details.


Export the WSUS certificate

Provision your downstream publishing servers with a WSUS certificate by exporting the certificate from the upstream WSUS server.

See Configure clients using Group Policy for details.

Import the WSUS certificate

After you export the certificate to a file, import the certificate file to both the Trusted Root Certification Authorities and Trusted Publishers stores. You can import the certificate into your GPO or perform the following steps to manually import the certificate to the PC.

1. Log on to the computer that is receiving the certificate error.

2. Copy the certificate to the local machine.

3. Launch the Microsoft Management Console by executing:

   MMC.exe

4. Click File > Add/Remove Snap-in.

5. Select Certificates and click Add.

6. Select the Computer account, and click Next.

7. Select the Local Computer, and click Finish.

8. Click OK.
9. Place the certificate in Trusted Root CA.
   a. Expand Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates.
   b. Search the directory for a WSUS Self-Signed Certificate.
   c. Make sure the serial number is identical with the certificate you exported from the WSUS server.
      If the certificate is identical, go to step 10. If not, go to step d.
   d. Right-click Certificates under Trusted Root Certification Authorities > All Tasks > Import.
   e. Click Next.
   f. Click Browse and navigate to the directory where you copied the certificate.
   g. Select the certificate, and then click Next.
   h. Make sure the certificate is placed in Trusted Root CA, and then click Next.
   i. Click Finish.

   a. In the certificates MMC, navigate to Trusted Publishers > Certificates.
   b. Search this directory for the WSUS Self-Signed Certificate, if it is present, make sure the serial number is the same as the certificate you exported from WSUS. If it is then attempt to download the update again, if the serial number doesn’t match continue to step b.
   c. If it is not present then right-click on Certificates under Trusted Publishers > All Tasks > Import.
   d. Click Next.
   e. Click Browse and navigate to the directory where you copied the certificate.
   f. Select the certificate, and click Next.
   g. Verify that the certificate is being placed in Trusted Publishers, and click Next.
   h. Click Finish.
Uninstall a program using Patch Manager Computer Explorer

If you need to uninstall a program from a managed computer, you can use Computer Explorer.

This tool allows you to:

- View information and execute tasks on remote computers directly from the Patch Manager Console
- Execute tasks against a single target
- Use the Task Options Wizard to extend that task to a group of managed computers

Patch Manager can only uninstall software programs with an MSI extension.

1. Log in to Patch Manager as an administrator.
2. In the navigation pane, locate and select the targeted computer. You can specify a group of computers later.
3. In the Actions pane, click Computer Explorer.
4. Click the Installed Software tab.
5. In the list, select the program you want to uninstall.
6. In the toolbar, click Uninstall Software.
7. In the Uninstall Software window, click Uninstall.
8. In the Task Options Wizard, add the computers you want to target with the uninstall task, and then click Next.
9. In the Scheduling and Notification Options screen, specify any scheduling or notification options, and then click Finish.
Generate an inventory and create reports

Inventory tasks pull information from your WSUS servers and managed computers to display patch status in the Patch Manager Administrator Console. Schedule inventory tasks each week to keep your report data current.

When you configure your inventory tasks for the first time, Patch Manager installs SolarWinds Client Components on the managed computers during the initial connection. This WMI Provider performs the following tasks:

- Initiates the connection between the application and each managed computer
- Adds additional functionality to the Native Windows WMI so the application can run specific queries and obtain specific information from each managed computer

If your managed computers are running a Patch Manager agent, Patch Manager initiates the connection to each managed computer through port 4092.

See Patch Manager Report Viewer and Report Builder for information about generating reports in the Patch Manager Summary dashboard.

Configure the inventory tasks

Check out this video (14:19) for information about how to set up a WSUS inventory and run reports.

Inventory tasks collect Microsoft® and third-party update status information from the WSUS servers and managed systems. This data is displayed in the Patch Manager Administrator Console, Patch Manager Summary dashboard in the Orion Web Console (for Orion integrations), and reports.

You can run the following inventory tasks in Patch Manager:

- **WSUS inventory**. Collects information about the WSUS server configuration (such as WSUS server statistics and basic computer inventory attributes). This inventory populates the WSUS reports.
- **Managed computer inventory**. Collects information about the processes running on your managed systems. This inventory populates the Configuration Management reports.
- **Additional inventories**. Collects information from other segments of your Patch Manager deployment, such as Microsoft® Windows® Network groups, approved agents, and additional management groups.
- **Specific datasource inventory**. Collects file, folder, or registry information from selected computers in your network.
Initiating the inventory connection

When you configure your inventory tasks for the first time, Patch Manager installs SolarWinds Client Components on the managed computers. This WMI Provider performs the following tasks:

- Initiates the connection between the application and each managed computer
- Adds additional functionality to the Native Windows WMI so the application can run specific queries and obtain specific information from each managed computer

If your managed computers are running a Patch Manager agent, Patch Manager initiates the connection to each managed computer through port 4092.

See Generate and view reports in Patch Manager for details about generating reports in the Patch Manager Web Console.

Configure the WSUS inventory task

The WSUS Inventory task uses the WSUS API to access data on your upstream and downstream WSUS servers and populate the WSUS reports located at Administration and Reporting > Reporting > WSUS Reports.

These reports provide information about WSUS server performance and update packages installed on managed systems by the WSUS server. Patch Manager includes several common WSUS reports that help you identify:

- Systems running approved updates
- Packages that failed to install during the update
- Systems with approved, installed, or failed Microsoft and third-party updates

Schedule your WSUS Inventory tasks to run each day outside of your normal operating hours. The WSUS Inventory task collects large amounts of data from all managed computers in your network, which can impact your business operations. When the task is completed, the data is stored in the Patch Manager database.

1. Log in to the Patch Manager Admin Console as an administrator.
2. In the Patch Manager menu, expand Enterprise > Update Services.
3. Select your WSUS server.

4. In the Actions pane, click WSUS Inventory.

5. In the WSUS Inventory Options dialog box, select Direct or All.

   If you select Direct, WSUS inventory will only gather the data from computers directly reporting to the WSUS server for which the targeted inventory is configured.

   If you select All, the WSUS inventory will gather data about all computers reporting to upstream and downstream WSUS servers. Select this option if your WSUS servers are in Replica Mode with your upstream and downstream servers.

   Select an option to review the description.
6. Verify the remaining options, and click Save.

7. Select a time and date when the WSUS Inventory task begins.

8. Select how often Patch Manager runs the task.
9. Select a time to stop the task, and click OK.

   SolarWinds recommends selecting No end date to ensure the WSUS server continues to receive updates from the WSUS database.

10. In the navigation menu, expand Administration and Reporting and select Scheduled Tasks.

11. Verify that the task is displayed in the Schedule Tasks pane.

Configure the managed computer inventory task

The managed computer inventory task collects data from the managed computers to populate the Configuration Management reports. These reports provide status information about the processes running on your managed systems (such as software applications, network configuration, and policies). Run these reports to ensure your managed systems comply with your corporate and department policies.

   If you are running this task for the first time, configure and schedule the WSUS Inventory task first. Otherwise, Patch Manager will prompt you during the following procedure.

These reports are located at Administration and Reporting > Reporting > Configuration Management Reports.
You can automate your inventory task by scheduling the task to run at a specific time and date. To prevent disruptions to your network, schedule your inventory task outside of your normal business hours.

1. Log in to the SolarWinds Patch Manager Admin Console as an administrator.
2. In the Patch Manager menu, expand Enterprise > Update Services.

3. Select your WSUS server.
4. In the Actions pane, click Inventory.
5. In the Inventory Options dialog box, select Inventory - include specific datasources and click OK.
6. In the Task Options Wizard, select one or more computers to include in the task, and click Next.

7. Enter a name and description for the task.

8. Schedule the task to run now or at a later date. Click Edit to set your daily, weekly, or monthly settings.

9. (Optional) Select an export option.
10. (Optional) Select an email option.

11. Click Next.

12. Review the task details, and click Finish.

The task is scheduled in Patch Manager.

Run a scheduled inventory task

You can schedule a task to run each day, week, or month. If you need run a scheduled task immediately, run the task from the Scheduled Tasks node in Administration and Reporting.

1. Log in to the SolarWinds Patch Manager Admin Console as an administrator.

2. In the Patch Manager menu, expand Administration and Reporting and select Scheduled Tasks.

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

4. In the Actions pane, click Run Task Now.

5. When prompted, click Yes to run the task.

6. Select Task History to review the task status.

Configure additional computer inventory tasks

In addition to creating an inventory for your managed computers, you can inventory other segments of your Patch Manager deployment. These segments include:

- Microsoft® Windows® Network groups
- Approved, pre-approved, or unapproved agents
After you complete the inventory, you can access the results in the Patch Manager Administrator Console, Patch Manager Summary dashboard (for Orion deployments), and the Configuration Management reports.

If you are running this task for the first time, set up the WSUS Inventory task first. Otherwise, Patch Manager will prompt you to create the task during the following procedure.

1. Log in to the Patch Manager Admin Console.
2. In the navigation pane, select one of the following options:
   - Enterprise > Update Services
   - Enterprise > Microsoft Windows Network
   - Enterprise > Agents
   - Patch Manager System Configuration > Management Groups
3. In the center pane, select the domain or workgroup you want to inventory.
4. In the Actions pane, click Inventory or Schedule Inventory (depending on your selection).
5. Complete the remaining windows and options to set up and schedule your inventory.

These options vary, depending on your selection.

Configure the specific data sources inventory tasks

The default inventory template collects WSUS and managed computer information from your managed systems. However, it does not collect file, folder, or Registry information as part of the inventory. To collect this information, customize the inventory templates using the File, Directory, and Datasource Configuration tab in the Inventory Configuration Editor.

1. In the navigation pane, select the targeted computer group.
   For example, you can maximize Enterprise > Microsoft Windows Network and select a computer group.
2. In the center pane, select the computer you want to inventory.
   Press <Ctrl> or <Shift> to select multiple computers.
3. In the Actions pane, click Inventory.
4. In the Inventory Options dialog box, select Inventory - include specific datasources.
5. In the Options box, select Create a custom inventory configuration template to configure a new template for the inventory task, and click OK.
6. In the Inventory Configuration Editor, click the File, Directory and Registry Datasource Configuration tab.

7. In the center pane, select the file system objects or registry objects you want to add, and click OK. You can also remove a Registry object.
Add a file system object

1. Click Manually Add/Modify above the File System Object table.

2. In the Add/Modify File or Directory dialog box, select File or Directory.

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

   - This field does not support Universal Naming Convention (UNC) paths, but it does support environment variables such as %PROGRAMFILES%.

4. Click Save.

   Patch Manager saves the inventory configuration associated with the specified path (such as the domain or workgroup).

Add a Registry object

1. Select a registry object in the Registry Object table.

   For example:
   Software\Microsoft\Driver Signing\Policy
2. Click Manually Add/Modify above the Selected Registry keys and Values Count table.

3. Complete the options and fields in the Add or Edit Registry Key or Value dialog box.
4. Click Save.

Patch Manager saves the inventory configuration associated with the selected manage scope (such as the domain or workgroup).

5. Repeat step 1 through step 4 for each additional file system object you want to add.

Remove a Registry object

If you no longer require a registry object, select the object in the File System Object or Registry Object table and click Delete.

**Generate and view reports**

Use the Patch Manager Report Builder and Report Viewer to generate a report, customize an existing report, and generate a custom report for your WSUS servers and managed clients.

**Generate a Patch Manager report**

When you generate a Patch Manager report (such as a WSUS report), Report Viewer opens in a new window. Use Report Viewer to customize the report layout and filter and sort the report results. When you are finished, configure the report viewer email settings, and then export and email the report results to one or more users.

💡 Beginning in 2.1.7, you can generate a report in the Orion Web Console when Patch Manager is integrated with the Orion Platform. See the Patch Manager Getting Started Guide for details.

**Generate a WSUS report**

After you set up the WSUS inventory, you can review the server status using the WSUS reports. These reports provide information about your WSUS server performance and update packages installed on managed systems by the WSUS server.

The WSUS reports are located at Administration and Reporting > Reporting > WSUS reports.
Windows Server Update Services reports

These WSUS reports provide high-level information about update packages installed on the managed systems by the WSUS server. This information includes the installation percentage for each update.

Below is a list of helpful Windows Server Update Services reports you can generate using Report Viewer.

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computers with approved update</td>
<td>Reports the percentage of systems running approved updates.</td>
</tr>
<tr>
<td>percentages</td>
<td></td>
</tr>
<tr>
<td>Percent Failed</td>
<td>Reports the percentage of update packages that were not installed during the update.</td>
</tr>
<tr>
<td>Percent Installed</td>
<td>Reports the percentage of update packages that were installed during the update.</td>
</tr>
<tr>
<td>Percent Not Installed</td>
<td>Reports the percentage of uninstalled update packages.</td>
</tr>
<tr>
<td>Update Approvals</td>
<td>Reports the update title, computer group name, release date, and administrator for each approved update.</td>
</tr>
</tbody>
</table>

Windows Server Update Services Analytics reports

These WSUS reports provide detailed information about update packages installed on the managed systems by the WSUS server. This information includes the update state for each update and computer.

Below is a list of helpful Windows Server Update Services Analytics reports you can generate using Report Viewer.
<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Update Status</td>
<td>Reports all Microsoft and third-party updates to each managed system and whether they are approved, installed, or failed. This report does not explain why an update failed.</td>
</tr>
<tr>
<td>Computer Update Status Approved Updates</td>
<td>Reports the approved upgrade packages and whether they are installed or not installed.</td>
</tr>
<tr>
<td>Computer Update Status Approved Updates Not Installed</td>
<td>Reports the approved upgrade packages that were not installed. This report does not state whether the upgrade was applicable for each system.</td>
</tr>
</tbody>
</table>

### Windows Server Update reports

These WSUS reports provide information about the Windows Update Agent. This agent runs on the managed computers and checks the WSUS server for the latest published updates.

### Generate a WSUS report

1. Log in to the Patch Manager Administrator Console.
2. In the navigation pane, expand Administration and Reporting > Reporting > WSUS Reports.
3. Select a report category.
   - For example, Windows Server Update Services Analytics.
4. In the center pane, select a report.
5. In the Actions pane, click Run Report.
Create a custom WSUS report

You can create custom Patch Manager reports using the Report Definition Builder. For example, you can create a WSUS report that displays all pending updates, update IDs, and update revision numbers in your environment. Using these values, you can install updates directly from the Report Viewer.

1. Schedule and run at least one inventory task for your managed computers.

   ![Schedule inventory tasks to populate empty reports](https://example.com)

   For details about scheduling inventory tasks in Patch Manager.

2. In the navigation pane, expand Administration and Reporting > Reporting > WSUS Reports.

3. Select a report category.

4. In the Reports pane, select the report you want to create.

5. In the Actions pane, click New Report.

6. In the Reports Definition Builder window, select the fields you want to include in the report.

7. Select the column and sort order for your fields.

8. Apply any filters you want to save in your report, and then click Next.

9. Name the report.

10. Select any scheduling preferences, and then click Finish.

Customize the report layout

You can customize how the information is displayed in the report. Any change you make to a report layout displays in all reports.

The following table lists the procedures for customizing a report layout.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase the number of lines Report Viewer displays per page</td>
<td>Click Navigation Configuration, and then enter a value up to 100,000. The default value is 2,000.</td>
</tr>
<tr>
<td>Reorganize the columns in the report</td>
<td>Drag and drop any column to a new position. For example, drag the Domain or Workgroup (Update Server) and Name (Update Server) columns to the far right of the data grid.</td>
</tr>
<tr>
<td>Resize the columns</td>
<td>Reposition the column separators in the header row.</td>
</tr>
<tr>
<td>Task</td>
<td>Procedure</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Group results by the values in a column</td>
<td>Drag the column header into the group bar.</td>
</tr>
<tr>
<td></td>
<td>For example, drag Computer Name into the group bar, as shown below.</td>
</tr>
<tr>
<td>Show or hide available columns</td>
<td>1. Click Column Chooser.</td>
</tr>
<tr>
<td></td>
<td>2. Select the columns you want to show.</td>
</tr>
<tr>
<td></td>
<td>3. Clear the columns you want to hide.</td>
</tr>
<tr>
<td></td>
<td>4. Close the Column Chooser window.</td>
</tr>
<tr>
<td>Save a custom layout</td>
<td>Click Save Layout.</td>
</tr>
<tr>
<td>Filter and sort the report results</td>
<td>You can sort the report list by the clicking the sort icons in each column. This sorts the entire report list by the contents of the selected column. You can sort each column in either ascending or descending order.</td>
</tr>
<tr>
<td>Filter report results</td>
<td>1. Click the column header once to sort in ascending (A-Z) order.</td>
</tr>
<tr>
<td></td>
<td>2. Click the column header twice to sort in descending (Z-A) order.</td>
</tr>
<tr>
<td>Sort a report by the values in a specific column</td>
<td>Click the column header once to sort in ascending (A-Z) order.</td>
</tr>
<tr>
<td></td>
<td>Click the column header twice to sort in descending (Z-A) order.</td>
</tr>
</tbody>
</table>
Configure the Report Viewer email settings

1. In the Report Viewer window, click Email Configuration.

2. Complete the options in the Console Email Settings dialog box.

   a. Enter the SMTP Server and Sender Email Address (required).
   
   b. If your email server uses a custom port, modify the Port value.
   
   c. If your email server uses a secure connection, select Use SSL or Use TLS.
   
   d. To specify one or more recipients who must receive a report, enter the email address(es) in the Favorite Recipients field separated by semicolons.

   e. If your email server requires credentials to send email, select Use Credentials, and then complete the related fields.

3. Click OK.
Email the report results to one or more users

1. In the Report Viewer window, click Email.

2. Complete the Email Recipients dialog box.
   a. In the Recipient field, enter at least one email address.
   b. (Optional) Enter a description.
   c. Click Add.
   d. Click OK.

3. In the Export Options window, select the format to use for your report.

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

5. Click Export.
Export a report

1. Log in to the Patch Manager Web Console.

2. Expand Administration and Reporting > Reporting.

3. Expand a report category that contains the report you need.
   For example, Task History Reports.

4. Select a report type.
5. In the top center console under Reports, select the custom report you want to export.

6. In the Actions menu, click Run Report.

7. In the Report Results menu options, click Export.

8. In the Export Options window, select a report format.
9. In the Export Filename field, enter a new path for the report or accept the default.

   Record this path so you can locate the report after the export.

10. Click Export.

11. When prompted, click OK.

12. Navigate to the path you recorded in the Export Filename field to access and open the report.

**Customize an existing report**

Use the Report Definition Builder to customize existing Patch Manager reports and refine or expand the results. The following example describes how to customize a Computer Update Status report to only include updates that are required but not installed.

1. Log in to the Patch Manager Admin Console.

2. In the navigation pane, expand Administration and Reporting > Reporting > WSUS Reports.

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

5. In the Actions pane, click Edit and Schedule Report.

6. Using the horizontal bar in each field, drag the Domain or Workgroup (Update Server) and Name (Update Server) fields to the bottom of the list.

7. Drag the Computer Name field to the top of the list.
8. Set the report to sort by the Computer Name column.
   Click Not Sorted next to Column Name and select Sort position 1 > Ascending.

9. Add the Update ID field to the report:
   a. Click [+] at the bottom of the first column, adding a new field.
   b. Click Select Field and select Computer Update Status > Update ID.

10. Add a filter to the report for updates to install upon approval.
    Choose records where all of the following apply
    ➔ Update Approval Action (Friendly Name) equals Install
a. Click [+] under Select the filter criteria for the report.

b. Click Select Field and select Computer Update Status > Update Approval Action (Friendly Name).

c. Click Select Operator and select equals.

d. Click <Enter Value> and select Enter Value.

e. In the text box, enter Install and press <Enter>.

11. 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 and select Computer Update Status > Update Installation State (Friendly Name).

   c. Click Select Operator and select does not equal.

   d. Click <Enter Value> and select Enter Value.

   e. In the text box, enter Installed and press <Enter>.

   f. Click the arrow next to Update Installation State (Friendly Name) and select Place in New Group.

   g. Click [+] and then click Select Field.

   h. Click Select Field and select Computer Update Status > Update Installation State (Friendly Name).

   i. Click Select Operator and select does not equal.

   j. Click <Enter Value>, and then select Enter Value.

   k. In the text box, enter Unknown and press <Enter>.

12. Click Next.

13. In the Report Name field, enter a unique name.

   For example, Computer Updates – Approved Not Installed.
14. Click Save and run report now, and then click Finish.

15. Examine your report in the Report Results tab and customize the layout (if required). See Using Patch Manager Report Viewer for additional details.

Generate a custom report

Use the Report Definition Builder to generate custom SolarWinds Patch Manager reports. You can generate a custom WSUS report with 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 describes how to:

- Create a custom WSUS report
- Install updates from a WSUS report
- Create a custom report that displays all pending updates
- Create a custom report that lists the third-party software installed on client systems

Before you begin

Before you generate a report, schedule and run at least one inventory task for your managed computers. See Schedule inventory tasks to populate empty reports for additional information about how to schedule inventory tasks in Patch Manager.

When you generate a custom report, be sure to select only the fields you need for the report. Otherwise, Patch Manager will continuously peg the database, allowing the tempdb file to grow until your drive space reaches maximum capacity. If this issue occurs, restart the SQL Server service to reclaim the space.
Generate a custom WSUS report

The following procedure describes how to create a custom WSUS report. This example describes how to customize a report to list and automatically install updates directly from the Report Viewer.

1. In the navigation menu, expand Administration and Reporting > Reporting > WSUS Reports.

2. Select Windows Server Update Services Analytics.

3. In the Reports pane, select the report you want to create.

4. In the Actions Pane, click New Report.

5. In the Report Definition Builder window, select the fields you want to include in the report.

6. Select the column and sort order for your fields.

7. Apply any filters you want to save in your report, and then click Next.

8. Name the report.

9. Specify any scheduling preferences, and then click Finish.

Install updates from a WSUS report

After you create a custom WSUS report, complete the following procedure to install updates directly from Report Viewer.

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. In the Update Management window, click OK.

6. In the Task Options Wizard window, add the computers that receive the updates, and click Next.

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

8. Click Finish.

Create a custom report that displays all pending updates

1. Log in to the Patch Manager Admin Console.

2. In the navigation menu, expand Administration and Reporting > Reporting > WSUS Reports.


4. In the Reports pane, select Select Computer Update Status.

5. Under Available Datasources, select Computer Update Status With Update Information.

6. In the Available Fields section, press Ctrl + click to select the following fields in this order:
   - Computer Name
   - Update Title
   - Update Installation State (Friendly Name)
   - Update ID
   - Update Revision Number
   - Name (Update Server)


8. Apply your preferences to one of the columns.
   - Click Not Sorted next to the Column Name.
   - Hover to Sort Position 1, and then select a sort option.

9. Add a filter to the report for updates that will install after the approval.
   - Select and expand the filter criteria for the report.
   - Click Select field for the new filter entry.
   - Hover to Computer Update Status With Update Information, and then select Update Approval Action (Friendly Name).
   - Click Select Operator > Select Equals.
   - Click Enter Value > Enter Value.
   - Enter Install.
10. Add a filter to the report for updates with Uninstalled or Unknowns states.
   a. Expand the existing filter.
   b. Click Select Field for the new filter entry.
   c. Hover to Computer Update Status With Update Information, and then select Update Installation State (Friendly Name).
   d. Click Select Operator > Does not equal.
   e. Click Enter Value > Enter Value.
   f. Enter Installed.
   g. Click the arrow and then select Place in New Group.
   h. In the new group, click [ + ].
   i. Click Select Field for the new filter entry.
   j. Hover to Computer Update Status With Update Information, and then select Update Installation State (Friendly Name).
   k. Click Select Operator > Does not equal.
   l. Click Enter Value > Enter Value.
   m. Enter Unknown.

11. Click Next.

12. Enter a unique name in the Report Name field.
    For example, Computers to update.

13. Select Save and run report now.

14. Click Finish.

Create a custom report that lists the third-party software installed on client systems

1. Log in to the Patch Manager Administrator Console.
2. In the navigation pane, expand Administration and Reporting > Reporting > Configuration Management Reports and select Installed Programs and Features.
3. In the center pane, select Installed Programs and Feature Basic (MS Product Omitted).
4. In the Actions pane, click New Report.
5. Define the report fields.
   a. Click + and then click Select Field.
   b. Mouse over Programs and Features.
   c. Select Name (Programs and Features).
6. Repeat step 5 to define the display name.
7. Click Next.
8. Add a name to the report.
9. Click Save and run report now.

💡 You can sort the data using the columns headers at the top, and add additional fields and filters to increase the amount of generated information.

Generate a custom report using Report Definition Builder

You can use the Report Definition Builder to create custom Patch Manager reports. For example, you can create a WSUS report that shows all 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.

Create a custom WSUS report

1. Log in to the Patch Manager Administrator Console.
2. In the navigation pane, expand Administrator and Reporting > Reporting > WSUS Reports.
3. Under WSUS Reports, select a report category.
4. In the center pane, select the type of report you want to create.
5. In the Actions pane, click New Report.
6. In the Report Definition Builder window, select the fields you want to include.
7. Specify the column and sort order for your fields.
8. Apply any filters you want to save in your report.
9. Click Next.
10. Enter a report name.
11. Specify any scheduling preferences.
12. Click Finish.
Create a custom report that includes all pending updates

1. In the navigation pane, 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 Field, Press Ctrl+click to select the following fields in this order:
   - Computer Name
   - Update Title
   - Update Installation State (Friendly Name)
   - Update ID
   - Update Revision Number
   - 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.

View the available data sources

Each report category in the Administration and Reporting > Reporting node includes a defined collection of data sources and fields you can use to build reports. In most cases, you can use several data sources to build reports with all of your selected fields.

- The data sources in the Windows Server Update Services Analytics and Computer (General) categories contain supersets of other data sources. As a result, you cannot combine data sources from these categories.

Perform the following steps to view the available data sources and fields in a report category.
1. In the navigation pane, expand Administration and Reporting > Reporting.

2. Expand a parent category.
   For example, WSUS Reports.

3. Select a report category.
   For example, Windows Server Update Services.

4. In the Available Datasources pane, locate and select an available data source.
   For example, Computer Group.
The available fields are displayed in the Available Fields box.

<table>
<thead>
<tr>
<th>Name</th>
<th>Data Type</th>
<th>Datasource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computers Up To Date Count (Including Downstr...</td>
<td>IntegerType</td>
<td>Computer Group</td>
</tr>
<tr>
<td>Computer Target Count (Including Downstream)</td>
<td>IntegerType</td>
<td>Computer Group</td>
</tr>
<tr>
<td>Computer Targets Needing Updates Count (Inclu...</td>
<td>IntegerType</td>
<td>Computer Group</td>
</tr>
<tr>
<td>ID (Computer Group)</td>
<td>StringType</td>
<td>Computer Group</td>
</tr>
<tr>
<td>Total Downloaded Count for Computer Group</td>
<td>IntegerType</td>
<td>Computer Group</td>
</tr>
</tbody>
</table>
Manage WSUS using Patch Manager

Use the Enterprise > Update Services node in the Patch Manager Administrator Console to manage your WSUS server. This node contains a child node for each WSUS server registered with Patch Manager. Each WSUS server node contains the native WSUS Updates and Computers and Groups child nodes.

See Set up Patch Manager with SCCM for details about managing WSUS in an SCCM environment.

Select the Microsoft products on the WSUS server

As your needs change, you can download additional Microsoft product updates on your WSUS server. After the server completes the synchronization, you can approve and push the updates to your managed computers.

1. Log in to Patch Manager as an administrator.
2. In the navigation pane, expand Enterprise > Update Services and select your WSUS server.
3. In the Actions menu, select Products and Classifications.
4. In the Products tab, select the targeted Microsoft products.
5. Click the Classifications tab and select the targeted classifications.
6. Click OK.

Patch Manager launches a task to update the WSUS server.

Synchronize the WSUS server with Microsoft Update

Schedule a task to synchronize the WSUS server with the Microsoft® Update site. When the task runs, the WSUS server connects with the Microsoft Update website, retrieves the latest Microsoft operating system updates, and stores the updates on the WSUS server. This process ensures that your WSUS server has the latest Microsoft updates you can apply to your managed systems.

Synchronize the WSUS server each day so you have the latest critical and security Windows updates for the managed systems.

After you select the WSUS server in the navigation pane, review the server synchronization information in the Details tab.
Schedule regular synchronization tasks for your WSUS servers to ensure they always have the latest updates.

1. Log in to SolarWinds Patch Manager as an administrator.
2. In the Patch Manager menu, expand Enterprise > Update Services.
3. Right-click the WSUS server and select Synchronize Server.

   In this example, SPM-MGOM is the WSUS server.

4. In the Task Options wizard, click Browse computers.
5. In the Patch Manager menu, expand Update Service Servers and select the WSUS server.
6. In the wizard, click Add Selected to add the WSUS server to the list, and then click OK.
7. Click Next.

8. Enter a name and description of the task.

![General Information]

9. Select Schedule the task to run daily, weekly, or monthly in the Scheduled Settings box, and then click Edit.

10. In the Schedule Time box, select a day and time. Select Universal Time for Greenwich Mean Time.

![Scheduled Time]

11. In the Recurrence pattern box, select when the WSUS server synchronizes with Windows Update.

12. Set the Range of recurrence to No end date to ensure that the WSUS server synchronization procedure never stops, and then click OK.

![Range of recurrence]

The settings are displayed in the Schedule Settings box.
13. Complete the Task Options Wizard, and click Next.
   A summary of the task settings are displayed in the window.

14. Click Finish.
   The Windows Update synchronization schedule task is created.

Check the WSUS server synchronization status

The WSUS server synchronizes with the Microsoft Update server based on your synchronization schedule. You can check the synchronization status by selecting the WSUS server in the navigation pane and reviewing the status in the Details tab.

1. Click the WSUS server in the Patch Manager menu.

2. In the Details tab, check the Synchronization Status.

1. In the Details tab, check the Synchronization Status.
Troubleshooting a failed synchronization

If the synchronization fails and you receive an error, do the following:

1. Verify that the hostname is correct.
2. Verify that the default port is correct.
   - For Windows Server 2008 R2 and earlier, the default is port 80 (443 for SSL).
   - For Windows Server 2012 R2 and later, the default is port 8530 (8531 for SSL).
3. Ensure that the ports are open and the host name can be resolved by DNS.
4. Verify the network connection to the upstream server.
5. Verify that the downstream server is connected to the upstream server.

See Set up a hierarchy of WSUS servers on the Microsoft Docs website for details.

Delete expired updates and revisions from the WSUS server

Over time, you may experience issues with content stored on the WSUS server drive. These issues may include:

- Drive consumes too much space
- WSUS views display inaccurate information, such as inaccurate status information on Windows 10 computers
- WSUS connection timeout errors
- Managed clients fail to install updates

Many of these issues are caused by a full WSUS database or a WSUS drive that is out of space. To resolve these issues, use the Server Cleanup Wizard to delete expired updates and revisions from the WSUS server.

The wizard configures a threshold for the number of days that the WSUS server retains non-reporting computers in the Patch Manager Administrator Console. When you are finished, you can schedule a clean-up task to run each day, week, or month.

1. Log in to Patch Manager as an administrator.
2. In the navigation pane, expand Enterprise > Update Services and select the WSUS server.
   - In the following example, SPM-MGOM is the WSUS server.
3. In the Actions pane, click Server Cleanup Wizard.

4. Select your cleanup options to perform on the WSUS server, and click OK.

5. In the Task Options Wizard, run the task now or create a schedule for the task.

6. Complete the wizard.
Repair and maintain the Windows Update Agent

Use the Windows Update Agent Maintenance and Repair task to identify and resolve issues with your Windows Update agents. In a standard WSUS environment, this functionality is only available from the command line, and can only be executed on one system at a time.

Repair a Windows Update Agent

Use Windows Update Agent Maintenance and Repair to diagnose and repair Windows Update agents on your remote systems. This will ensure that your remote systems can contact the WSUS server from a remote location and download Microsoft updates.

1. Log in to the Patch Manager Administrator Console as an administrator.
2. In the navigation pane, expand Enterprise and select one or more computers. For example, you can select Managed Computers and select a workgroup in the center pane.
3. In the Actions pane, click Windows Update Agent Maintenance and Repair.
4. In the dialog box, select one or more repair options.

The repair options include the following listed below.
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset Authorization</td>
<td>Resets the connection to the WSUS server. Use this option when you change the client group memberships on the WSUS server or identify duplicate client IDs.</td>
</tr>
<tr>
<td>Flush Background Intelligent Transfer Service (BITS) cache</td>
<td>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.</td>
</tr>
<tr>
<td>Reset Windows Update Agent SUS Client ID</td>
<td>Resets the client ID on the client system. Use this option when cloning a system that is registered with the WSUS server.</td>
</tr>
</tbody>
</table>

5. Click OK.
6. Complete the wizard.

**Run maintenance on a Windows Update agent**

Use Windows Update Agent Maintenance and Repair to manage, install, or reinstall the Windows Update Agent on your remote systems. This will ensure that your remote systems can contact the WSUS server from a remote location and download Microsoft updates.

1. Log in to the Patch Manager Administrator Console as an administrator.
2. In the navigation pane, expand Enterprise and select one or more computers.
   
   For example, you can select Managed Computers and select a workgroup in the center pane.

3. In the Actions pane, click Windows Update Agent Maintenance and Repair.
4. In the dialog box, select one or more maintenance options.
The following table lists the available options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description / Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Re)Install the Windows Update Agent or install</td>
<td>Enter a path (in URL or UNC format) to the Windows Update Agent Installer for your</td>
</tr>
<tr>
<td>Windows Update Agent Update</td>
<td>32-bit (x86) or 64-bit (x64) systems.</td>
</tr>
<tr>
<td></td>
<td>If you provide a path in URL format, ensure the targeted clients can access the URL.</td>
</tr>
<tr>
<td></td>
<td><strong>URL example:</strong> <a href="https://download.windowsupdate.com/windowsupdateagent30-x86.exe">https://download.windowsupdate.com/windowsupdateagent30-x86.exe</a></td>
</tr>
<tr>
<td></td>
<td>If you provide a path in UNC format, ensure that the targeted clients can access the</td>
</tr>
<tr>
<td></td>
<td>server.</td>
</tr>
<tr>
<td></td>
<td><strong>UNC example:</strong> \fileServer\share\windowsupdateagent30-x86.exe</td>
</tr>
<tr>
<td>Delete KB Update Uninstall Directories</td>
<td>Applies to Windows Server 2003 systems.</td>
</tr>
<tr>
<td>Delete Service Pack Uninstall Directories</td>
<td>Applies to Windows Server 2003 systems.</td>
</tr>
<tr>
<td>Change Update(s) Hidden Status To Un-hidden</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description / Action</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Change Update (s) Hidden Status To Un-hidden</td>
<td>Applies to Windows 7 systems.</td>
</tr>
</tbody>
</table>

5. Click OK.

6. Complete the wizard.

**Update the Windows Update Local Policy on remote systems**

When your managed systems are not governed by a Group Policy (GPO), you can configure your Windows Update local policy to access the WSUS server and download the required updates. This procedure is also helpful for managed systems outside of an Active Directory environment.

This configuration requires WMI connectivity with the remote systems. See [Manage client WMI connectivity](#) for details about enabling WMI connectivity between the Patch Manager server and remote systems.

> See the WSUS Deployment Guide located on the [Microsoft Docs](#) website for additional information about deploying updates using WSUS.

1. Log in to the SolarWinds Patch Manager Admin console as an administrator.

2. In the navigation pane, locate and select a system that needs access to the WSUS server and third party updates.

3. In the Actions pane, click Windows Update Local Policy Management.

   The Windows Update Local Policy Settings window displays.
4. Enable the following settings, and then click Save:
   - Specify intranet Microsoft update service location. This setting indicates the WSUS server location.
   - Allow signed content from intranet Microsoft update service location. This setting enables the system to download third party updates.
   - (Optional) Configure Automatic Updates. This enables the system to update automatically by policy.

5. Click OK.

6. Complete the Task Options wizard to schedule or execute the task for one or more remote systems.
   
   See Task Options Wizard for details.

**Move computers between WSUS groups**

When required, you can change the group assignment of a computer by moving the computer to another WSUS.

1. Log in to Patch Manager as an administrator.

2. In the navigation pane, expand Enterprise > Update Services > Your_WSUS_server > Computers and Groups > All Computers.

3. In the top center console, locate and select the computer(s) you want to move.
Press Control to select multiple computers.

4. In the Actions pane, scroll down and select Change Group Membership.
    If Change Group Membership displays in the Action menu, go to step 5.
    If Change Group Membership does not display in the Actions menu:
        a. In the navigation pane, select Patch Manager System Configuration.
        b. Under Patch Manager System Tasks, click Select Products and Features.
        c. Uncheck the WSUS Extension Pack and click Continue.
        d. Log out of Patch Manager.
        e. Repeat step 1 through step 4.

5. Select the groups where these computers should belong, and then click OK.
Advanced configuration options

This section describes advanced configuration options commonly used in distributed Patch Manager environments. Review this section if you use Patch Manager to manage several sites, domains, or business units, or deploy additional SolarWinds Patch Manager servers for load balancing or fault tolerance.

See Advanced deployment scenarios for details about deploying Patch Manager in a distributed environment.

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, and the inventory information for each management group has its own database.

When you install the Patch Manager Primary Application Server (PAS) with the Management Server, Patch Manager automatically creates a management group at Patch Manager System Configuration > Management Groups called Managed Enterprise.

You can have more than one management group defined in Patch Manager, or just use the management group created during the initial installation.

Deploy multiple management groups if you want to:

- Keep information stored in your database for two company segments
- Maintain a separate database for a testing environment

During the configuration, use the Managed Resource Enterprise Configuration wizard to select the resources you want to manage. You can:

- Add a management group
- Add and remove servers and resources
Add a management group

Each management group resides on its own Patch Manager server. When you create a new management group, it must correspond to a new Patch Manager server in the Management Server role.

You can use additional Management Server roles 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 sub-domain.

Use an additional Management Server role with the Application Server role in a testing lab. The additional Management Server role server and testing lab would have its own management group.

1. In the navigation pane, expand Patch Manager System Configuration and select Management Groups.

2. In the Actions pane, click Patch Manager Group Wizard.

3. In the Name field, select or enter a management group name that reflects the group purpose or types of managed devices in the group.

4. Enter a description, and click Next.

5. Select the type of managed scopes to add or remove from the management group, and click Next.
6. Complete the wizard.

7. Repeat step 1 through step 6 for each additional management group.

After you create a management group, you can:

- **Configure managed resources** to the group.
- Deploy a new Patch Manager server in the Management Server role and assign it to the new management group.
- Configure additional managed resources for the new management group.

### Add and remove servers and resources

After you add and configure your Patch Manager management groups, you can:

- **Add or configure a WSUS server**
- **Register an SCCM site server**
- **Add or remove resources from an existing management group**

### Add or configure a 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 Admin Console or add it to an existing management group.

1. Log in to the Patch Manager Admin Console as an administrator.
2. In the Patch Manager menu, expand Enterprise and select Update Services.
3. In the Actions pane, click Add or Configure WSUS Server.

4. Enter the settings for the WSUS server.

   a. In the Server Name field, enter the WSUS server host name and click Resolve.
   
   b. Complete the remaining fields as required.
   
   c. Click Test Connection to test the connection to the WSUS server.
   
   d. Click Save.
Register an SCCM site server

Use the Configuration Manager Site Server Registration Management task to register a Microsoft® System Center Configuration Manager (SCCM) site server with Patch Manager. The site server must be registered with Patch Manager before it is displayed in the Patch Manager Administrator Console.

See Set up Patch Manager with SCCM for details about using Patch Manager in an SCCM configuration.

1. Log in to the SolarWinds Patch Manager Administrator Console as an administrator.
2. In the navigation pane, expand Enterprise and select Configuration Manager Site Servers.
3. In the Actions pane, click Configuration Manager Site Server Registration Management.
4. In the Add/Modify Configuration Manager Site Server window, enter the site server settings.
a. In the Server Name field, enter the site server host name, and click Resolve.
b. Complete any remaining fields as required.
c. Click Save.

Add or remove resources from an existing management group

Use the Management Group wizard to add or remove resources from an existing Patch Manager management group. Before you add a WSUS server to a management group, register the server with Patch Manager.

1. Log in to the Patch Manager Admin Console as an administrator.
2. In the Patch Manager menu, select Patch Manager System Configuration.
3. In the center pane, double-click Configure Patch Manager Management Groups.

4. Click the Name drop-down menu, select a management group to modify, and click Next.
   - The default group is Managed Enterprise.

5. Select the type of managed scope to add or remove from the management group, and click Next.
   - Active Directory Domains or Workgroups
   - This selection will allow you to select Active Directory Domains or Workgroups. Typically these scope types are considered top-level scope objects and can contain other scopes types such as computers and organizational units.
   - Windows Server Update Services Servers
   - This selection will allow you to assign a registered Windows Server Update Services server to a management group. Once assigned to a management group, the WSUS Server and all related information and tasks will be assigned to this management group.

6. Complete the tasks for your selection.

Select Active Directory Domains or Workgroups

If you selected Windows Server Update Services Servers, perform the following steps:
1. In the Name field, click [...] to open the network browser.

2. Select the targeted resource in the Enterprise menu.

3. In the right pane, select the resource you want to add, and click Add Selected.

4. Repeat step a through step c for each additional resource.

5. Click OK.

6. Go to Complete the wizard.

Select Windows Server Update Services Servers

If you selected Windows Server Update Services Servers, perform the following steps:

1. Click the Server drop-down menu and select the WSUS server.

2. Complete the remaining fields as required.

3. Complete the wizard

Complete the wizard

1. Click Next.

2. Review the selections in the Management Group Summary window, and click Finish.
Assign a new Patch Manager server to a management group

1. Log in to the Patch Manager Admin Console.
2. In the navigation pane, expand Patch Manager System Configuration and select Patch Manager Servers.

3. In the Actions pane, click Patch Manager Server Wizard.
4. In the Patch Manager Server Configuration Wizard, select Edit an existing Patch Manager Server’s configuration settings, and click Next.
5. Enter your Patch Manager server configuration settings.
a. Click the Server Name drop-down menu and select the new server.
b. Click Resolve to populate the fields.
c. Complete any remaining fields, and click Next.

6. Associate the Patch Manager server with a management group.

   a. Click the Management Group drop-down menu and select a management group.
   b. Configure the remaining settings, and click Next.

   See the system requirements for the Patch Manager port requirements.

7. On the Summary page, verify the settings for the new server.

8. Click Finish.
Install the Patch Manager Administrator Console on a remote system

In a standalone configuration, the Patch Manager Administrator Console is installed on a server hosting the Primary Application Server role. If your deployment is spread across a wide geographical area and you cannot access the Patch Manager Administrator Console running on the Primary Application Server, install an additional administrator console on a remote server in your environment. This server can be any Patch Manager server in an Application Server role.

When you install the Patch Manager Administrator Console on a remote server using the Patch Manager software installer, associate the remote console and server with a server hosting the Application Server role.

If you plan to integrate SolarWinds Patch Manager with SCCM, install all SolarWinds Patch Manager administrator consoles on systems currently running SCCM.

1. Locate the Patch Manager installer you downloaded from the SolarWinds Customer Portal.
2. Temporarily disable the anti-virus software on the targeted server.
3. Run the Patch Manager installer on the targeted server.
   
   If the server is missing C++ Runtime or Microsoft .NET Framework, click Install to allow the installation wizard to install the missing component(s).

4. In the Installation Type window, select Install the Patch Manager Administration Console, and then click Next.
5. In the Patch Manager Installation Wizard window, click Next.
6. If Patch Manager is integrated with the Orion Platform, click Yes to create a backup of your Orion database, and click Next.
7. If you accept the terms in the End User License Agreement, click Next.
8. Click Next to use the default installation folder or click Browse to select a different folder.
9. Select Advanced Install, and click Next.
10. Click Next to install the selected Patch Manager components.
11. Click Next to begin the configuration wizard.
12. Select Application Server, and click Next.
13. Enter the host name of the Patch Manager Primary Application Server (PAS), and then click Test
to ensure the computer can connect to the PAS.

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.

14. Click Next.

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

16. Click Next.

17. If you do not have a WSUS server, select Install the Patch Manager WSUS service (recommended), and click Next.
   If you have a WSUS server, select I’ll supply my own WSUS server, and click Next.

18. Select how Patch Manager should configure IIS.

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

20. Select Provision the WSUS Server to the Patch Manager to manage WSUS from Patch Manager, and click Next.

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

22. Select your SQL instance, enter the credentials, and click Next.

23. Select Use the default service account or enter different service account credentials for Patch Manager, and click Next.

24. Click Finish.

Configure additional Patch Manager servers

Patch Manager is installed on a dedicated server running the Primary Application Server role. This role hosts the primary configuration management database and serves as the Certificate Authority for all certificates used to register and encrypt Patch Manager communications.

All Patch Manager operations are controlled from this server. When you install Patch Manager for the first time, the host server is called the Primary Application Server (PAS).

You can add additional server roles on remote systems to add additional functionality. The following table lists the additional server roles included with Patch Manager.
The Patch Manager installer includes an Express option that allows you to install an evaluation version of Patch Manager and SQL Server Express. Select the Advanced Install option to install the additional server roles. SolarWinds recommends installing these server roles on separate, dedicated servers to maximize application performance.

<table>
<thead>
<tr>
<th>Server Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Server</td>
<td>Interfaces with the Patch Manager Admin Console or integrated SCCM administration consoles, and manages all communications between the console and the Patch Manager deployment.</td>
</tr>
<tr>
<td>Automation Server</td>
<td>Manages the local Patch Manager processes on each Patch Manager server. Each Automation server performs the inventory and configuration management tasks and interfaces with the Windows Management Instrumentation (WMI) providers to collect data and supervise remote management functions. An Automation server can also resolve API mismatch errors that can occur when you publish to the WSUS server. This issue occurs when Patch Manager and WSUS are installed on servers running disparate Windows Server operating systems. See <a href="#">Set up an Automation Server</a> for installation and configuration instructions.</td>
</tr>
<tr>
<td>Management Server</td>
<td>Maintains all inventory and discovery data for specific systems in the Patch Manager environment. Each Management server includes a defined collection of managed entities specified by their corresponding domain, workgroup, or WSUS server.</td>
</tr>
</tbody>
</table>
Manage users and security

Patch Manager uses the following components to manage security in the Patch Manager Administrator Console:

- **Credentials** that you assign to credential rings to grant Patch Manager access to managed resources
- **Credential rings** to map credentials to managed resources
- **Security roles** to grant or deny console users to application functionality
- **User preferences** to create and manage profiles for specific Microsoft® Windows® users with access to the Patch Manager Administrator Console
- **Server certificates** to encrypt all communications between Patch Manager servers and the console sessions
- **Patch Manager Web Console user accounts** to access the console on the Orion server

You can select and map your credentials to specific resources in the default credential ring during the initial setup. As you become more familiar with the product and expand your deployment, these security components help you configure Patch Manager to function efficiently and securely.

Patch Manager uses specific user credentials to manage security in the Patch Manager Web Console. See Web Console User Accounts for details.

The security management tasks described in this section are available regardless of the Microsoft product you are extending. Although you cannot perform these functions from within the SCCM console, all of the Patch Manager functionality is available in the Patch Manager Admin Console. See Set up Patch Manager with SCCM for details.

Credentials

Credentials are pairs of user names and passwords that you assign to credential rings to grant Patch Manager access to managed resources. Patch Manager stores user credentials in the Patch Manager database. Using the Patch Manager Admin Console, you can manage all user credentials in your deployment.

Be sure to update credentials when a user name or password changes in your Microsoft® Windows® operating system.
Manage user credentials

The Security and User Management node in the Patch Manager Admin Console contains tabs that display your security and user settings.

In this node, you can:

- Add a new credential
- Change the credential password
- Delete existing credentials

Add a new credential

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

1. Log in to the Patch Manager Administrator Console as an administrator.
2. In the navigation pane, expand Patch Manager System Configuration and select Security and User Management.
3. In the center pane, click the Credentials tab.
4. In the Actions pane, click Add Credential.
5. In the Add User window, enter the new user name in User Principle Name (UPN) format (such as JoeAdmin@example.com) or pre-Windows 2000 format (such as DOMAIN\userName).

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.
6. Enter and confirm the new password.

7. Click Save.

When you add a new credential, map it to the appropriate resources using the Credential and Credential Ring Rules Wizard. See Managing Credential Rings for details.

Change the credential password

When you change a user account password in Microsoft Windows, you must change the corresponding credential password in Patch Manager.

1. Log in to the Patch Manager Admin Console as an administrator.

2. In the navigation pane, expand Patch Manager System Configuration and select Security and User Management.

3. In the center pane, click the Credentials tab.
4. Select the credential you want to modify.
5. In the Actions pane, click Change Password.
6. In the Change Password window, enter and confirm the new password.
7. Click Save.

Delete a credential

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

1. Log in to the Patch Manager Admin Console as an administrator.
2. In the navigation pane, expand Patch Manager System Configuration and select Security and User Management.
3. In the center pane, click the Credentials tab.
4. Select the credential you want to delete.
5. In the Actions pane, click Delete.
6. Click Yes to confirm.

If the credential is associated with one or more managed resources, map the resources to a new credential in the Credential and Credential Ring Rules Wizard. See Managing Credential Rings for details.

Credential rings

Patch Manager uses credential rings to map credentials to managed resources. This allows Patch Manager to know which credentials 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 setup and configuration. During the configuration process, you can map the credentials to the corresponding resources using rules. In a credential ring, you can set up the Default rule and rules for:

- WSUS servers, SCCM site servers, or specific computers
- Active Directory Organizational Units (OUs)
- Active Directory domains or workgroups

As you add and delete credentials in Patch Manager, be sure to add the credentials to a credential ring and modify these rules to map them to the appropriate resources.

### Add new credentials to a credential ring

Use the Credential and Credential Ring Rules Wizard to add new credentials to a credential ring. When you are finished, the wizard adds the credentials to the Patch Manager database and maps those credentials to the targeted resources.

1. Log in to the Patch Manager Admin Console as an administrator.
2. In the navigation pane, expand Patch Manager System Configuration and select Security and User Management.
3. In the center pane, click the Credential Rings tab.
4. Select the credential ring you want to modify.
5. In the Actions pane, click Credential Ring Wizard.
6. In the Credential and Credential Rings Rules Wizard, enter the credentials you want to add to the Patch Manager database.
   
a. In the User Name field, click the drop-down menu and select a user name or enter a name in UPN or flat format.

   \begin{center}
   \textbf{Step 2: Select an existing credential or add new credential information}
   \end{center}
   
   Specify credentials using fully qualified user names. Names can be specified in either UPN format or flat format. For example, useradmin@corp.contoso.com or CONTOSO\useradmin. To specify a local machine account that is common across computers, specify a \ before the user name.

   \begin{tabular}{|l|}
   \hline
   User Name: \\
   Password: \\
   Confirm Password: \\
   \hline
   \end{tabular}

   For example, enter \texttt{user@domain.example.com} (UPN format) or \texttt{DOMAIN\user} (flat format).

   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 the user account.
   c. Click Add.
   d. Repeat step a through step c for each additional account you want to add.

7. Click Next.

8. Create credential ring rules to map credentials to the targeted resources.

   If you do not map a resource to a specific credential, Patch Manager uses the default rule to choose credentials for that resource.
a. Click Add Rule and select the type of rule you want to add.

b. In the Select Computer window, browse the left pane until the resource you want to add is in the upper-right pane.

c. Select the resource you want to add, and click Add selected.

   The dialog box varies, depending on your selected rule type.

d. Repeat step a through step c for each resource you want to add.

e. Click OK.

f. In the Select User for Credential Rule window, select the credential you want to map to the resource and click OK.

g. Repeat step a through step f for each additional rule you want to add.

9. Click Finish.

**Security roles**

Patch Manager uses security roles to grant or deny console users to application functionality. Each role grants access to specific functionality in the application. This allows you to create a granular security management architecture.

The Patch Manager security roles can be divided into the following categories:

- Default roles
- Operational roles
- Special roles

As your organization grows, you can add or remove users from a security role.
Default roles

By default, Patch Manager includes the server local Administrators group in the following security roles:

- EminentWare User role
- EminentWare Enterprise Administrator role

In Active Directory environments, users in the Domain Admins group are default members of the local Administrator group for all domain members. 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 required.

EminentWare User role

This role grants access to the Patch Manager Administrator Console. To use the console, users must be a member of the EminentWare User role and at least one security role.

EminentWare Enterprise Administrator role

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 Administrator Console.

Microsoft® Windows® users outside of this security role could potentially alter memberships by using the MMC Authorization Manager snap-in or altering the EminentWare.BusinessObjects.xml file.

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

Patch Manager stores all authorizations in the following location:

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

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

Operational roles

Use the following operational roles to grant access to everyday functions in the Patch Manager console in either Administrators or Viewers capacity:
The following table lists the functions for each operational role.

<table>
<thead>
<tr>
<th>Access To:</th>
<th>Administrators Can:</th>
<th>Users Can:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer configuration</td>
<td>View, create, modify, or delete information obtained from direct connections to managed computers. For example, information gathered using Windows Management Instrumentation (WMI), WMI-based tasks, such as Computer Explorer, Update Management, and Update Management Wizard tasks.</td>
<td>View the information about managed computers.</td>
</tr>
<tr>
<td>EminentWare reports</td>
<td>View, create, modify, or delete EminentWare reports in the Patch Manager Administrator Console.</td>
<td>View EminentWare reports.</td>
</tr>
<tr>
<td>WSUS servers</td>
<td>View, create, modify, or delete information involving WSUS servers.</td>
<td>View information about WSUS Servers.</td>
</tr>
<tr>
<td></td>
<td>Similar to WSUS Administrators group on the WSUS servers.</td>
<td></td>
</tr>
</tbody>
</table>

**Special roles**

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

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

The following table lists the functions for each special role.

<table>
<thead>
<tr>
<th>Access To:</th>
<th>Administrators Can:</th>
<th>Users Can:</th>
</tr>
</thead>
<tbody>
<tr>
<td>EminentWare Computer Group Administrator</td>
<td>Access and manage all Patch Manager computer groups</td>
<td>Create, modify, or delete Patch Manager computer groups from within the Patch Manager Administrator Console</td>
</tr>
<tr>
<td>Access To</td>
<td>Administrators Can</td>
<td>Users Can</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WSUS Approval Delegation Administrator</td>
<td>Access and administer WSUS approval delegation</td>
<td>Enable or disable approval delegation for a WSUS target group, grant or revoke accounts’ approval privileges, and modify the account update classifications</td>
</tr>
<tr>
<td>EminentWare Security Administrator</td>
<td>Access and administer user and credential management functions in the Patch Manager Administrator Console</td>
<td>Manage credentials, credential rings, and user preferences</td>
</tr>
</tbody>
</table>

Add or remove users from a security role

Perform the following steps to add or remove users from a `default`, `operational`, or `special` security role in Patch Manager.

1. Log in to the Patch Manager Admin Console.

2. In the navigation pane, expand Patch Manager System Configuration and select Security and User Management.

3. In the center pane, click the Security Roles tab.

4. Select the security role you want to modify.

5. **Add** or **remove** users from the role.
Add a new user

1. Click Add in the Actions pane.
2. In the Select Users and Groups window, expand Enterprise and select a user or user group you want to add.
3. Select the user or group to add in the center pane and click Add Selected.
4. Repeat step 2 and step 3 for each additional user or group and click OK.

Remove an existing user

1. Select the user you want to remove in the lower-center pane.
2. In the Actions pane, click Remove.

User preferences

Use the User Preferences tab in Security and User Management to create and manage profiles for specific Microsoft® Windows® users with access to the Patch Manager Administrator Console.

If a Patch Manager Administrator Console user does not have a specific profile in the User Preferences tab, Patch Manager uses the Default profile when this user connects to a console.

Patch Manager includes a default profile that applies user properties to all users. You can also add users and apply specific preference settings to each user profile.

Preference settings

When you add a new user, Patch Manager opens the Preference Settings window, which includes tabs for each user preference setting.

The following table describes the settings in the Preference Settings window.
### Setting | Description
--- | ---
**General** | Applies the following user preferences to all user profiles:
- Credential Ring: Assigns a specific credential ring to each user profile. Patch Manager assigns the Default credential ring to the Default user profile during setup, but you can modify this setting.
- Export Directory: Specifies 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: Specifies the preferences Patch Manager passes to `mstsc.exe` to establish the following RDP connection settings:
  - Default screen resolution
  - Using an alternate port for RDP Connection
  - Connecting to the console session on the selected computer

| Management groups | Limits profile access to specific Patch Manager management groups. Patch Manager allows the Default user profile access to all management groups. |
| WSUS servers | Displays specific WSUS servers within an associated management group in the Patch Manager navigation pane. Patch Manager allows the Default user profile access to all associated WSUS servers. |
| Patch Manager Computer Groups | Limits profile access to specific Patch Manager computer groups. Patch Manager allows the Default user profile access to all computer groups. |
| Domains and Workgroups | Limits profile 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. |
Specify preferences for a user profile

1. Log in to the Patch Manager Admin Console as an administrator.

2. In the Patch Manager console, expand Patch Manager System Configuration and select Security and User Management.

3. In the center pane, click the User Preferences tab.

![User Preferences tab in Patch Manager console]

To modify the preferences for an existing profile:

a. Select the user profile.

b. In the Actions pane, click Edit.

To add a new user profile:

a. In the Actions pane, click Add User.

b. In 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.

d. Click Add selected, and then click OK.

4. Specify the preferences settings for the user profile.

5. Click Save.

Server certificates

Patch Manager uses a 2048-bit security certificate to encrypt all communications between Patch Manager servers and the console sessions.

A single SolarWinds Patch Manager server includes at least two certificates:

- Certificate installed on the Primary Application Server (PAS) for the certificate authority (CA)
- Certificate for each server installation (which includes the PAS)

When Patch Manager revokes a certificate, it indicates this action at the beginning of the certificate name. This process occurs when you replace a certificate or uninstall a Patch Manager server. In these cases, you can delete the revoked certificate.
Delete a Patch Manager certificate

1. Log in to the Patch Manager Admin Console as an administrator.

2. In the navigation pane, expand Patch Manager Server System Configuration and select Security and User Management.

3. In the center pane, click the Server Certificates tab.

4. Select the certificate you want to delete.

5. In the Actions pane, click Delete.

6. When prompted, click Yes.

   The certificate is deleted.

Deploy a Patch Manager certificate using Group Policy

You can deploy a certificate to multiple computers by using the Active Directory Domain Services and Group Policy Object (GPO). This procedure is useful each time a certificate needs to be pushed to clients. For example, you can use this procedure to push a WSUS self-signed or CA-signed certificate to all of your clients before they can trust the published third party packages.

See Deploy certificates using Group policy for details.

Web Console user accounts

The Patch Manager Admin Console and Web Console implement separate user accounts and passwords. To add the Patch Manager Web Console to your deployment:

1. Install and configure the Patch Manager Web Console on the Orion server.

2. Add a Patch Manager user account for each Patch Manager Web Console user or role.
Roles allow you to limit the Patch Manager Web Console views available to specific groups of users.

3. Define the user account settings for each user account to add or restrict access to the Patch Manager Web Console and additional dashboards in the Orion Web Console.

Add a Patch Manager user account

When you set up a Patch Manager Web Console account, you can create one of the following accounts:

- **Orion individual account**
- **Windows individual account**
- **Windows group account**

Orion and Windows accounts require different types of user authentication.

When you create an Orion individual account, Orion uses the user name and password to authenticate each user. Users must enter these credentials each time they access the Orion Web Console.

When you create a Windows individual or group account, Orion uses the Active Directory database to authenticate each user. You can also implement pass-through authentication so users are not required to enter a name and password to access the Orion Web Console.

Before you create a new account, consider what tasks the user must perform, and what views and menu bars are most suitable. Users created using default settings can log in to the Orion Web Console and see information available in views, resources, and reports. For administration and customization tasks, users require additional rights.

Create an Orion individual account

Use Windows individual accounts to enable Windows users to log in to the Orion Web Console with their local or domain Windows accounts. These accounts are independent of any local or Active Directory account or group.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings.
3. Scroll down to User Accounts and click Manage Accounts.
4. In the toolbar, click Add New Account.
5. Select Orion Individual account, and click Next.

6. Enter the user name and password for the account, and click Next.

7. Define the account settings, and then click Next.

8. Complete the settings for this account.

   Click Help in the toolbar for assistance.

9. Click Submit.

Create a Windows individual account

Use Windows individual accounts to enable Windows users to log in to the Orion Web Console with their local or domain Windows accounts. Perform the following steps to enable Windows users to access the Orion Web Console using their existing local or domain Windows accounts.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings.
3. Scroll down to User Accounts and click Manage Accounts.
4. Click Add New Account.
5. Select Windows individual account, and click Next.
6. Enter the account credentials.
   a. Select an account to access Active Directory or the local domain or specify the credentials in the User Name and Password fields.
   
   ![Image of Active Directory or Local Domain Authentication]
   
   In the User Name field, use the `DOMAIN\userName` format.

   ![Image of Search for Account]
   
   This field requires the domain and at least a partial user name in `DOMAIN\userName` format. If the exact user name is not available, use * as a wildcard character to represent the unknown portions. For example, enter `DOMAIN\Jimmy*`.

   b. Test the Active Directory connection (if required).
   
   c. Enter a search string for the user account you want to add as a Patch Manager Web Console user.

   ![Image of Search for Account]
   
   d. Click Search.
   
   e. Select the user(s) you want to add, and click Next.

7. Define the account settings for the new users in this Windows group. Provide the rights so the
user can perform assigned tasks, and select default views and menu bars.

Click Help in the toolbar for assistance.

8. Click Submit.

Create a Windows group account

Windows group accounts are designated for previously configured local or Active Directory group accounts. Perform the following steps to enable users to use their existing Active Directory credentials to log in to the Orion Web Console.

To maintain administrative privileges, individual and group Windows user accounts must be defined in the same domain as the SolarWinds server they can access. Additionally, only Security Active Directory groups are supported. Distribution groups are not supported.

1. Log in to the Orion Web Console as an administrator.

2. Enable Windows Account Login in the Orion Web Console.
   a. Click Settings > All Settings.
   b. Scroll down to Product Specific Settings and click Web Console Settings.
   c. In Windows Account Login, select Enable automatic login, and click Submit.

3. Click Settings > All Settings.

4. Scroll down to User Accounts and click Manage Accounts.

5. Click Add New Account.

6. Select Windows group account, and click Next.

7. Provide the credentials for an account with administrative access to the Active Directory or local domain.
If a system account is available, select Use [Account Name] account to access Active Directory or Local Domain, and click Test Active Directory.

This option is not available when LDAP is enabled. In this scenario, manually enter the credentials.

If a system account is not available, select Specify credentials to access Active Directory or Local Domain, and provide the credentials. In the User Name field, use the `<domain\username>` format. To search for all users or groups in the domain, enter `<domain name\*>`.

8. Click Search.

9. Select the group(s) you want to add, and click Next.

10. Define the account settings for the new users in this Windows group. Provide the rights so the user can perform assigned tasks, and select default views and menu bars.

   Click Help in the toolbar for assistance.

11. Click Submit.

   Users can now log in to the Orion Web Console using their local domain or Active Directory credentials.
If you use Active Directory, users can also automatically log in with their Windows credentials.

**Define the user account settings**

When you create new users in the Orion Web Console, you can configure the user settings to limit what each user can access in the console. You can modify user settings at any time, either individually or in batches. Only Orion Web Console users with administrator rights have permission to change the user settings.

See [Customize the Patch Manager Widgets](#) for details about defining a user’s account settings to modify the Patch Manager Summary widgets.

1. Log on to the Orion Web Console as an administrator.
2. Click Settings > All Settings.
4. Select the user you want to modify, and click Edit.
   
   If you select multiple users, select the specific setting you want to modify.
5. In the Edit Account screen, modify the user settings as required, and click Submit.
   
   See [Patch Manager Web Console User Settings](#) for setting descriptions.
6. Click Submit.
Manage client WMI connectivity

Patch Manager installs SolarWinds Client Components whenever a connection is first established to any machine.

Initially, it uses the WMI Providers if you prefer not to use a Patch Manager agent. If you decide to use a Patch Manager agent, it communicates to Patch Manager through port 4092.

WMI requirements

The following table lists the WMI requirements required by systems running Microsoft® Windows® operating systems to establish a successful WMI connection with a remote system.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed Component Object Model (DCOM)</td>
<td>Remote systems</td>
</tr>
<tr>
<td>File and Print Sharing</td>
<td></td>
</tr>
<tr>
<td>RPC Service</td>
<td></td>
</tr>
<tr>
<td>WMI Firewall Exception</td>
<td></td>
</tr>
<tr>
<td>Credentials with Local Administrator rights</td>
<td>Remote systems in the credential ring</td>
</tr>
<tr>
<td>DCOM</td>
<td>Local systems</td>
</tr>
</tbody>
</table>

WMI technology is based on DCOM / Remote Procedure Call (DCOM/RPC) communication. DCOM/RPC allocates the ports used by the server within a dynamic port range—typically between ports 1024 and 65536. To configure these ports using Windows Firewall on your managed computers, enable the Inbound Rules in the WMI group. See the Microsoft operating system documentation for details.

Ports 135, 445, and dynamic ports 1024 to 65536 must be open between Patch Manager and the remote system. See Port requirements for all SolarWinds products to review all Patch Manager ports.

WMI Providers security and permissions

By default, Patch Manager automatically deploys the WMI providers when required for specific configuration management tasks. WMI Providers runs as a process on the remote system when needed and does not run as a service.
By default, SolarWinds WMI Providers run under their own process using the Local System account, impersonating the security context of the caller. They use the appropriate credential stored in the Patch Manager database as assigned by the user credential ring.

See Manage Patch Manager users and security for details.

## Install the SolarWinds WMI Providers

The SolarWinds WMI Providers provide additional management and inventory tools that are not native to WSUS. Without them, you can only use Patch Manager to interface with WSUS and not directly with any managed clients.

The following table lists the actions you can perform in Patch Manager with and without WMI Providers.

<table>
<thead>
<tr>
<th>Without WMI Providers, you can...</th>
<th>With WMI Providers, you can...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish third-party updates to the WSUS server</td>
<td>Deploy updates on demand using the Update Management and Update Management Wizard tasks</td>
</tr>
<tr>
<td>Perform all WSUS administrative functions</td>
<td>Conduct a managed computer inventory to retrieve detailed information about managed clients</td>
</tr>
<tr>
<td>Conduct a WSUS Inventory for details about your WSUS servers</td>
<td>Perform configuration management tasks, such as shutting down or restarting computers, refreshing the group policy, and managing client certificates</td>
</tr>
<tr>
<td>Conduct a WSUS Extended Inventory to access a basic collection of system-level inventory data</td>
<td>Use Computer Explorer to browse computer details and launch configuration management tasks</td>
</tr>
</tbody>
</table>

Use the following procedures to manually deploy the SolarWinds WMI Providers to your managed clients.

See Set up Patch Manager with SCCM for deploying WMI Providers in an SCCM deployment.

## Enable or disable the SolarWinds WMI Providers

By default, Patch Manager automatically deploys the WMI providers. If you disable the Automatically provision SolarWinds WMI Providers option, Patch Manager no longer deploys the WMI providers to the managed computers as needed for specific configuration management tasks. You must manually deploy the SolarWinds WMI Providers before Patch Manager can use them.

You can enable or disable WMI Providers in the Patch Manager Administrator Console. After they are enabled, Patch Manager can use them for configuration management.
See Set up Patch Manager with SCCM for deploying WMI Providers in an SCCM deployment.

1. In the navigation pane, expand Patch Manager System Configuration and select Management Groups.

   For example, Managed Enterprise.

2. In the center console, select the management group for the WMI Providers.

3. Select the Settings tab.

4. Under Setting Name, double-click Automatically provision SolarWinds WMI Providers.

5. Select Enabled or disabled as required.

6. Click OK.
Install the SolarWinds WMI Providers on a group of client computers

1. In the navigation pane, locate and select the group that require WMI Providers.
   For example, Managed Computers.

2. Run the task.
   To run the task for all affected computers, select the group and then click Check and Manage Computer Connectivity in the Actions pane.
   To run the task for a specific computer in the group, select the computer in the center pane and then click Check and Manager Computer Connectivity in the Actions pane.

3. In the Computer Access Management window under SolarWinds WMI Provider Actions, select Install the WMI providers (if not already selected) and any additional options.

4. Select any additional options **except Enable DCOM if disabled**.
5. Click OK to run the task.

See [Task Options Wizard](#) for more information.

If the task fails and generates an error, see [Troubleshoot "Access Denied" errors in Patch Manager](#).

**Install the SolarWinds WMI Providers on specific client computers**

Use the following procedure to install the WMI Providers to selected client systems immediately using the Remote Install Service.

1. Log in to the Patch Manager Administrator Console as an administrator.

2. In the navigation pane, expand Enterprise > Managed Computers.

3. In the Managed Computers pane, select a computer.

4. In the Actions pane, click Deploy Client Components.

5. Select Install or Repair Client Components, and click Next.

6. Select Install WMI Providers, and click Next.

7. Select Install using Remote install Service, and click Next.
8. Select the clients you want to deploy the components, and click Next.
9. Verify your selections, and click Finish.

**Verify WMI connectivity**

After you [deploy the WMI Providers](#) in your environment, use the Inventory – verify access only Managed Computer Inventory option to verify WMI connectivity with your remote systems.

- If you cannot connect to your Patch Manager clients using WMI, see [Unable to connect to clients using WMI](#) for troubleshooting.
- If you integrated Patch Manager with SCCM, see [System Center Configuration Manager 2012 Procedures](#) for details about verifying WMI connectivity.

1. Log in to the Patch Manager Administrator Console as an administrator.
2. In the navigation pane, expand Enterprise and select Managed Computers.
3. In the center pane, select the computer you want to verify.
4. In the Actions pane, click Inventory.
5. In the Inventory Options window, select Inventory – verify access only, and click OK.

   - **Inventory - verify access only**
   
   Select this option to verify access to the selected computers which will check for TCP and WMI connectivity as well as required administrative permissions. The detailed results of the inventory can be viewed in the Patch Manager Managed Computers view.

6. Complete the Task Options Wizard to specify the target systems and schedule and execute the task.

   See [Task Options Wizard](#) for more information.

- You can view the results from this verification in the Patch Manager Task History, or configure a task that sends you the results by email.
# Troubleshoot the WMI connections

After you target remote systems for a Managed Computer Inventory task, Patch Manager lists the targeted systems in the Managed Computers node. Select a system in the center pane to view the WMI connectivity details and troubleshoot the WMI connection. These systems include WSUS servers, SCCM servers, and managed clients in your corporate enterprise.

## View WMI connectivity details

The Enterprise > Managed Computers node in the navigation pane displays the systems included in one or more Managed Computer inventory events, including all Patch Manager and WSUS servers. When you select the Managed Computers node, Patch Manager displays the WMI connection status of each managed computer in the center pane.

When a managed system has a WMI connectivity issue, the console displays the system in the center pane with a connection failure 🚲 or warning 🚸 status icon in the Name column.

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>AB</td>
<td>🚲</td>
<td></td>
</tr>
<tr>
<td>AB01</td>
<td>🚸</td>
<td></td>
</tr>
<tr>
<td>APE01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AVILLAR-VM</td>
<td>🚸</td>
<td></td>
</tr>
<tr>
<td>DC01</td>
<td>🚸</td>
<td></td>
</tr>
<tr>
<td>DC02</td>
<td>🚸</td>
<td></td>
</tr>
</tbody>
</table>

Click the Computer Details tab in the center pane to display the WMI connectivity issues for your selected system.
In some cases, the Last statuses (such as Last DNS resolution attempt) can report Success while Patch Manager returns a connection error in the Computer Details tab. In these cases, troubleshoot the specific data source or object cited in the error message or modify your Inventory task to exclude the target data source.

1. Log in to the Patch Manager Administrator Console as an administrator.

2. In the navigation pane, expand Enterprise, and select Managed Computers.

3. In the center pane, select a computer.

4. In the center pane, click the Details tab.

5. Review the following connection attempts:
6. Troubleshoot any Failed statuses using the table below.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last DNS resolution attempt</td>
<td>Shows the status for resolving the computer name Patch Manager obtained from the computer container defined in the Inventory task. The status can be Success for Failed.</td>
<td>If the status is Failed, check the network DNS records and the local hosts file (if applicable).</td>
</tr>
<tr>
<td>Last ARP resolution attempt</td>
<td>Shows the status for resolving the IP address Patch Manager obtained from DNS. After Patch Manager resolves the IP address, it stores the MAC address in the computer record. The status can be Success or Failed.</td>
<td>If the status is Failed, ensure that the Patch Manager server can access the DNS server.</td>
</tr>
<tr>
<td>Last Endpoint Mapper connection attempt</td>
<td>Shows the status for connecting to the RPC Endpoint Mapper (port 135) on the remote system. The status can be Success or Failed.</td>
<td>If the status is Failed and DNS resolution was successful, verify that the firewall is not blocking traffic to the remote system on port 135.</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
<td>Action</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last File and Printer Sharing connect attempt</td>
<td>Shows the status for establishing a file sharing session on port 445 using Server Message Block (SMB) over IP. The status can be Success or Failed.</td>
<td>If the status is Failed, ensure that the File and Print 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.</td>
</tr>
<tr>
<td>Last WMI connect attempt</td>
<td>Shows the status for establishing the WMI session. The status can be Success or Failed.</td>
<td>If the status is Failed and the previous statuses are Success, ensure that 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.</td>
</tr>
</tbody>
</table>

If you cannot connect to your Patch Manager clients using WMI, see [Unable to connect to clients using WMI](#) for additional troubleshooting.

## Resolve WMI connection issues

If you encounter an issue (such as a Failed status) with WMI connectivity to a remote system, verify the connection to the managed computers. If you cannot connect to the computers, install the WMI Providers or an agent.

### Verify the connection to the managed computers

Use the Check and Manage Computer Connectivity action to verify the connection to the managed computers. This action launches the same dialog box used to provision the WMI Providers to remote systems. You can execute this action from the Enterprise > Managed Computers view.

1. Log in to the Patch Manager Web Console as an administrator.
2. In the navigation pane, expand Enterprise and select Managed Computers.
3. In the center pane, select the targeted computer.

4. In the Actions pane, click Check and Manage Computer Connectivity.

5. In the Computer Access Management window, select the appropriate options, and click OK.

6. Complete the Task Options Wizard to specify the target systems and schedule and/or execute the task.

   See Task Options Wizard for more information.

   If you cannot connect to the managed computers, install the WMI Providers or a Patch Manager agent (for remote computers).

**Install the WMI Providers or an agent**

1. Log in to the Patch Manager Web Console as an administrator.

2. In the navigation pane, expand Enterprise.

3. Locate and select the computer that requires an agent. You can:
   - Select Managed Computers and then select the targeted computer in the center console.
   - Expand Update Services > WSUS_server > Computers and Groups > All Computers, locate and select the computer that requires an agent.

4. In the Actions pane, click Deploy Client Components.

5. Select Install or Repair Client Components, and click Next.

6. Select an option:
   - Install WMI Providers
   - Install the Patch Manager Agent (for remote computers)

7. Select an option:
   - Install using Remote Install Service
   - Create a WSUS Installer Package
Install using Remote Installer Services

If you choose Remote Installer Services, the wizard launches a task to install the agent with Patch Manager. Complete the steps in the task.

Create a WSUS Installer Package

1. Expand Administration and Reporting > Software Publishing and select SolarWinds Inc. Packages.
2. In the center pane, locate and select the SolarWinds Patch Manager Agent package.
3. Publish the package to your WSUS.
4. Approve the package for your groups.

Computer Actions Management window

The Computer Access Management window includes the SolarWinds WMI Provider Actions box, which provides options to install, reinstall, or uninstall the SolarWinds WMI Providers.

The following table describes the actions.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check if WMI Providers are installed</td>
<td>Checks the WMI Providers on the remote system. You can view the results from this check in the Patch Manager Task History or configure the task to email you the results.</td>
</tr>
<tr>
<td>Install the WMI Providers if not already installed</td>
<td>Installs the WMI Providers (if needed). This option also allows you to reinstall the WMI Providers when required.</td>
</tr>
<tr>
<td>Uninstall the WMI Providers</td>
<td>Uninstalls the WMI Providers from the remote system.</td>
</tr>
</tbody>
</table>

The Computer Access Management window includes additional options to configure remote systems that allow WMI connections.
The following table lists the available settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable DCOM if disabled</td>
<td>Enables Distributed COM (DCOM) on the remote system. This setting is required for Patch Manager to enable WMI Providers to connect to the remote systems.</td>
</tr>
<tr>
<td>Configure DCOM permissions to include 'Administrators' group if needed</td>
<td>Modifies the DCOM permissions to include users from the Windows Administrators group. Patch Manager requires local Administrator permissions on remote systems to run the WMI Providers.</td>
</tr>
<tr>
<td>Enable the 'Remote Administration' firewall rule</td>
<td>Enables the Remote Administration firewall rule set in the Windows Firewall. If you are using a third-party firewall solution, configure the required rules in your firewall through other means.</td>
</tr>
<tr>
<td>Create ADMIN$ share if missing</td>
<td>Creates the ADMIN$ share on Windows systems.</td>
</tr>
<tr>
<td>Enable Windows Installer service if disabled</td>
<td>Re-enables the Windows Installer service on the remote system. Patch Manager requires this service to install the WMI Providers.</td>
</tr>
<tr>
<td>Enable MSI Logging</td>
<td>Enables MSI logging on the remote system. This option is selected by default.</td>
</tr>
</tbody>
</table>
Additional requirements for Windows XP systems

If you are troubleshooting a system running Windows XP in a workgroup, configure the Windows XP Workgroup clients to allow WMI connections.

1. Open the Registry Editor (regedit.exe) on the Windows XP system.
2. Expand:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
3. Select Lsa.
4. Change the value for 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.
Patch Manager agents

Patch Manager is an agentless patch deployment solution that uses Windows Management Instrumentation (WMI) to manage computers in an organization. You may encounter situations where an agent is the best solution in your environment. These situations include:

- Computers that cannot be managed with WMI
- Computers that are protected by stringent firewall rules or virtual private networks (VPNs)

In these situations, Patch Manager agents provide the best option for patching computers that are offline most of the time.

Ensure that each managed computer meets the agent requirements. After you deploy, approve, and configure the Patch Manager agent on the managed computer, the agent contacts the Patch Manager server (or Primary Application Server) using a secure connection and requests a certificate exchange. The certificate provides mutual authentication and must be installed on the managed computer before the agent can perform any tasks. Agents with exchanged certificates display in the Approved category in the Patch Manager Administrator Console.

You can deploy pre-provisioned agents that have exchanged certificate information. These agents poll the server at preconfigured intervals using asynchronous remote procedure calls (RPC).

Agent requirements

Ensure that the client systems that require a Patch Manager agent meets the following requirements:

- **Managed system requirements**
  - 30 MB or more of available RAM
  - 55 MB hard disk
Make sure that port 4092 on the Patch Manager server is open and available for agent communications.

Deploy agents

You can deploy Patch Manager agents to online or offline computers, multiple computers using WSUS, and computers using the WMI Providers installer.

Deploy agents to online computers

Push the Patch Manager agent to the client computer from the Patch Manager Administrator 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.

1. Log in to the Patch Manager Admin Console as an administrator.
2. In the navigation pane, expand Enterprise and select Managed Computers.
3. In the center pane, select a computer that requires an agent.
4. In the Actions pane, click Deploy Client Components.
5. In the Task Options Wizard, select Install or Repair Client Components to prepare the client system to work with Patch Manager, and click Next.
6. Select the following options, and click Next:
   - Install WMI Providers: Installs the WMI providers on your managed computer
   - Install the Patch Manager Agent: Installs the agent on your managed computer to poll for WSUS updates

7. Select Install using Remote install Service, and click Next.
8. Select the clients you want to deploy the components, and click Next.
9. Review your selections, and click Finish.
Deploy agents to offline computers

Push the Patch Manager agent to the client computer from the Patch Manager Administrator Console. After the agent is installed on the client, provision the agent with a certificate so agent approval is not required.

💡 To minimize errors during your agent deployment, do not deploy an agent with the same host name on two or more computers.

1. Log in to the Patch Manager Admin Console as an administrator.
2. In the navigation pane, expand Enterprise > Managed Computers.
3. In the center pane, select a computer that requires an offline agent deployment.
4. In the Actions pane, click Provision Agent Offline.
5. In the Agent Provisioning wizard, ensure that the host information is correct, and click Next.
6. Click Browse and select the location where you want to place the provisioning installer.

7. Select the Recreate existing certificate checkbox if you do not want to use the existing certificate.

8. Enter the password used to protect the signed Patch Manager server certificate, and click Finish.
Distribute agents using WSUS

To distribute the agent to multiple computers at once, create a WSUS installer package and distribute the package through the WSUS server.

1. Log in to the Patch Manager Admin Console as an administrator.
2. In the navigation pane, expand Enterprise > Managed Computers.
3. In the center pane, select the targeted computer.
4. In the Actions pane, click Deploy Client Components.
5. In the Task Options Wizard, select Install or Repair Client Components, and click Next.
6. Select the following options, and then click Next:
   - Install WMI Providers: Installs the correct providers on your managed computer
   - Install the Patch Manager Agent: Installs the Patch Manager agent on your managed computer
7. Select Create a WSUS Installer Package, and click Next.
8. Select the clients you want to deploy the components, and click Next.
9. Review the information in the dialog box, and click Finish.
10. Publish the package.
Deploy agents using the WMI Providers installer

The SolarWinds Windows Management Instrumentation (WMI) Providers for managed clients provide additional management and inventory tools that are not native to WSUS. Without them, you can only use Patch Manager to interface with WSUS and not directly with the managed clients.

By default, Patch Manager does not deploy the WMI providers automatically unless you enable the Automatic all provision SolarWinds WMI Providers option under Management Groups > Settings. When enabled, Patch Manager deploys the WMI Providers to the managed computers as needed for specific configuration management tasks.

Install the SolarWinds WMI Providers on the managed computers

1. Ensure that WMI-in and WMI-out are enabled on the workstation. If these settings are disabled, you cannot access the machine.
   See your Windows documentation for instructions.
2. Log in to Patch Manager as an administrator.
3. In the navigation menu, locate and select the group that contains the targeted workstation.
4. To run the task on a specific computer, select the computer in the center pane and then click Check and Manage Computer Connectivity in the Actions pane.
5. In the Computer Access Management window, select Install the WMI Providers (if not installed) and select the appropriate options.
6. Select all options outside of the SolarWinds WMI Providers Actions group except Enable DCOM (if disabled).
7. Click OK to run the task.

Approve agents

You can view all approved, preapproved, and unapproved Patch Manager agents in the Patch Manager Administrator Console by expanding Enterprise > Agents in the navigation pane.

After you approve an agent, the agent can exchange data from the managed computer with the Patch Manager server. All agents must be approved before they can perform any actions on the remote client.
Enable or disable automatic agent approvals

1. Log in to the Patch Manager Administrator Console as an administrator.

2. In the navigation pane, expand the Patch Manager System Configuration > Management Groups and select a managed group.

   The default group is Managed Enterprise.

3. Click the Settings tab and select Enable automatic approval of agents.

4. In the Actions pane, click Edit.

5. Select Enabled or Disabled, and click OK.

Manually approve agents

If you disable automatic approvals, you can manually approve agents in the Patch Manager Admin Console.

1. Log in to the Patch Manager Administrator Console as an administrator.

2. In the navigation pane, expand Enterprise and select Agents.

3. In the Actions pane, click Approval Management.
4. In the Pending Agents Approvals dialog box, select the computer hosting the agent and click Approve Selected.

5. Click Done.

Configure agents

You can use policies and policy templates to configure the agents. You can also add configuration settings (such as polling intervals, auto-update settings, and timeouts) to a policy template and assign these settings to an agent or multiple agents using routing rules.

Create a policy

Perform the following steps to create a policy or policy template that configures client systems running a Patch Manager agent.

1. Log in to the Patch Manager Administrator Console as an administrator.

2. In the navigation pane, select Patch Manager System Configuration.

3. In the center pane, click Policy Editor.

4. In the Policy List dialog box, click Create Policy.

5. In the Edit Policy dialog box, enter a policy name.

6. Double-click a setting, enter or select a new value, and click OK.

7. Repeat step 5 to edit additional policy settings.

8. Click Scopes to modify the scope of the policy, and then click Save.

Apply a policy to specific scopes

Perform the following steps to select a scope category and define a new scope for client systems running a Patch Manager agent.
1. In the navigation pane, select Patch Manager System Configuration.

2. In the center pane, click Policy Assignment.

3. In the Scope List dialog box, create a scope or select a scope.

4. Select a Policy and click Save.
Integrate Patch Manager with the Orion Platform

The Patch Manager Administrator Console is the primary console used to manage Microsoft and third-party patching on your servers and desktop. If you are using the Orion Platform to manage your IT infrastructure, you can integrate Patch Manager with the Orion Web Console. This configuration allows you to monitor your patch deployment and other aspects of your IT environment in one location.

The Patch Manager Summary view does not display your Orion data.

To create the integration, run the Patch Manager Orion Web Console installer on your Orion server or a stand-alone server in your Orion Platform. After you configure the Patch Manager Web Console settings, you can log in to the Orion Web Console and access your Patch Manager data and Orion Platform data in one location.

You can download the Patch Manager Orion Web Console installer from the Customer Portal. See the Patch Manager Installation and Upgrade Guide for details.

When you run the Patch Manager Orion Web Console installer on the Orion server, the installation procedure installs an integration module and additional Orion services on the server. After the integration setup is complete, the Orion services create a direct connection to the Patch Manager database to retrieve data for the web reports. This data is cached to the Orion database.

To populate the Patch Manager Summary view, the Orion services connect to the Patch Manager Service running on the Patch Manager server. The Patch Manager Service connects to the Patch Manager database, retrieves the data for the Orion Web Console, and then passes this data to the Orion services. This data is cached to the Orion database.

When you open the Orion Web Console, the cached data is transferred from the Orion database to the Orion Web Console and displays in the console at My Dashboards > Patches > Patch Manager Summary.

All data is cached to the Orion database every five hours by default. You can adjust the caching interval in the Patch Manager settings.

See Patch Manager Orion Integration architecture for a visual representation of the Patch Manger and Orion Platform integration.
Patch Manager Orion integration architecture

The following illustration describes how the Orion server collects data from the Patch Manager server and database so it displays in the Orion Web Console.

You can use SQL Server Configuration Manager to enable the Named Pipes and TCP/IP protocols for the SQL Server network configuration. Web Reports require these protocols enabled on the SQL Server instance where the EminentWare database is located. For added security, configure a Windows firewall for this port. See the SQL Server Configuration Manager documentation on the Microsoft Docs website for instructions.
Access Patch Manager data in the Orion Web Console

The Orion Web Console includes the My Dashboards menu, which provides shortcuts to Patch Manager and Orion Web Console views. The default menu bars include Home and a menu bar for each installed Orion Platform product.

Patch Manager deployment

In a Patch Manager deployment, the Patch Manager Orion Web Console installer adds the Orion Web Console to the Patch Manager server, along with an integration module and supporting Orion services. The integration module adds the Patches option to the My Dashboards menu. When the installation is completed and you log in to the Orion Web Console, the My Downloads menu includes the Patches module with a link to the Patch Manager Summary page.

In a Patch Manager deployment, the Orion Web Console is also referred to as the Patch Manager Web Console.

Integrated Orion Platform deployment

In an integrated Orion Platform deployment, the Patch Manager Orion Web Console installer detects the current Orion Web Console on the Orion server and only installs the integration module and the supporting Orion services.

When the installation is completed and you log in to the Orion Web Console, the My Downloads drop-down menu includes the Patches module with your existing Orion Platform software modules.
Configure the Patch Manager Web Console settings

After you run the Patch Manager Orion Web Console installer on the Orion server, set up the Patch Manager Orion Web Console and configure your Patch Manager cache refresh settings. When you are finished, the Orion Services connect to the Patch Manager database through the Patch Manager Service running on the Patch Manager server. If you purchased a Patch Manager license, you can also check your product license.

After the Orion Services retrieves and caches the data to the Orion database, it displays in the Patch Manager Summary view in the Orion Web Console.

See the Orion Platform Administrator Guide for details about customizing the look, views, settings, charts, and maps for your Orion products.

Make sure that your user account includes login credentials to the SQL database server hosting the Patch Manager (EminentWare) database. You can use Microsoft SQL Server Management Studio to add your login credentials to the database.

Set up the Patch Manager Orion Web Console

Perform the following procedure to connect the Orion Web Console with the Patch Manager Orion Web Console.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings.
3. Under Product Specific Settings, click Patch Manager Settings.
4. In the Patch Manager Settings page, click Web Console Setup.
5. In the Web Console Setup page, enter your Patch Manager server credentials to link the web console to your Patch Manager server.

   a. Enter the IP address and port of the server hosting your Patch Manager software.

   ```
   Server name or IP address: [Input field]
   Port: [Input field]
   ```

   b. Enter the Windows Credentials of the server hosting your Patch Manager software.

   ```
   Windows Credentials for server entered above
   User name: [Input field]
   Password: [Input field]
   Confirm password: [Input field]
   ```

   c. Click Test to verify the connection.

   d. Click Submit.

**Configure the Patch Manager Cache refresh settings**

By default, the Orion server saves your Patch Manager cache to the Orion database every five hours. If you need to update the Patch Manager Summary page more or less frequently, you can adjust the Cache Validate Duration setting in the Patch Manager Settings.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings.
3. Under Product Specific Settings, click Patch Manager Settings.
4. In the Patch Manager Settings page under Global Settings, click Settings.
5. In the Settings page, enter a new value between 1 and 240 hours. The default value is five hours.

![Cache Validate Duration](image)

6. Click Submit.

**Check your SolarWinds product licenses**

Each SolarWinds product includes a license key that enables product use for a specific time period. For example, if you are evaluating Patch Manager, the evaluation license is valid for 30 days.

You can view the license status of each SolarWinds license using the License Details view in the console. The view lists the module name, version, service pack, and the number of days remaining for your product license.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings.
3. Under Product Specific Settings, click Patch Manager Settings.
4. In the Patch Manager Settings page under Global Settings, click License Summary.
5. Locate your product license details.
For example, the SolarWinds NPM license on the Orion server is an evaluation license that is valid for 89 days.

<table>
<thead>
<tr>
<th>NPM</th>
<th>License</th>
<th>89 day(s) left in evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product Name</strong></td>
<td>Network Performance Monitor</td>
<td></td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>2019.4</td>
<td></td>
</tr>
<tr>
<td><strong>Service Pack</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>Current number of interfaces</strong></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td><strong>Allowed number of interfaces</strong></td>
<td>500</td>
<td></td>
</tr>
</tbody>
</table>

**Patch Manager Summary view**

The Patch Manager Summary view displays the patch status of your managed systems in the Orion Web Console. After you locate an issue in your deployment, you can access the Patch Manager Administrator Console and troubleshoot the issue.

$i$ See the Orion Platform Administrator Guide for details about customizing the Orion Web Console look, views, settings, charts, and maps.

**About the widgets**

The Patch Manager Summary view includes widgets that notify you about vulnerabilities in your monitored servers and desktop systems. If the Patch Manager Summary view indicates an issue in your deployment, you can generate a Patch Manager report in PDF or Microsoft Excel format and send the report to your IT team to resolve the issue.

Widgets present important high-level information in an easy-to-read graphical format, such as graphs or drop-down menus. They provide information about specific aspects of your deployment, such as system health, available patches, and systems that require critical operating system updates.

Below is an example of the All Patches widget in the Patch Manager Summary view located at My Dashboards > Patches > Patch Manager Summary.
Identify the patch severity

Some widgets include icons that indicate the risks associated with known vulnerabilities identified by Microsoft and third-party software manufacturers. These icons warn you that the patch is required to prevent unauthorized access to your system.

You can review the details about each patch by maximizing the category (such as Adobe) and hovering over each patch. Click the patch link for specific details.
The following table describes the severity icons that display in the widgets.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Critical Icon]</td>
<td>Critical</td>
<td>May prevent malicious code from executing on a system without the user’s knowledge.</td>
</tr>
<tr>
<td>![Warning Icon]</td>
<td>Warning</td>
<td>May prevent user identity or data from being compromised by a third party.</td>
</tr>
<tr>
<td>![Moderate Icon]</td>
<td>Moderate</td>
<td>May prevent unauthorized access by a third party based on authentication requirements or system configuration.</td>
</tr>
<tr>
<td>![Unspecified or Low Icon]</td>
<td>Unspecified or Low</td>
<td>No severity or low severity to the managed system. You must evaluate whether the patch applies to your managed systems.</td>
</tr>
</tbody>
</table>

View additional resource information

Some widgets use popovers that display additional information about a patch or system. These popovers appear when you hover over a monitored object or patch in the Orion Web Console. They provide additional information and quick access to commands without taking up space or cluttering the page with too much information.

Below is an example of a popover that displays when you hover over a WSUS server link in the WSUS Servers widget.
Some widgets include links to additional information about a resource (such as a node or WSUS server) that provide additional information. Below is an example of a details window that displays when you click a WSUS server link in the WSUS Servers widget.

![WSUS Server Details](image)

**Explore the widgets**

This section describes the widgets that display in the Patch Manager Summary view.

**All Patches**

This widget displays all patches that were published to your WSUS server. Maximize each company title to access the patches. Hover over each patch for details about the patch.
Desktop Node Health Overview

This widget displays all desktop systems by patch status that are managed by your WSUS server.

<table>
<thead>
<tr>
<th>Node Count: 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>0</td>
</tr>
</tbody>
</table>

When you click a category such as Computers up to date, a legend page displays with additional details.

- **0 Computers up to date**
- **0 Computers needing updates**
- **4 Computers with unknown status**
  - node001
  - node002
  - node003
  - node004
- **0 Computers with update errors**

From here, you can maximize a category (such as Computers with unknown status) to view the nodes and corresponding WSUS server. You can hover over a node or server name to view general information, or click one of these links to view details about the system.

Last 10 Tasks

This widget displays the last ten tasks that were initiated in your deployment. These tasks correspond with the last 10 tasks in Task History located under Administration and Reporting in the Administrator Console.
### Latest 10 Tasks

<table>
<thead>
<tr>
<th>TASK</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️ Update Management for 1 computers created at</td>
<td></td>
</tr>
<tr>
<td>✔️ WSUS Inventory Task for</td>
<td></td>
</tr>
<tr>
<td>✔️ WSUS Inventory Task for</td>
<td></td>
</tr>
<tr>
<td>✔️ Update Management for 1 computers created at</td>
<td></td>
</tr>
</tbody>
</table>

### Latest 10 Patches on WSUS Servers

This widget displays the last ten patches by product that were published to your WSUS servers. The widget includes details about the severity, installation, and arrival date for each product title.

Maximize a product title to view the related patches. From here, you can hover over a patch to view the patch description, or click the patch link to view detailed information about the patch.

### Nodes Managed by WSUS Servers

This widget displays the WSUS servers in your deployment and the servers and workstations managed by each WSUS server.
You can maximize a category to view the nodes that are managed by the corresponding WSUS server, along with their **node status**.

Hover over a server to view information about the server, such as the polling IP address, Windows Server operating system version, and the percentage of used memory. Click the patch link to view detailed information, which includes the last synchronization date and the server make and model.

### Nodes Managed by WSUS Servers by Target Groups

This widget displays the WSUS servers in your deployment and the target groups (such as All Computers and Unassigned Computers) managed by each WSUS server.

You can maximize a target group (such as All Computers or Unassigned Computers) to view the nodes and their **node status** in that group. Nodes in a category that are not managed by a WSUS server display the 📀 icon next to the node name.
Hover over a server to view information about the server, such as the IP address, Windows Server operating system version, and the WSUS server IP address. Click the node link to view detailed information, which includes the node IP address and the node make and model.

Operating System Overview

This widget displays the number of servers and workstations managed by your WSUS servers based on their Windows operating system.

![Operating System Overview](image)

Node Count: 6
- 4 Windows 7
- 2 Windows Server (Version 10.0)

Click an operating system to view the legend details. From here, you can view the nodes, node status, and their corresponding WSUS servers.

![Operating System Overview Details](image)

Hover over a node or WSUS server link to view general information such as the polling IP address, server name, and used memory. Click a node or server to view details about the system, such as the processor type and the server make and model.

Recent 10 Patch Manager Posts

This widget displays the 10 most recent Patch Manager comments posted in the Product Forum on THWACK. Click a link to view the article on the THWACK website.
Server Node Health Overview

This widget displays all Windows-enabled servers by patch status that are managed by your WSUS server.

Click a category link to access the legend details. From here, you can maximize a category to view the nodes, node status, and corresponding WSUS Server.
Hover over a node or server name to view general information, such as the polling IP address, update details, and memory used in the system. Click a node or server to view addition details about the system, such as the last sync time, processor type, and the make and model of the system.

Top 10 Patches Missing

This widget displays the top 10 patches that need to be updated on your managed systems, including the number of systems that require the patches.

Hover over a patch name to view the description. Maximize the patch name to view the node associated with the patch.

Hover over the node or WSUS Server name to view general information about the node, such as the polling IP address, update details, and the percent of memory used on the system. Click the node or WSUS server name to view details about each node, such as the last sync time and result, processor type, and the system make and model.
Top 10 Most Vulnerable Machines

This widget displays the top 10 servers and workstations in your environment that are missing the most patches.

Each machine is listed with their current node status. The icon indicates that the machine is not managed by a WSUS server.

The Updates Missing column lists the number of updates missing from the machine. Red values indicate that some updates are critical operating system updates. Expand a machine name to view the required updates.

Hover over a machine name to view general information about the machine, such as the machine type (for example, Hyper-V Server or Windows Server), update details, and the percent of used memory on the system. Click a machine name for additional details, such as the last sync time, processor type, and the system make and model.

Hover over an update name to view a description. Click the update for details about the update provided by the software manufacturer.

WSUS Servers

This widget displays all WSUS servers in your deployment grouped by their Windows Server operating system.
Maximize an operating system vendor to view the WSUS server running the targeted operating system. The node name and node status display in the widget.

Hover over a server to view information about the server. This information includes the polling IP address, server health, and the percentage of used memory.

Click the WSUS server link to view detailed information about the server. This information includes the domain name, NetBIOS name, and Windows operating system version.

Customize the Patch Manager widgets

The Patch Manager Summary view consolidates data from the Patch Manager and WSUS servers and presents the information in configurable objects called widgets. If your user settings allow you to customize the widgets in the Patch Manager Summary view, you can change the layout and composition of the resources in the web console. See Define the user account settings for additional customization details.

Based on your user account settings, you can change the layout and composition of the Patch Manager Web Console views. These changes impact all users who share the views.

Update the user account settings

This procedure describes how to change a user's account settings so the user has permissions to customize the Patch Manager Summary view widgets.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings.
4. Select a user account and click Edit.
5. At the top, change Allow Administrator Rights to Yes. This allows the user to add and edit other accounts and reset passwords.
6. Under Alerts, change Allow Account to Customize Views to Yes. This allows the users to customize the Patch Manager view, as well as all views in the Orion Web Console.
7. Click Submit.
8. Click My Dashboards > Patches > Patch Summary.
9. Click the view you want to change.
10. Click Customize Page.
11. Make your changes, and then click Done.
12. Repeat step 2 through step 11 for each additional user who needs permissions to modify the Patch Manager Summary view widgets.

Change the custom widget layout

1. Click Edit next to the column definition.
2. Select the number of columns you want in the view.
3. Specify the width, in pixels, of each column.
4. Click Submit.

Delete a widget from a column

1. Select the widget.
2. Click [x] next to the column.

Add a widget to a column

Repeat the following steps for each widget you want to add.

1. Click [+] next to the column you want to modify.
2. Expand the appropriate widget category or categories.
3. Select the widget(s) you want to add.
4. Click Submit.

You can duplicate resources in the view.

Rearrange the widgets

Use the directional arrows next to each widget in the Column box.

Patch Manager Web Console user settings

The following table defines each user setting in the Patch Manager Web Console.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Enabled</td>
<td>Enables the user to log in to the Patch Manager Web Console. Select Yes or No.</td>
</tr>
<tr>
<td>Account Expires</td>
<td>Sets the date when the user cannot log in to the Patch Manager Web Console. Enter or select an expiration date or enter Never if the account should never expire.</td>
</tr>
<tr>
<td>Disable Session Timeout</td>
<td>Enables the user to stay logged in indefinitely to the Patch Manager Web Console. Select Yes or No.</td>
</tr>
<tr>
<td>Allow Administrator Rights</td>
<td>Enables the user with administrative rights to add or edit other user accounts and reset passwords. Select Yes or No.</td>
</tr>
<tr>
<td>Allow Node Management Rights</td>
<td>Enables the user to manage Orion nodes. This setting applies to an Orion Web Console running only the Patch Manager module. Select Yes or No.</td>
</tr>
<tr>
<td>Allow Account to Customize Views</td>
<td>Enables the user to customize the views they see when they log in to the Patch Manager Web Console. When a user customizes a view, the changes apply to all users who share the same views. Select Yes or No.</td>
</tr>
<tr>
<td>Allow Account to Clear Events, Acknowledge Alerts and Syslogs</td>
<td>Enables the user to clear and acknowledge Orion-generated events, alerts, and syslogs in the Orion Web Console. In consoles with only the Patch Manager module, this setting is negligible. Select Yes or No.</td>
</tr>
<tr>
<td>Allow Browser Integration</td>
<td>Enables the user to use client browser tools with information provided in the Orion Web Console. Select Yes or No.</td>
</tr>
<tr>
<td>Alert Sound</td>
<td>Enables audible alerts in the Orion Web Console. In web consoles with only the Patch Manager module, this setting is negligible.</td>
</tr>
<tr>
<td></td>
<td>If applicable, select a WAV file to use for alerts. The web console populates this list from the following directory: %SystemDrive%\Inetpub\SolarWinds\NetPerfMon\Sounds</td>
</tr>
<tr>
<td>Number of items in the breadcrumb list</td>
<td>Specifies the number of items the Orion 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.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Account Limitations</td>
<td>Specifies the network devices the user can view. For example, you can 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. See the Administrator Guide for your Orion Platform product for details.</td>
</tr>
<tr>
<td>Home Tab Menu Bar</td>
<td>Displays the menu bar the user sees on the Home tab. Select the menu bar from the list.</td>
</tr>
<tr>
<td>Patches Tab Menu Bar</td>
<td>Displays the menu bar the user sees on the Patches tab. Select the menu bar from the list.</td>
</tr>
<tr>
<td>Tabs ordering</td>
<td>Specifies the tab order in the Patch Manager Web Console. Use the up and down arrows to move tabs up or down in the list. The Patch Manager Web Console displays the tab at the top of the list.</td>
</tr>
<tr>
<td>Home Page View</td>
<td>Specifies the view the user sees when they log in to the Patch Manager Web Console. Select the home page from the list.</td>
</tr>
<tr>
<td>Default Network Device</td>
<td>Specifies the network device the user sees on the corresponding details page when they log in to the Patch Manager Web Console.</td>
</tr>
<tr>
<td></td>
<td>This setting only applies if the users 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.</td>
</tr>
<tr>
<td>Default Summary View</td>
<td>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.</td>
</tr>
<tr>
<td>Report Folder</td>
<td>Specifies the folder used by the Orion Web Console to pull reports for the selected user.</td>
</tr>
<tr>
<td></td>
<td>To assign a specific set of reports to a user, create a sub-folder in the Reports folder and place the specific reports in this folder. Select the user folder for this setting. The default location of the Reports folder is %PROGRAMFILES%\SolarWinds\Orion\Reports.</td>
</tr>
</tbody>
</table>

ADMINISTRATOR GUIDE: PATCH MANAGER
### Setting | Description
--- | ---
Orion General Settings | Selects the views the user can see after they click an element in the web console. Select a view from the list or select None to hide the user details.

The following settings are available:

- Node Details View
- Volume Details View
- Group Details View

Patch Manager Settings | Selects the views the user can see after they click an element in the web console. Select a view from the list or select None to hide the user details.

The following settings are available:

- Patch Manager Summary View
- WSUS Node Details View
- WSUS Server Details View
- Update Details View

---

**Generate Patch Manager reports in the Orion Web Console**

After you integrate Patch Manager with the Orion Platform, you can generate a Patch Manager report in the Orion server (Main Polling Engine) or the Orion Additional Web Server. After you install the web interface on the Orion server, you can log in to the Orion Web Console, click My Dashboards > Patches > Patch Summary to view the Patch Manager Summary view.

**Note:** This view is a read-only view and does not provide any client-related data to the WSUS server. As a result, you cannot generate an Orion report that provides Patch Manager data.

You can generate a Patch Manager report in the Patch Manager Administrator Console, schedule the report, and export the report in HTML format. When you are finished, you can access the report using a web browser.

See [Configure the inventory tasks and generate reports](#) for details about creating a custom report in Patch Manager.
Access the reports

1. Log in to the Orion Web Console.
2. Click Reports > All Reports.
3. In the left column, select the category that corresponds with the report you want to generate.

Below is a list of Patch Manager reports you can generate in the Orion Web Console.

Make sure that all user accounts include login credentials to the SQL database server hosting the Patch Manager database and the Orion Web Console is configured with the Windows credentials for each user. See Configure Access to the Patch Manager reports for details.

<table>
<thead>
<tr>
<th>Report</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Update Status (Approved Updates)</td>
<td>Inventory</td>
<td>Lists all patches installed on your machines. You can filter the results based on the patch and machine names.</td>
</tr>
<tr>
<td>Latest Patches Within Last 7 Days</td>
<td>Inventory</td>
<td>Lists all Microsoft and third-party patches published to the Windows Server Update Services (WSUS) or System Center Configuration Manager (SCCM) server for a specific date range. The default range is seven days.</td>
</tr>
<tr>
<td>Machines Pending Reboot</td>
<td>Inventory</td>
<td>Lists all machines that require a reboot after the machine is patched.</td>
</tr>
<tr>
<td>Missing Patches (All)</td>
<td>Custom</td>
<td>Lists all patches that are not installed on your machines.</td>
</tr>
<tr>
<td>Missing Patches (Approved)</td>
<td>Custom</td>
<td>Lists all approved patches that are not installed on your machines.</td>
</tr>
<tr>
<td>Missing Patches Pie Chart</td>
<td>Inventory</td>
<td>Displays all missing patches in a pie chart, including the number of nodes that require the patch.</td>
</tr>
<tr>
<td>Patching Tasks</td>
<td>Inventory</td>
<td>Displays the latest Patch Manager tasks and whether a task was successful or failed.</td>
</tr>
<tr>
<td>Software Installed</td>
<td>Inventory</td>
<td>Lists the software applications installed on all machines across your environment.</td>
</tr>
</tbody>
</table>
Configure access to the Patch Manager reports

To allow authorized users to create reports in the Orion Web Console, add the user login credentials to the SQL database server. When you are finished set up Patch Manager users in the Orion Web Console so each authorized user can generate a report in the console.

Add user login credentials to the SQL database server

When you configure your Patch Manager settings in the Orion Web Console, make sure that your user account includes login credentials to the SQL database server hosting the Patch Manager database. You can use Microsoft SQL Server Management Studio or SQL Server Configuration Manager to add your login credentials to the database.

To add your login credentials using SQL Server Configuration Manager:

1. Log into the SQL database server.
2. Open a Run window and execute:
   ```
   compmgmt.msc
   ```
3. Expand Services and Applications > SQL Server Configuration Manager.
4. Expand SQL Server Network Configuration and select Protocols for SOLARWINDS_ORION.
5. Enable the following protocols:
   - Named Pipes
   - TCP/IP
6. Save your changes.

Set up Patch Manager users in the Orion Web Console

To enable authorized users to generate reports in the Orion Web Console, enter the Windows credentials for each Patch Manager user in the console.

Before you enter the Windows credentials, make sure that each user account includes login credentials to the SQL database server hosting the Patch Manager database. You can use Microsoft SQL Server Management Studio to add the user logins to the database.

1. Make sure that Patch Manager is integrated with the Orion Platform.
2. Log in to the Orion Web Console as an administrator.
3. Click Settings > All Settings.
4. Under Product Specific Settings, click Patch Manager Settings.
5. Click Setup Web Console.
6. Enter the server name or IP address of the server hosting Patch Manager.

```
<table>
<thead>
<tr>
<th>Windows Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>for server entered above</td>
</tr>
<tr>
<td>User name:</td>
</tr>
<tr>
<td>Password:</td>
</tr>
<tr>
<td>Confirm password:</td>
</tr>
</tbody>
</table>
```

7. Enter a user name and password.

```
<table>
<thead>
<tr>
<th>Windows Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>for server entered above</td>
</tr>
<tr>
<td>User name:</td>
</tr>
<tr>
<td>Password:</td>
</tr>
<tr>
<td>Confirm password:</td>
</tr>
</tbody>
</table>
```

8. Click Test to check the credentials.

9. Click Submit.

10. Repeat step 5 through step 9 for each additional Patch Manager user authorized to generate and print reports.

### Generate a report

![Tip] Before you generate a report, select and download the latest updates. When you are finished, generate a systems inventory so Patch Manager has the latest information about your managed computers. See the Patch Manager Getting Started Guide for details.

SolarWinds provides predefined reports for Patch Manager and each Orion product. You can generate a report using one of the predefined reports listed at the beginning of this article or create a custom report that includes two or more predefined reports. Click Reports > All Reports to view a list of all predefined reports in the Orion Web Console.

The following sections provide examples of generating a predefined report:
Generate a report from a web-based report

After you integrate Patch Manager with the Orion Platform, the Orion Web Console will include several reports that describe the status of your patch deployment. You can access these reports from the All Reports page in the Orion Web Console.

1. Verify that your login credentials were added to the SQL database server.
2. Log in to the Orion Web Console.
3. Click Reports > All Reports.
4. In the left column, click the report you want to generate. See the table of reports listed earlier in this article.
   For example, in the Group By column, select Inventory and then click Patch Status.
5. (Optional) Click Edit Report, add additional content, and then click Next.
6. Select an output.
   You can export the report to Microsoft Excel or print the report.

Generate a report from multiple web-based reports

You can combine content from several reports by creating a custom report. This report allows you to pull content from other Patch Manager reports into a single, multi-column report. If your report includes content-sensitive information, you can assign limitations that restrict the report from unauthorized personnel.

1. Verify that your login credentials were added to the SQL database server.
2. Click Reports > All Reports > Manage Reports > Create New Report.
3. Select Patch Manager as the available resource.
4. Select a resource name (for example, Patching Tasks), and click Select and Continue.
5. At the top of the Layout Builder, click Fix to window width.
6. In the Header area, add header content that will display in the report.
   
   a. Enter a report title and subtitle.
      
      For example:
      
      ![Finance Department Patches]
      
      Summary of all patches applied to workstations in the Finance Department

   b. Keep, change or deselect the logo.

7. In the Content area, add resources and sections to the report.
   
   a. Click the Page Layout drop-down menu and select a layout for this report.
      
      For example, you can select a two-column layout.

   b. Click Add Content and add additional resource names for the Patch Manager resource. If you selected a multi-column layout, click Edit resource on each additional resource and update the name.

   c. Click Edit Resource to include a specific set of data. Not all resources can be filtered.

   d. Filter the resource, and click Submit.
Each resource includes different filter options.

e. If your page layout includes more than one column, click Add Content in each column to add additional resource names.

You can drag-and-drop resource objects between columns.

f. Click Add Section to add additional sections and resources to the report.

8. In the Footer area, select and edit the text you want to include in the footer, and then click Next.

Deselect the Footer checkbox to remove the footer from the report.

9. Review the report to ensure that it includes the data you need, and then click Next.

Click Back to modify the report.

Each report resource is self-contained. You can scroll through each resource page from within the report.
10. Add report properties, such as categories, custom properties, and limitations, and then click Next. These properties will help you locate the report at a later date.

11. To schedule the report, click Schedule this report to run regularly, create a new schedule or assign a schedule, and click Next. You can schedule a report to be generated, emailed, saved, or printed.

12. Review the Summary and then click Submit to save the report.

The report is saved to the Custom category.

Generate a report with a custom table

1. Verify that your login credentials were added to the SQL database server.

2. Click Reports > All Reports > Manage Reports > Create New Report.

3. Click Custom Table, and then click Select and Continue.

4. Click the selection method drop-down window and select Specific Objects (static selection).
5. Click the Show drop-down menu and select Patch Manager Tasks. Accept the default selection for Group By.

```
Available Patch Manager Tasks:
```

<table>
<thead>
<tr>
<th>SHOW:</th>
<th>GROUP BY:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patch Manager Tasks</td>
<td>[No Grouping]</td>
</tr>
</tbody>
</table>

6. Under Search For, select the objects you want to include in the report.

```
SEARCH FOR:
```

- [ ] Approve Updates
- [ ] Approve Updates
- [ ] Approve Updates
- [ ] Approve Updates
- [x] Change Computer Group Membership
- [ ] Change Computer Group Membership
- [x] Client Certificate Management

7. Enter a data source name or accept the default and click Add To Layout.

8. Click Add column to select the columns to include in the table.

```
Table layout: Edit column widths
```

9. Select the columns for another entity that has a relationship with the selected Orion object (Patch Manager Tasks).

For example, Completion Time and Display Name.
10. Click Add Column.

11. Select additional filters and options. You can also drag the columns to another location in the table layout.

ℹ️ Click Preview Layout to preview the report.

12. Click Submit.
13. Click Fit to window width to expand the report across your screen.

14. In the Header area, add header content that will display in the report.
   
a. Enter a report title and subtitle.
   
   For example:
   
   ![Task Completion Time](image)
   
   b. Keep, change or deselect the logo.

15. In the Content area, add resources and sections to the report.
   
a. Click the Page Layout drop-down menu and select a layout for this report.

   For this example, accept the default.

   b. Click Add Content and add additional resource names for the Patch Manager resource. If you selected a multi-column layout, click Edit resource on each additional resource and update the name.

   c. Click Edit Table to modify your filtering options (if needed).

   ![Custom Table](image)

   d. If your page layout includes more than one column, click Add Content in each column to
add additional resource names.

- You can drag-and-drop resource objects between columns.

16. In the Footer area, select and edit the text you want to include in the footer, and then click Next. Deselect the Footer checkbox to remove the footer from the report.

17. Click Next.

18. Review the report to ensure that it includes the data you need, and then click Next.

<table>
<thead>
<tr>
<th>Task Completion Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task completion time</td>
</tr>
<tr>
<td>Summary of Orion Objects: <strong>Datasource 1</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Custom Table for Datasource 1</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DISPLAY NAME</td>
<td>COMPLETION TIME</td>
<td></td>
</tr>
<tr>
<td>Change Computer Group Membership</td>
<td>4/30/2019 9:05:08 AM</td>
<td></td>
</tr>
</tbody>
</table>

19. Add report properties, such as categories, custom properties, and limitations, and then click Next. These properties will help you locate the report at a later date.

20. To schedule the report, click Schedule this report to run regularly, create a new schedule or assign a schedule, and click Next. You can schedule a report to be generated, emailed, saved, or printed.

21. Review the Summary and then click Submit to save the report.

The report is saved to the Custom category.

Generate and configure additional reports

See [Manage and view reports in the Orion Platform](#) in the [Orion Platform Administrator Guide](#) for details. This section describes how to create additional custom reports with charts and tables, restrict access to reports, and generate reports on a schedule.
Be sure to verify that your login credentials are added to the SQL database server before you create a table and chart report.

Install the Patch Manager Orion Web Console on a separate server

You can install the Patch Manager Orion Web Console on any server running a supported Microsoft® Windows Server® operating system. This server can be an Orion server or a stand-alone server. The web console must be able to connect to a Patch Manager Application server for the Web Console to function properly.

Use the following procedure to install the Patch Manager software components on the web server.

Do not install Patch Manager, WSUS, and the Patch Manager Administrator Console on the Orion server. This configuration will impact the performance of your Orion-based applications.

1. Back up your Web Help Desk database to a separate location.
2. Verify that the web server meets the Windows Server operating system requirements.
3. Install the Patch Manager Orion Web Console on the Windows server.
   See the Patch Manager Installation Guide for details.

After you install the Patch Manager Orion Web Console, you can generate Patch Manager reports in the Orion Web Console. See the Patch Manager Getting Started Guide for details about the reports.
Administrator functions and settings

This section describes how to maintain your Patch Manager environment.

These tasks are not available in the SCCM console.

Manage Patch Manager tasks

Patch Manager uses tasks to initiate procedures in your deployment. When you install updates on your managed computers, schedule updates, or generate an inventory, Patch Manager creates tasks to perform these procedures in your deployment.

Some actions and procedures use a wizard (such as the Task Options Wizard) to help you select the options required to complete a task. These options may include computers in your network; configuration information (such as IP addresses); and the date, time, and frequency when the task runs.

To ensure that your client systems receive timely updates, ensure that the scheduled tasks run on a specific day, week, or month. After a task is completed, Patch Manager stores a record of the task in Task History—one of two components used by SolarWinds to license Patch Manager.

After you review the scheduled tasks, verify that all Task History items only apply to computers you are actively managing in your deployment. This process ensures that you do not exceed the maximum node count for your license.

Manage the scheduled tasks

When you schedule a task to occur in the future or reoccur at a given time (such as daily, weekly, or monthly), Patch Manager stores these recurring tasks in the Scheduled Tasks node. This node allows you to view all scheduled tasks in your deployment. Use this node to run, view, or reschedule tasks to run at a future or recurring date and time.

When a scheduled or unscheduled task runs, it displays in the Active Tasks node.

To access the node, log in to Patch Manager as an administrator. In the navigation node, expand Administration and Reporting and select Scheduled Tasks.
All scheduled tasks display in the center pane.

The Schedule column lists when each task is scheduled to run. When you select a task, the Information tab displays in the bottom center console with details about the task. You can review the task description, its purpose, when it is scheduled to run, and the task outcomes.

**WSUS Inventory Task for**

**Description:** This is a scheduled task to collect WSUS inventory information for.

**Purpose:** Inventory

**State:** N/A

**Submitted By:**

**Created:** 11/13/2019 10:40:50 AM

**Started:** N/A

**Completed:** N/A

**ID:** 1bb1fbd3d-402c-4a93-b3ca-4048fa160beb

**Task ID:** N/A

**Schedule:** Daily at 12:00 AM and starts on 11/14/2019 and reoccurs with no end date.

**Export Options:** The results will not be exported.

**Email Options:** The results will not be emailed.
Run a task

1. In the center console, select a task.
2. In the Actions pane, click Run Task Now.
3. Click Yes to continue.

   The task runs. You can view the task status by clicking the Active Tasks node in the navigation menu.

Reschedule a task

1. In the center console, select a task.
2. In the Actions menu, click Properties.
3. In the Task Options Wizard, click Next.

   Depending on the task, you can select and add additional resources (if desired).
4. Adjust your scheduling and notification options as needed, and then click Next.

   See Scheduling and Notification Options Page for details.
5. Review your changes, and click Finish.

Disable a task

1. In the center console, select a task.
2. In the Actions menu, select Enable/Disable task.
3. Click Yes to disable the task.

Manage the Task History

SolarWinds licenses Patch Manager based on the number of computers managed in a deployment. The Primary Application Server (PAS) calculates the number of managed computers using two sources located in the Patch Manage Administrator Console navigation menu:

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

Use the Task History node to review your current tasks and ensure that all Task History items only apply to computers you are actively managing in your deployment. When you are finished, choose whether to archive or delete the Task History items.
Delete the Task History items

Review your Task History items and delete computers you no longer manage with Patch Manager. For example, if you have an Inventory task that includes a computer that is no longer enabled, delete the task to remove that computer from the pool of Patch Manager nodes.

1. Log in to the Patch Manager Administrator Console.
2. In the navigation pane, expand Administration and Reporting and select Task History.
3. In the center pane, select the Task History item you want to delete.
4. In the Actions pane, click Delete Task.
5. Click Yes to confirm your selection.

Configure the Task History retention settings

By default, Patch Manager deletes Task History items after 60 days. You can customize the Application Servers node to retain items for a longer or shorter period of time. You can also define whether you want to archive—rather than delete—Task History items.

1. Log in to the Patch Manager Administrator Console as an administrator.
2. In the navigation pane, expand Patch Manager System Configuration > Patch Manager Servers and select Application Servers.
3. In the center pane, select the application server.
4. Click the Application Server Settings tab.

5. In the Category column, click ☑ and select General.


7. Verify the setting, and click OK.


9. Verify the setting, and click OK.

When Patch Manager archives Task History items, it stores them in the %PROGRAMFILES%\SolarWinds\Patch Manager\Server\archives directory.

Clear outdated files from the Patch Manager server

During normal operations, Patch Manager stores files on your Patch Manager server to complete various functions and tasks. These files include cache files, tasks, and downloaded packages. Patch Manager also stores custom layout files on your Patch Manager server when you sort column data in a data grid and click Save View Layout in the Actions pane.

Over time, these files can consume excessive drive space on your Patch Manager server. Additionally, new resources (such as managed computers) may not display in the console because they are filtered out by the custom layout. To delete unused files and custom view layouts, use the Cache, Layouts and Tasks Maintenance screen to clear these items from your Patch Manager server.
All cache, layout, task, and package files are stored on the Patch Manager server in specific directories based on your operating system. The following table lists the directory paths for the stored files.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Default Paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP Professional</td>
<td>%PROGRAMFILES%%SolarWinds\Patch Manager\Server\Data</td>
</tr>
<tr>
<td>SP3 or later</td>
<td>%USERPROFILE%\Local Settings\Application</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>Data\EminentWare</td>
</tr>
<tr>
<td>Windows 8 and later</td>
<td>%PROGRAMFILES%%SolarWinds\Patch Manager\Server\Data</td>
</tr>
<tr>
<td></td>
<td>%USERPROFILE%\AppData\Local\EminentWare</td>
</tr>
</tbody>
</table>

Run the following procedure on your Patch Manager server to clear the cache, layout, task, and package files.

1. Log in to the Patch Manager Admin Console as an administrator.
2. In the navigation pane, select Administration and Reporting.
3. In the center pane, click General Settings.
4. In the center pane, click Clear Caches and View Layouts.
5. In the Cache, Layouts and Tasks Maintenance window, click or select one or more options based on your needs.
### Cache, Layouts and Tasks Maintenance

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear Caches</td>
<td>Clears all cache files. These files are stored in the <code>\Server\Data</code> directory on the Patch Manager server.</td>
</tr>
<tr>
<td>Delete Old Tasks</td>
<td>Deletes console-related worker files for old tasks. These files are stored in the <code>\EminentWare\Tasks</code> directory on the Patch Manager server.</td>
</tr>
<tr>
<td>Clear View Layouts</td>
<td>Reverts all custom view layouts in the Patch Manager console to their default configurations. These files are stored in the <code>\EminentWare\gridlayout</code> directory.</td>
</tr>
<tr>
<td>Clear Packages</td>
<td>Deletes console-related worker files for old packages. These files are stored in the <code>\EminentWare\Packages</code> directory on the Patch Manager server.</td>
</tr>
<tr>
<td>Clear All</td>
<td>Clears caches, old tasks, layouts, and packages from the Patch Manager server.</td>
</tr>
<tr>
<td>Delete tasks older than</td>
<td>Automatically deletes the console work files for old tasks based on your chosen value.</td>
</tr>
</tbody>
</table>

6. Click OK.
View the server settings and details

Use the Patch Manager Servers node to view Patch Manager server settings and details. The resources in this node can help you configure, monitor, and troubleshoot the Patch Manager servers in your environment.

The Patch Manager Servers node contains a child node for two of the three Patch Manager server roles that also display as nodes in the navigation window:

- Application Servers
- Management Servers

The parent Patch Manager Servers node contains details about the Automation Server role on every Patch Manager server. This server includes the Patch Manager server file system.

Patch Manager Servers node

The Patch Manager Servers node contains the Application Servers and Management Servers nodes, which add additional functionality to your deployment.

You can access the Patch Manager Servers node from the navigation menu.

1. Log in to Patch Manager as an administrator.

2. Expand Patch Manager System Configuration > Patch Manager Servers.

3. In the Patch Manager Servers pane, select the WSUS server.
In this example, WSUS01 is the WSUS server.

The tabs display in the lower Patch Manager Servers pane.

When you select a node in the drop-down menu, the console displays the following tabs with information about that server in the lower-center pane.

**Summary**

This tab provides details about the server, including the name, Patch Manager server roles, and management group.

**Server Files Details**

This tab 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.
See Patch Manager Server File System for additional information about Patch Manager server files.

### Tasks Diagnostics

This tab displays details about the tasks currently running on the Automation role server. These details also appear on the Task Diagnostics tab for the Management Servers node, which can contain details for several Automation role servers.

### Worker Process Jobs

This tab displays details about the tasks currently running on the Automation Server node. These details also appear on the Task Diagnostics tab of the Management Servers node, which can contain details for several Automation role servers.

### Automation Server Settings

This tab displays the Patch Manager server settings that are specific to the Automation Server role. See Automation Server Settings for additional information about these settings.

The Logging settings on this tab override the corresponding settings on both the Application Servers and Management Servers nodes.
Application Servers node

The Application Server node interfaces with the Patch Manager Administrator Console or integrated SCCM administration consoles. This node manages all communications between the console and the Patch Manager deployment.

When you select Applications Server node in the drop-down menu, the console displays the following tabs with information about that server in the lower-center pane.

You can access the Patch Manager Servers node from the navigation menu.

1. Log in to Patch Manager as an administrator.
2. Expand Patch Manager System Configuration > Patch Manager Servers.
3. In the Patch Manager Servers pane, select the WSUS server.

In this example, WSUS01 is the WSUS server.

The tabs display in the lower Patch Manager Servers pane.

Summary

This tab displays details about the server, such as the server name, Patch Manager server roles, and management group.
Sessions

This tab displays a list of active console connections to the selected Patch Manager server.

Task Diagnostics

This tab displays details about the tasks currently running on the Automation Server role. 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

This tab lists the Patch Manager servers with the Management or Application Server roles. This tab displays detailed information about the status of each server. In this example, WSUS01 is the management server.
Application Server Settings

This tab displays the Patch Manager server settings that are specific to the Application Server role.

See Application Server Settings for more information about these settings.

Management Servers node

The Management Servers node maintains all inventory and discovery data for specific systems in the Patch Manager environment. Each Management Server includes a defined collection of managed entities specified by their corresponding domain, workgroup, or WSUS server.

You can access the Patch Manager Servers node from the navigation menu.

When you select a Patch Manager server in the Management Servers node, the console displays the following tabs with information about the server in the lower-center pane.

1. Log in to Patch Manager as an administrator.

2. Expand Patch Manager System Configuration > Patch Manager Servers and select Management Servers.

3. In the Patch Manager Servers pane, select the WSUS server.
In this example, WSUS01 is the WSUS server.

Summary

This tab displays details about the server, such as its name, Patch Manager server roles, and management group.

Automation Server Monitoring

This tab lists all of the Automation Servers assigned to the selected Management Server.

Task Diagnostics

This tab displays details about the tasks currently running on the Automation 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

This tab displays the Patch Manager server settings that are specific to the Management Server. See Management Server Settings for additional information about these settings.
**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

> 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. The Server root folder root contains the log files. These files are in addition to the EminentWare event log Patch Manager maintains on the host operating system.

<table>
<thead>
<tr>
<th>Subfolder</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archives</td>
<td>Contains XML files for Task History items that Patch Manager has automatically purged from the Patch Manager server.</td>
</tr>
<tr>
<td>certs</td>
<td>Contains a CER file for each certificate created by the PAS.</td>
</tr>
<tr>
<td>data</td>
<td>Contains operational data for the Patch Manager server, including task definitions.</td>
</tr>
<tr>
<td>database</td>
<td>Contains the SQL script files used to initialize the Patch Manager database. If Patch Manager was installed with a local instance of SQL Server Express, this folder also contains the SQL Server master database files (MDFs) and log database files (LDFs) files that comprise the database.</td>
</tr>
<tr>
<td>exports</td>
<td>The default storage location for all task results and scheduled report exports.</td>
</tr>
<tr>
<td>packages</td>
<td>Contains the WMI redistributable, the WMI provider installer, and all content related to locally published packages.</td>
</tr>
<tr>
<td>Subfolder</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>scheduled</td>
<td>Contains a repository of work files Patch Manager uses to execute scheduled tasks.</td>
</tr>
<tr>
<td>templates</td>
<td>Contains all configuration templates used by the server-resident console sessions. On remote consoles, the templates are stored in %AppData%\Local\SolarWinds\Templates.</td>
</tr>
</tbody>
</table>
Wake on LAN

Wake on LAN (WoL) is an industry standard protocol used to remotely power on Wake on LAN-enabled computers from a low-power mode using a UDP broadcast on the local subnet. Patch Manager uses Wake on LAN to ensure a targeted system is running before performing a scheduled task.

Ensure that all targeted computers meet all Wake on LAN requirements. When you are finished, set up Wake on LAN in the Patch Manager Administrator Console to discover all computers in a subnet that require Wake on LAN for patch management.

After you schedule the Wake on LAN, Update Management, and Shutdown or Reboot Computers tasks, you can power on remote computers, apply your updates, and shut down the targeted computers when the updates are completed.

Wake on LAN requirements

To implement Wake on LAN in your Patch Manager deployment, ensure that:

- All target systems include a network interface card (NIC) that supports Wake on LAN.
- All target systems have Wake on LAN enabled in the BIOS.
- Patch Manager can connect to the target systems using a UDP broadcast.

By default, many network devices do not forward UDP broadcasts. For best practice, initiate Wake on LAN from the local subnet containing the target system by configuring additional Patch Manager servers with the Automation Server role to any subnets that contain Wake on LAN targets.

- Wake on LAN is set up in the Patch Manager Administrator Console to collect the MAC address of all targeted systems on one or more subnets.
- Wake on LAN is scheduled in the Patch Manager Administrator Console.

Set up Wake on LAN

After you confirm all targeted systems meet the Wake on LAN requirements, set up a task in the Patch Manager Administrator Console to discover all computers in a subnet that require Wake on LAN for patch management. When the task is completed, Patch Manager stores the MAC addresses of all NICs attached to computers that require Wake on LAN.
When the discovery is completed, schedule a Wake on LAN task to power on the targeted computers before the WSUS server publishes your Microsoft® and third-party updates.

Discover all Wake on LAN computers in a subnet

Configure and schedule a subnet discovery to collect the MAC addresses for all computers that require Wake on LAN to install your software updates. When you are finished, the Patch Manager Administrator Console will not generate notifications prompting you to configure your subnets for Wake on LAN prior to publishing your software updates.

1. Log in to the Patch Manager Admin Console as an administrator.

2. In the navigation menu, expand Patch Manager System Configuration > Management Groups and select Managed Enterprise.

3. Select the Discovery Subnets tab.

4. If a subnet displays in the tab window, go to step 5.

   If a subnet does not display in the tab window, perform the following steps:

   a. In the Actions pane, click Add Subnet.

   b. In the Add TCP/IP Subnets window, enter an IP address, subnet mask, starting address, and ending IP address.
c. Click Add Subnet and select a subnet that contains the targeted computers.

d. Click OK.

5. In the Managed Enterprise pane, select a subnet.

6. In the Actions pane, click Discovery Configuration.

7. In the Discovery Port Configuration window, select the ports used to discover the targeted computers, and click Save.
8. In the Actions pane, click Schedule Discovery.

9. Complete the schedule options to schedule the discovery task, and click OK.

Schedule Wake on LAN

After you discover all computers that require Wake on LAN for patch management, schedule Wake on LAN to power on the targeted computers before the WSUS server publishes the Microsoft and third-party updates to all managed computers.

Wake on LAN requires at least one successful network discovery to retrieve the MAC address from all targeted computers. Ensure that Patch Manager discovered all Wake on LAN computers before you schedule this task.

1. Log in to the Patch Manager Admin Console as an administrator.

2. In the navigation pane, select Administration and Reporting.
3. In the center pane, click Administrative Tasks.

4. In the Administrative Tasks pane, click Wake on Lan.

5. Complete the Wake on Lan Options window.

   a. Enter the broadcast IP address for the subnet that contains the target systems.
      If you want to send the broadcast to all subnets, enter 255.255.255.255.

   b. If you configured a non-standard port for Wake on LAN, enter the port number in the UDP Port field.

   c. If you configured a Secure On password for the targeted systems, enter the password in the Secure On Password field.

   d. Click OK.

6. In the Task Options Wizard, select one or more computers to include in the task, and click Next.

7. Complete the scheduling and notification options, and click Next.

8. In the Summary page, click Finish to schedule or execute the task according to your specifications.
Advanced deployment examples

This section provides several scenarios for deploying additional Patch Manager servers to balance server load and connect to remote systems across a distributed network.

Server roles

Patch Manager consists of three server roles: Primary Application Server (PAS), Management Server, and Automation Server. By default, all Patch Manager servers include the Automation Server role. When you deploy additional Patch Manager servers, you can deploy just an Automation Server role, or add one or both of the remaining roles. All Patch Manager servers require separate SQL Server instances.

The server that hosts the Patch Manager installation is called the Primary Application Server. This server contains all three server roles.

SolarWinds licenses Patch Manager by the number of managed computers. As a result, there are no additional license costs associated with deploying additional Patch Manager servers.

Primary Application Server

The Primary Application Server provides a separate console connection point for load balancing, separate business units, and users located at separate locations. The server interfaces with the MMC-based Patch Manager Administrator Console, SolarWinds Orion® Web Console, and the SCCM integrated console.

Servers in this role manage all communication between the console and the Patch Manager environment. Configure Application role servers to work with one or more servers in the Management role to specify which systems can be managed by what Patch Manager consoles.

Management Server

The Management Server manages Microsoft Server Manager servers in secondary management groups. The 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 Server roles to partition managed systems into defined security or network management boundaries.
Automation Server

The Automation Server provides a workers service so the Primary Application Server can delegate the Automation Server to create connections to specific hosts. The server also bridges the gap between disparate WSUS API versions included with different Windows Server versions.

The 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 or access-controlled networks, such as a perimeter (DMZ) network.

Design Considerations

When you design your Patch Manager deployment strategy for a distributed environment, decide where to place the Patch Manager servers and consoles in your deployment. When you are finished, you can configure the Patch Manager databases.

Distribute the Patch Manager servers

You can distribute multiple Patch Manager servers in your environment for load balancing and fault tolerance, and to resolve issues caused by geographic distribution or securities boundaries within your organization. When you deploy multiple Patch Manager servers, consider the following requirements:

- Geographically-distributed environments
- Large environments
- Wake-on-LAN
- Port considerations and bandwidth restrictions

Geographically-distributed environments

In geographically-distributed environments, deploy an additional Automation Server role to each remote site. This server role allows you to facilitate client management and configuration processes on the local LAN of the target systems rather than across the WAN.

You can also deploy additional Management Server roles to each site to segregate management and data collection tasks. Management Server roles work in conjunction with the additional Application Server role to support remote system administrators.
Large environments

In large environments with multiple subnets or large inventory requirements, deploy additional Application Server or Management Server roles to optimize your Patch Manager environment. You can use additional Application Server roles to support multiple administration consoles and additional Management Server roles to create smaller management groups for administration and reporting.

Wake-on-LAN

In environments that implement Wake-on-LAN (WoL), deploy additional Automation Server roles to facilitate WoL broadcasts for distributed systems. This deployment minimizes the administrative time in configuring 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 issues, you can deploy additional Automation Server or Management Server roles to minimize these issues. You can add additional Application role servers to limit WAN communication to port 4092—the port used for server-to-server communication. With an Automation Server role on each LAN, the remaining ports required in the Patch Manager environment must only be open on each LAN.

Additionally, use additional Management Server roles to limit the amount of traffic traveling across the WAN. With a Management Server role on each LAN, inventory data will cross the WAN only if a Patch Manager administrator runs a report for that LAN from a remote site.

Install multiple Patch Manager administrator consoles

You can install multiple Patch Manager administrator consoles to connect to a single Primary Application Server (PAS) from multiple locations, or to connect to a Secondary Application Servers (SAS) as needed.

Multiple consoles with a single PAS

In environments that require one Application Server role, deploy additional Patch Manager administrator consoles to allow console connections from more than one computer. See Configuring Remote Administration Consoles for details.

Multiple consoles with dedicated servers

In environments that require multiple Application Server roles, the Patch Manager installer adds a Patch Manager administration console on each additional server. If you need to connect to these servers from separate computers, deploy additional Patch Manager administrator consoles and connect them to the appropriate Application Server role as required.

See Install the administrator console on a remote system for details.
Configure the Patch Manager databases

The Patch Manager database stores all consolidated data from a WSUS inventory, Managed Computer inventory, and Discovery tasks. To generate a WSUS inventory report for this data, the Patch Manager Administrator Console pulls the data directly from the database.

When you install your Patch Manager servers, you have several Microsoft® SQL Server® database configuration options. You can install:

- SQL Server Express on the Patch Manager server
- SQL Server on the Patch Manager server
- SQL Server on a remote server

To ensure optimal performance, SolarWinds recommends the following:

- Use SQL Server 2008 R2 Express Edition (included with the Patch Manager installer) for Patch Manager servers that require less than 10 GB of storage space.

> If you exceed 10 GB, you must migrate your database to an SQL Server instance.

- 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 configurations require high reporting services.
- Use a remote database server for Patch Manager server roles hosted on a WSUS or SCCM server.
- Deploy additional Management Server roles to split storage requirements between each additional server.

Set up an Automation Server

When you install Patch Manager in large or distributed networks, your network environment may require additional Automation Servers to manage your deployment. To address this issue, Patch Manager uses Automation Servers to initiate RPC/WMI connections to remote systems.

When you deploy an Automation Server, Patch Manager can simultaneously target more systems. Additionally, deploying an Automation Server closer to the remote systems they manage allows the RPC/WMI connection to travel a shorter distance.

> If an Automation Server is not set up correctly, you can re-provision the server. See Re-provision an Automation Server for details.

You can use Automation Server roles to manage a dedicated target or manage geographically distributed networks.
You can define specific worker process settings to limit the capacity of each Automation Server. See Automation Server Settings for details.

To set up an Automation Server:

1. Download and run the Patch Manager Installer.
2. Configure the Automation Server routing rules.
3. (Optional) Configure the subnet routing rules.

Run the Patch Manager Installer

1. Log in to the Customer Portal.
2. Download the Patch Manager software.
   a. Click Downloads > Download Product.
   b. Click the Products drop-down menu and select Patch Manager.
   c. Click the Licenses drop-down menu and select your license tier.
   d. Download the Patch Manager FULL with SQL installer.
   e. Log out of the Customer Portal.
3. Launch the installer on your WSUS server.
   During the installation, the installer extracts the .NET Framework files.
4. Select the following, and then click Next:
   - Install the Patch Manager Server Components
   - Install the Patch Manager Administrations Console
5. If you accept the License Agreement, click Next.
6. Select the Destination location and Click Next.
7. (Important) In the Orion Install selection, select Advanced Install.
   
   ![Advanced Install]
   
   Install Patch Manager for use with an existing SQL Server database.
   
   Note: Advanced Install requires an existing SQL Server database for use with Patch Manager. If you do not already have a SQL Server database to use with Patch Manager, select Express Install.

8. Select Start Copying Files, and click Next.
The Wizard installs the Administrator Console and closes automatically.

9. When prompted, click Next to launch the SolarWinds Patch Manager Configuration Wizard.

10. Select Automation Server, and click Next.

11. Enter the name of the Primary Patch Manager server and test the connection.

   If the test passes, click Next.

   If the test does not pass, troubleshoot the issue, and then click Next to test the connection.

12. Configure the Windows Firewall for the server, and click Next.

13. When prompted, enter the WSUS server information, and click Next.

14. Enter a local administrator account that is in the WSUS Administrators group, and click Next.

15. Select Install SQL Server Express, and click Next.

16. Select the Default service account and click Next.

17. Complete the Patch Manager Configuration Wizard and click Next.

**Configure the Automation Server routing rules**

Patch Manager uses Automation Server routing rules to manage tasks sent to each Automation Server. They define whether or not to assign a task to a default round-robin pool if an assigned server is unavailable.

1. Log in to the WSUS server as an administrator.

2. Launch the Patch Manager Administration Console.

3. In the navigation pane, expand Patch Manager System Configuration and select Patch Manager Servers.

4. In the center pane, select the Automation Server.

5. In the Actions pane, click Patch Manager Server Wizard.
6. In the Patch Manager Server Configuration Wizard, select Edit an Existing Patch Manager Server configuration settings, and click Next.

7. Click the Server Name drop-down menu, select the Automation Server, and click Next.

   If the remaining fields do not populate automatically, click Resolve.
8. Associate your Patch Manager Server with a Patch Manager Management Group.

![Patch Manager Server Configuration](image)

- Click the Management Group drop-down menu and select Managed Enterprise.
- Click Server Role and select Automation.
- Review the remaining options, then click Next.

9. Complete the Wizard.

10. In the navigation pane, expand Patch Manager System Configuration > Management Groups and select Managed Enterprise.

12. In the Actions pane under Routing Rules, select Add WSUS Server Rule.

13. Click the Server Name drop-down menu, select the WSUS server, and click Save.

   - If the remaining fields do not populate automatically, click Resolve.
14. Click Test Connection.
   If the connection passes, a dialog box displays. Click OK.

   ![Success dialog box](image)

   If the connection does not pass, check the configuration settings in the window.

15. Select the Automation Server and Absolute Rule checkboxes and click OK.

16. Restart the EminentWare Data Grid Server Service on the Patch Manager Server and the Automation Server.
   If you do not have WSUS servers located at different sites or domains, you are finished.
If you have WSUS servers located at different sites or domains, configure the subnet routing rules.

(Optional) Configure the Subnet Routing Rules

In the navigation pane, expand Patch Manager System Configuration > Management Groups and select Managed Enterprise.

1. In the navigation pane, expand Patch Manager System Configuration > Management Groups and select Managed Enterprise.

2. Click the Automation Server Routing Rules tab.

3. In the Actions pane under Routing Rules, click Add Subnet Rule.

4. In the dialog box, enter the subnet, click Add Subnet, and then click OK.
5. Select the Automation Server to use for the subnet, and then click Absolute Rule.

6. Click OK.

7. Repeat step 3 through step 6 for each additional subnet you want to add to the Automation Server.

**Set up an Automation Server role to manage a dedicated target**

You can add a second Automation Server role to manage tasks on the Patch Manager Primary Application Server (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 scenario, add an additional Automation Server role to handle tasks Patch Manager executes against itself.
In other examples, SolarWinds recommends deploying additional Automation Server roles on dedicated systems. However, since the additional server in this scenario is only responsible for a single system, you can deploy this server in tandem with a related system, such as a desktop system running the Patch Manager Administrator Console or a WSUS server.

Create an Automation Server routing rule

To deploy this configuration, create an Automation Server routing rule that instructs Patch Manager to direct all tasks against the PAS to the additional Automation Server role as long as it is online. If the additional server is offline, Patch Manager should direct the task to the PAS.

1. Log in to the Patch Manager Administrator Console as an administrator.
2. In the navigation pane, expand Patch Manager System Configuration > Management Groups.
3. Select the management group for which you want to configure the rule.
4. In the center pane, click the Automation Server Routing Rules tab.
5. In the Actions pane, click Add Computer Rule.
6. In the Add Computer dialog box, enter the details for the PAS.
7. Click Add.
8. Complete the Select Automation Server(s) for routing rule and rule type dialog box.
   a. Select the additional Automation Server role.
   b. Clear the Absolute Rule check box.
   c. Click OK.

Set up additional Automation Server role to manage geographically-distributed networks

If your managed computers are spread out across a geographically-distributed network, install an Automation Server on a duplicate WSUS server or a dedicated desktop system in each remote location.
Additionally, you can install a separate Automation Server to offload task management 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. In this configuration, the Automation Server on the PAS provides a backup for the secondary Automation Server.

Create an Automation Server routing rule for this example

Use the Absolute Rule option to instruct Patch Manager to abandon a task if none of the Automation Servers you explicitly define for a location are online.

1. Log in to the Patch Manager Administrator Console as an administrator.
2. In the navigation pane, expand Patch Manager System Configuration > Management Groups.
3. Select the targeted management group for the configuration rule.
4. In the center pane, click the Automation Server Routing Rules tab.
5. In the Actions pane, click Add Subnet Rule.
6. Complete the Add TCP/IP Subnets dialog box.
   a. In the IP Address field, enter the subnet IP address.
   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.

7. Click OK.

8. Complete the Select Automation Server(s) for routing rule and rule type dialog box.
   a. Select the additional Automation role servers.
   b. Select Absolute Rule.
   c. Click OK.

Set up additional Application and Management Servers

An Application Server allow you to provide redundancy or additional load capacity for console connections, or to create isolated sandboxes in which a console user manages an environment. They have their own credentials, user profiles, and security roles. For example, you can add an additional Application Server to manage separate Patch Manager Administrator Console connections.

Management Servers allow you to create additional management groups. Because each Patch Manager server uses its own Microsoft SQL Server instance, you can create multiple management groups that segregate Patch Manager data into multiple data stores. For example, you can manage isolated segments that store sensitive and confidential data or create reports at a granular level, such as by department or site.

You can use Application Server or Management Server roles (or a combination of both roles) to:

- Manage console connections
- Segregate patch and asset data
- Manage a test lab

Use an Application Server role to manage console connections

You can add multiple Application Server roles to manage a large number of console connections. This configuration provides High Availability for your deployment.
To create this configuration, deploy at least three Application server roles:

- Primary Application Server (PAS) where you installed Patch Manager. Patch Manager does not use the PAS for console connections.
- At least two Secondary Application Servers (SAS) to segregate groups of console users and provide a redundancy in case of failure.

This HA configuration scales to as many Application Server roles as you require. If necessary, each console user could have a dedicated Application Server role for their console connection.
Set up a Management Server role to segregate patch and asset data

You can add Management Server roles to improve performance or limit space requirements to avoid purchasing an additional SQL Server instance. The Management Server roles allow you to segregate patch data collected from the WSUS server from the asset inventory data collected from managed computer inventory tasks.

This scenario can help you manage your patch data if you installed Microsoft SQL Server Express as your primary Patch Manager database. Because this SQL version has a 10 GB size limit, it is not enough space to store both patch and asset data. To stay within the 10 GB restriction, you can deploy an additional Management Server role to store the asset data from a domain inventory. This scenario reserves the PAS for patch data from the WSUS server.

If you exceed the 10 GB limit, you must migrate your Patch Manager database to an SQL Server instance.
Since Patch Manager physically segregates the data, each database is significantly smaller. This scenario also improves performance and enhances security by keeping unique data sets separate from each other.

**Set up Application Server and Management Server roles in a test lab**

You can deploy an additional Patch Manager server with Application Server and Management Server roles to test your software packages before you deploy them to your environment. This scenario allows you to isolate the testing environment from the production environment.
This scenario shows a separate management group for the test environment resources. These resources should include the subdomain or workgroup for the environment and a dedicated WSUS server. A similar example would be to use an additional server for a special business or perimeter network (DMZ).

**Configure a downstream WSUS server**

Perform the following steps to add a downstream WSUS server to your Patch Manager deployment.

1. Log in to SolarWinds Patch Manager as an administrator.
2. In the navigation pane, expand Enterprise > Update Services and select the WSUS server.
3. In the Action menu, click Register Downstream Servers.
4. In the WSUS Server Downstream Server Auto-Registration window, select the downstream server, and click Register.
5. If required, update the credential ring to access the WSUS server.
   
   No other configuration is required if the domain account set for the server can access the new domain account.
6. Troubleshoot downstream WSUS server issues in Patch Manager as required.

**Add a managed domain or workgroup**

You can add a managed domain or workgroup to your deployment using the Patch Manager Administrator Console. When you are finished, add the credentials to access the resource.

1. Log in to the SolarWinds Patch Manager Admin Console as an administrator.
2. In the Patch Manager menu, expand Patch Manager System Configuration and select Managed Enterprise.

   ![Patch Manager (wsus01)](image)
   
   3. Click Management Group Wizard in the Actions pane.
5. Select Active Directory Domains or Workgroups, and then click Next.

6. Enter a flat name in the Name field.

7. Enter the fully qualified domain name (FQDN) in the DNS Domain Name field.

8. Click Resolve.
   The remaining fields populate with the Active Directory domain information.

9. Click Add Domain/Workgroup, and then click Next.

10. Complete the wizard to add the domain or workgroup.

Add credentials to access the new domain

1. In the Patch Manager menu, select Security and User Management.

2. Click Add Credential in the Actions pane.

3. Enter a fully qualified user name (for example: mgomez@company.com) and password in the window, and click Save.

4. Click the Credential Rings tab, and then double-click the <Default> credential ring.

5. In the Credential and Credential Rings Rules Wizard, click the User Name drop-down menu and select the user account to be managed by the new domain.

6. Click Add, and then click Next.

7. Click Add Rule, and then select Active Directory Domain or Workgroup.

8. In the menu, select the network (such as Windows Network) that contains your domain.

9. In the center pane, select your domain and then click Add Selected.
The domain object moves to the bottom of the center pane.

10. Click OK.

11. Select the credential used to create the credential rule, and then click OK.

![Credential Selection](image)

12. Complete the wizard.

**Manage servers in a DMZ outside the local domain**

Perform the following steps to manage your servers in a DMZ outside of your local domain.

1. Verify that HotFix 3 for WMI Providers is installed on the Patch Manager server.

2. Log in to Patch Manager as an administrator.

3. In the Patch Manager navigation menu, expand Enterprise and select Managed Computers.

4. In the Actions pane, click Provision Agent Offline.

5. Complete the procedures in the Patch Manager Agent Provisioning dialog box.

6. Copy the created agent installation package to the machine in the DMZ.

7. Install the agent on the machine in the DMZ.

   See [Patch Manager Agents](#) for details.

8. In the Patch Manager navigation menu, expand Agents.

9. Locate and select your DMZ machine.
Troubleshoot Patch Manager

This section provides basic troubleshooting procedures for Patch Manager. See Patch Manager Logging and Troubleshooting for basic troubleshooting steps you can use in your Patch Manager deployment. See Patch Manager Diagnostics for details about running the Patch Manager Full Diagnostics utility.

General issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>How to troubleshoot and resolve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive consuming too much space on the WSUS server hosting WSUS content</td>
<td>These issues occur when the WSUS database or the disk storing WSUS content is full. As a result, the Patch Manager Web Console can timeout when you select any WSUS view. To resolve these issues, use the Server Cleanup Wizard to remove all unnecessary updates based on rules. This procedure will free up space on your disk and help your WSUS server run at optimal performance.</td>
</tr>
<tr>
<td>WSUS views display inaccurate information</td>
<td></td>
</tr>
<tr>
<td>WSUS connection timeout errors</td>
<td></td>
</tr>
</tbody>
</table>

1. Log in to Patch Manager as an administrator.
2. In the navigation pane, expand Enterprise > Update Services and select your WSUS server.
3. In the Actions pane, click Server Cleanup Wizard.
4. In the WSUS Server Cleanup Options window, select your cleanup options, and then click OK.
5. In the Task Options Wizard, run the task now or create a schedule for the task.
6. Complete the wizard.

Note: See The complete guide to Microsoft WSUS and Configuration Manager SUP maintenance on the Microsoft Support website for additional methods to maintain your WSUS server.

Unable to change the Eminentware Data Grid Server account or password  See Change the account or password used for the Patch Manager service for details.
<table>
<thead>
<tr>
<th>Issue</th>
<th>How to troubleshoot and resolve</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Server Publishing Setup Wizard fails when generating a self-signed WSUS certificate</td>
<td>See <a href="#">How to create a self-signed WSUS certificate when the Server Publishing Setup Wizard fails</a> for details.</td>
</tr>
<tr>
<td>Unable to connect to the Patch Manager clients using WMI</td>
<td>See <a href="#">Unable to connect to clients using WMI</a> for details.</td>
</tr>
<tr>
<td>Unable to connect to the Patch Manager server using a remote console</td>
<td>See <a href="#">Unable to connect to the Patch Manager server using a remote console</a> for details.</td>
</tr>
<tr>
<td>Issues with a downstream WSUS server</td>
<td>See <a href="#">Troubleshoot downstream WSUS server issues in Patch Manager</a> for details.</td>
</tr>
<tr>
<td>Troubleshooting WMI connections</td>
<td>When you target a remote system for a Managed Computer Inventory task, Patch Manager displays that system in the Enterprise &gt; Managed Computers node. Select a system in the center pane of this view to see useful information about the most recent WMI connection attempt.</td>
</tr>
<tr>
<td>Managed Computers and Update Services do not display an identical list of managed computers</td>
<td>See <a href="#">Managed Computers and Update Services inventories do not match</a> for details.</td>
</tr>
</tbody>
</table>

### Error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>How to troubleshoot and resolve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error when performing an Advanced install with Microsoft® SQL Server 2012</td>
<td>The SQL Server® name was not entered correctly during the installation. See <a href="#">Error when installing Patch Manager on Microsoft SQL Server 2008 or 2012</a> for details.</td>
</tr>
<tr>
<td>Error message stating that you exceeded the allowed license count</td>
<td>SolarWinds licenses Patch Manager according to the number of managed systems. Managed systems include all WSUS, ConfigMgr, and Patch Manager servers, as well as all managed clients. The Primary Application Server (PAS) calculates the number of managed systems using the Managed Computers and Task History nodes located in the Patch Manager menu. See <a href="#">License Count exceeded error in Patch Manager</a> for details.</td>
</tr>
<tr>
<td>Error</td>
<td>How to troubleshoot and resolve</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Access Denied error when you connect Patch Manager to a remote computer</td>
<td>This error can occur when you deploy updates to remote systems or execute other tasks on a remote computer, such as opening Computer Explorer. See Troubleshoot Access Denied Errors in Patch Manager for details.</td>
</tr>
<tr>
<td>Error when generating a report</td>
<td>See Error displays when generating a Patch Manager report for details.</td>
</tr>
<tr>
<td>CreateDirectory Failed error when publishing updates to WSUS</td>
<td>See CreateDirectory Failed error when publishing updates to WSUS for details.</td>
</tr>
<tr>
<td>&quot;Invalid Namespace&quot; errors from the Patch Manager server or managed clients</td>
<td>This error occurs when the Patch Manager server cannot access the WMI Providers or the WMI Providers are not present on the client systems. See Troubleshoot &quot;Invalid Namespace&quot; errors from the Patch Manager server or managed clients for details.</td>
</tr>
<tr>
<td>&quot;Failed to publish packageName&quot; error when publishing packages from Patch Manager to the WSUS server</td>
<td>See Unable to publish packages from Patch Manager to the WSUS server for details.</td>
</tr>
<tr>
<td>&quot;Verification of Signature failed for file&quot; error when publishing packages from Patch Manager to the WSUS server</td>
<td>See Publishing packages error: Verification of Signature failed for file in Patch Manager for details.</td>
</tr>
<tr>
<td>Access Denied error</td>
<td>See Troubleshoot Access Denied errors in Patch Manager for details.</td>
</tr>
<tr>
<td>License count exceeded error when starting the Patch Manager Administrator Console</td>
<td>See License count exceeded error in Patch Manager.</td>
</tr>
<tr>
<td>Error</td>
<td>How to troubleshoot and resolve</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>API Mismatch error</td>
<td>This error occurs when Patch Manager servers are not running identical Microsoft Windows Server® operating systems. If Windows Server Update Services (WSUS) is configured on a separate system with a different Windows Server operating system, install and enable the Automation Server role on that server to translate the API communications between the WSUS server and the Primary Application Server. See <a href="#">WSUS API Mismatch error in Patch Manager</a> for details.</td>
</tr>
<tr>
<td>Error code 1064: could not start the EminentWare Data Grid Server Service</td>
<td>See <a href="#">Troubleshoot Patch Manager error 1064</a> for details.</td>
</tr>
<tr>
<td>Troubleshooting Microsoft installer error messages and failures</td>
<td>When you deploy a Microsoft® Installer (MSI) package and the installation fails, troubleshoot the issue at the installer lever. For example, you can run the installer from the command line or troubleshoot MSI logging. See <a href="#">Troubleshooting Microsoft Installer Error Message and Failures</a> for details.</td>
</tr>
<tr>
<td>HTTP status 401 error when connecting to a WSUS server</td>
<td>This error can occur when you connect to a WSUS server from the Patch Manager server. See <a href="#">HTTP status 401 error when testing the WSUS connection to Patch Manager</a> for details.</td>
</tr>
<tr>
<td>Incompatible installation type error</td>
<td>The Patch Manager installer does not support an installation on Web Only versions of Orion. See <a href="#">Error: Incompatible installation type found</a> for details.</td>
</tr>
<tr>
<td>Invalid name space error from the Patch Manager server or managed systems</td>
<td>The Patch Manager server can generate an <a href="#">Invalid namespace error when User Account Control (UAC) prevents the server from communicating with the WSUS server</a>. Managed clients can also receive this error when WMI Providers are not installed on these systems. See <a href="#">Troubleshoot Invalid Namespace Errors - server or managed clients</a> for details.</td>
</tr>
<tr>
<td>Timeout error when you execute an Update Services task</td>
<td>Timeout issues can be caused by an unhealthy update server. See <a href="#">Troubleshoot Timeout Errors in Patch Manager</a> for details.</td>
</tr>
</tbody>
</table>
Error | How to troubleshoot and resolve
---|---
Error when connecting to a WSUS server: Failed to retrieve the Update Server Information | See Patch Manager cannot retrieve the Update Server information for details.
Error when connecting to an Application Server | See Unable to connect to the Application Server for details.

Downstream WSUS server issues

The following issues may occur due to downstream WSUS server configurations:

- Systems cannot be moved from an unassigned group
- Systems will not change groups
- Options to change groups or settings are disabled in WSUS
- Patch Manager reports only display upstream server information
- The downstream WSUS does not display added systems

When a WSUS server is in Replica Mode, it inherits the update approvals and computer groups from the parent WSUS server. Most options and settings are disabled (including moving computers and group) because the downstream WSUS server mirrors the parent WSUS server. As a result, a generated report will only show the upstream WSUS server to prevent duplicate information.

The following table lists the differences between autonomous and replica downstream WSUS server configurations.

<table>
<thead>
<tr>
<th>Autonomous Downstream</th>
<th>Replica / Downstream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses another WSUS server as the master repository. Any updates downloaded by the master server are available to the downstream server.</td>
<td>Uses another WSUS server as the master repository. Any updates downloaded by the master server are available to the downstream server.</td>
</tr>
<tr>
<td>Not required to be in the same Active Directory forest as the master to provide full reporting.</td>
<td>Must be in the same Active Directory forest as the master to provide full reporting.</td>
</tr>
<tr>
<td>Allows individual approvals for updates different from the master.</td>
<td>Updates must be approved on the upstream (master) server. Mirrors update approvals, settings, computers, and groups from its parent.</td>
</tr>
<tr>
<td>Downstream WSUS servers must be administered separately.</td>
<td>Downstream WSUS servers are administered by the upstream server.</td>
</tr>
<tr>
<td><strong>Autonomous Downstream</strong></td>
<td><strong>Replica / Downstream</strong></td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Allows flexibility in creating computer groups.</td>
<td>Reports on status of its clients available to the master server.</td>
</tr>
<tr>
<td>Reduces overall bandwidth off-campus as the updates are downloaded from Microsoft once and then distributed to other servers.</td>
<td>Does not upload reports to the master server.</td>
</tr>
</tbody>
</table>

To resolve downstream WSUS server issues, adjust the settings using the WSUS Administration Console.

1. Log in to the server hosting WSUS Server.
2. Open the WSUS Administration Console.
3. Expand the server name and click Options.
4. In the Options pane, click Update Source and Proxy Server.
5. On the Update Source page, select Synchronize from another Windows Server Update Service server.
6. In the Server name field, type the name of the local upstream WSUS server.
7. In the Port number field, type the port number that this WSUS server will use to communicate with the upstream WSUS server. The default port number is 80 (port 8530 on Windows Server 2012).
8. Deselect the This is a replica of the upstream server option, and then click OK.
Set up Patch Manager with SCCM

Microsoft System Center Configuration Manager (SCCM) is a systems management solution used to manage Windows-based computers. This section describes how to set up Patch Manager on a system running SCCM, and supplements the content in this guide.

SCCM is also known as Microsoft Endpoint Configuration Manager.

See the Microsoft Endpoint Configuration Manager documentation on the Microsoft Docs website for details on how to use and implement SCCM in your organization.

Integrate Patch Manager with SCCM

You can integrate Patch Manager and SCCM in one of the following configurations:

- Patch Manager is installed for the first time on an SCCM server
- Patch Manager and SCCM are installed but not integrated on the same server

Below is an example of the System Center Configuration Manager Console.
After you integrate Patch Manager with SCCM, communications between the SCCM console and the host server remain intact.

The Patch Manager Administrator Console communicates with the WSUS servers, while the SCCM console communicates with the WSUS servers through the SCCM server. Patch Manager does not modify the SCCM server, but integrates with the toolbar menus in the SCCM console to extend its functionality.

The following illustration shows a typical deployment for a Patch Manager and SCCM integration.
Integrate Patch Manager and SCCM after installing Patch Manager for the first time

1. Log on to the SCCM server as an administrator.
2. Temporarily disable any antivirus software.
4. Run the SolarWinds Patch Manager installer on the SCCM server.
   The installer prompts you to install any missing prerequisites.
5. Select Patch Manager server components and Patch Manager administration console, and click Next.
6. In the Patch Manager Setup window, click Next.
7. If you accept the End User License Agreement, click Next.
8. Click Next to use the default installation folder. Click Browse to choose a different folder.
9. If you are evaluating Patch Manager, select Express Install - Recommended, and then click Next.

This option installs the WSUS server and Microsoft SQL Server Express. Follow the onscreen instructions to finalize your evaluation installation.

- SQL Server Express has a 10 GB storage limit. To prevent the application from generating errors after several weeks of use, SolarWinds recommends installing SQL Server Express for evaluation purposes only.

- The Patch Manager Configuration Wizard installs and configures the IIS components, Microsoft Update Services, WMI Providers, Patch Manager database, and third-party catalogs. The Patch Manager configuration may require a few minutes to complete.

10. Verify that the Run administration console after this wizard is finished checkbox is selected, and click Finish.

11. In the Product Features Selection window, select WSUS Extension Pack and System Configuration Manager Extension Pack, and click Continue.

   Patch Manager continues with the post configuration, and launches the Patch Manager Administrator Console.

Integrate Patch Manager and SCCM when both applications are installed but not integrated

1. Log on to the SCCM server as an administrator.

2. Temporarily disable any antivirus software.


4. Run the Patch Manager upgrade package.

   - The upgrade package may be the same version as your currently installed Patch Manager version. Patch Manager does not support a 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 Patch Manager version. Contact Technical Support for assistance.

5. If you accept the End User License Agreement, click Next. Patch Manager upgrade installation begins.

   - 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.
Publish 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 SCCM software update point (SUP).

Verify the SUP is configured to synchronize locally published updates

Verify that the software update point (SUP) component properties are configured to synchronize locally-published updates and display the available third-party updates in the Windows Server Update Services (WSUS) or Software Update Point (SUP) servers. Perform this procedure each time you publish third-party updates.

1. Log in to the SCCM console.
2. In the navigation pane, click Administration.
3. In the navigation pane, expand Site Configuration and select Sites.
4. In the center pane, right-click a site and select Configure Site Components > Software Update Point.
5. Click the Products tab.
6. In the tab window, make sure that the Local Publisher and Locally published packages options are selected. You can also select Vendors of already published packages.
7. Click OK.

Publish third-party updates with a direct download URL

Use the Publishing Wizard to download third-party updates and copy the update definition to the Software Update Point (SUP) server. After you publish the third-party updates, verify that the updates are synchronized locally.

1. Log in to the SCCM Console.
2. In the navigation pane, click Software Library.
3. In the Software Library navigation pane, expand 3rd Party Updates > Updates Overview and select All Updates.
4. In the center pane, select the third-party update you want to publish.
5. In the toolbar, click Publish.
6. Click Next.
   The publishing wizard downloads the package.

7. Select the package, and click Next.

8. Click Finish.
   The package is published in your SUP server.

**Publish third-party updates without a direct download URL**

Some third-party update packages require you to download the package from a vendor website (such as Adobe) and accept an end user agreement. Use the Package Download Assistant to download the third-party update files.

When you are finished, use the Publishing Wizard to copy the installation file and update definitions to the Windows Server Update Services (WSUS) or Software Update Point (SUP) server. After the package is published on the SUP server, [verify that the SUP is configured to synchronize locally published updates](#).

1. Log in to the SCCM Console.
2. In the navigation pane, click Software Library.
3. In the Software Library navigation pane, expand 3rd Party Updates > Updates Overview and select All Updates.
4. In the center pane, select the third-party update you want to publish.
5. In the Packages toolbar, click Publish.
6. In the Patch Manager Publishing wizard window, select the third-party update you want to publish, and click Next.
7. Download the source file from the vendor website.
8. Return to the Package Download Assistant window and click Import Source.
9. Browse to the directory that contains the file you want to import, and click Open.

   - The file you select must match the update you selected in step 4. The Package Download Assistant provides the correct filename by default. No need to select the file after you browse to the appropriate folder.

10. Click OK.

11. In the Patch Manager Publishing Wizard window, select the package you want to publish, and click Next.
12. Click Finish.
   The package is published on your SUP server.

**Deploy third-party updates**

After you publish the third-party updates *with* or *without* a direct download URL, deploy the third-party updates to your managed computers.

1. Log in to the SCCM Console.
2. In the navigation pane, click Software Library.
3. In the Software Library navigation pane, expand Software Updates and select All Software Updates.
4. In the toolbar, click Synchronize Software Updates, and then click OK.
   
   i This operation may require several minutes to complete based on the number of updates. You can track the update progress using the `wsyncmgr.log` file in CMTrace.

5. In the center console, click the Add Criteria drop-down menu, select Vendor, and then click Add.
6. In the search criteria, click the link following the search condition **AND** Vendor.

   The list of available vendors populates automatically.

7. Select the third-party update vendor you previously published, and click Search.

   i To save the search criteria, click Save Current Search under the Search tab.

8. Select a previously-published update.
   
   When you select an update, information about the update displays at the bottom of the console.

9. Right click the update and select Deploy.

10. In the Deploy Software Updates Wizard, complete the Deployment Name, Software Update Group, and Collection fields, and then click Next.

11. In the Deployment Settings window, keep the default values, and click Next.

12. In the Scheduling window, set the Time based on setting to UTC (Coordinated Universal Time) and choose an installation deadline, and then click Next.

13. In the User Experience window, define the user experience for your deployment, and click Next.

   For example, the following settings force the installation if the deadline is met and prevents a forced server restart.
14. In the Alerts window, set the alert thresholds to alert you if a defined percentage of machines were not updated prior to the deadline, and click Next.

   If alert thresholds are not required, keep the default settings, and click Next.

15. Under Deployment Package, select Create a new deployment package and set Package source to your shared source folder on the SCCM server, and click Next.

   ! To prevent the download from failing, verify that the target folder exists.

16. Click Add and select Distribution Point.

17. In the Add Distribution Points window, select a distribution point, and click OK.

18. Click Next to continue.

19. In the Download Location window, select Download software updates from a location on my network.

20. Point to your WSUS Content folder on WSUS or SUP server, and click Next.

21. In the Language Selection window, select English for your select products and click Next.

22. In the Download Settings window, select Download software updates from distribution point and install, and then click Next.

23. In the Summary window, review the settings and save the deployment as a template, and then click Next.

   The updates download to the SCCM source folder and deploy to the distribution point.

   If the download is successful, the following message displays:

   The Deploy Software Update Wizard completed successfully.

24. Click Close.

**Install third-party updates on the client computer**

After you deploy the third-party updates, use the Software Center to check and install the third-party updates in your client machine.

1. Log in to the targeted client computer.

2. Click the Search icon, search for Software Center, and then select this option.

   ! The Software Center page may vary based on policies implemented in your company or organization.

3. In the Available Software tab, select the third-party updates to install.
4. Click Install Selected.

If the installation is successful, the STATUS column for the update displays Installed.

Manage the published third-party updates

This section provides general instructions for managing third-party updates from the SCCM console. For detailed examples of how to publish specific vendor updates, see Publish trial updates.

Create a third-party updates view in the SCCM console

You can publish, manage, and deploy third party updates from the Patch Manager server. The SCCM console allows you to view your third-party updates by vendor using saved searches.

Create a saved search in the SCCM console to differentiate between third-party update vendors. When you are finished, you can access the saved searches in the Search tab.

1. Log in to the SCCM console.
2. In the navigation pane, click Software Library.
3. In the Software Library navigation pane, expand Overview > Software Updates and click All Software Updates.
4. Click Add Criteria, select a search category, and then click Add.
   For example, Downloaded.
5. (Optional) Repeat step 4 to add additional search criteria.
6. Under the Search field, click the link next to AND Downloaded and select No.
7. Click the Search tab.
   SCCM returns a list of software products that are not downloaded on the targeted systems.
8. In the toolbar, click Save Current Search.
9. Enter a saved search name. For example, Software Not Downloaded.

10. Click OK.

Manage the publishing servers in SCCM

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

The Server Publishing Wizard is not available in the SCCM console. If required, complete the wizard in the MMC-based Patch Manager Administrator Console. See Manage the publishing servers for details.

Import and export catalogs using the SCCM console

You can import and export package catalogs in the SCCM console to move software publishing catalogs between Patch Manager servers.

Import catalogs from a portable catalog file

Run 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.

1. Log in to the SCCM console.
2. In the navigation pane, click Software Library.
3. In the Software Library navigation pane, expand 3rd Party Updates > Updates Overview and select All Updates.
4. Click Import To Catalog.
5. In the Select Catalog File screen, locate or enter the complete path for the catalog (.cab) file you want to import, and then click Next.
6. In the Import Details screen, select the package(s) you want to import, and then click Next.
7. Review the import results, and then click Finish.

Export catalogs to a portable catalog file

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:
• Export the entire library of packages into a catalog file
• Export one or more selected packages into a catalog file

The following table describes the export options in this wizard.

<table>
<thead>
<tr>
<th>Selection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include downloaded package content when exporting</td>
<td>Exports all installers and other files you downloaded for the packages you are exporting.</td>
</tr>
<tr>
<td></td>
<td>If you select this option, use the Additional Files dialog to select files on a per-file basis.</td>
</tr>
<tr>
<td>Export the selected software packages to a cabinet file that can be</td>
<td>Select this option if you selected one or more packages to export prior to launching the wizard.</td>
</tr>
<tr>
<td>imported by other publishers</td>
<td></td>
</tr>
<tr>
<td>Export all software packages to a cabinet file that can be imported by</td>
<td>Exports all packages in your library.</td>
</tr>
<tr>
<td>other publishers</td>
<td></td>
</tr>
<tr>
<td>Export File Name</td>
<td>Enter or browse to the file you want to use for the export. This field requires a fully qualified file path.</td>
</tr>
</tbody>
</table>

To export packages to a portable catalog file:

1. Log in to the SCCM console.
2. In the navigation pane, click Software Library.
3. In the Software Library navigation pane, expand 3rd Party Updates > Updates Overview and select All Updates.
4. In the center pane, select one or more packages.

   The wizard lets you export specific packages based on your selection, or all packages regardless of your selection. Press Ctrl+click to select multiple packages.
5. In the toolbar, click Export To Catalog.
6. Complete the Export Options screen, and click Next.
7. Review the export results, and click Finish.

Create and publish software packages

Use Patch Manager to create and publish custom software packages to the SolarWinds third-party updates library on your WSUS server. These packages can be distributed to your managed computers in your Patch Manager deployment.
Manage third-party packages in SCCM

After you [create a software package](#), select the package in the Patch Manager Administrator Console to view the package details in the Details pane.

**View the package details**

When you select a package in the All Updates node of the console, Patch Manager displays detailed information about the package in the following tabs.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package Details</td>
<td>Displays the package description and metadata. Similar to the Update Details tab for WSUS updates.</td>
</tr>
<tr>
<td>Prerequisite Rules</td>
<td>Displays the package prerequisite rules. These rules typically apply to the machine and the operating system.</td>
</tr>
<tr>
<td>Applicability Rules</td>
<td>Displays the package applicability rules. If the package is new, these rules determine if the package is currently installed. If the package is an upgrade, these rules check for a previous version.</td>
</tr>
<tr>
<td>Installed Rules</td>
<td>Displays the package installed rules. When the machine checks in with WSUS for the latest updates, these rules verify if the software is currently installed.</td>
</tr>
</tbody>
</table>

**Verify the 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 previously downloaded for the package to what is currently available from the vendor.

This task:

- 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.
- 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 defined files.
- Provides a Repair option to remediate any repairable conditions.

To check the integrity of one or more downloaded packages:

1. Select one or more downloaded packages.
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.

Check the package publication status
Use the Check Publication Status task to determine if a package was published to a WSUS server.

1. Select the packages you want to check.
2. In the Actions pane, click Publication Status.
3. In the Package Publication Status Wizard, select the update servers you want to check against, and click Next.
4. Review the results, and click Close.

Manage the WSUS servers using the SCCM console
Use the 3rd Party Updates > Administration > Update Servers node in the SCCM console to manage your Windows Server Update Services (WSUS) or Software Update Point (SUP) server as you would in the native WSUS console. This node lists each WSUS server you registered with Patch Manager in the center pane. Select a WSUS server to view WSUS management options in the ribbon.

Synchronize the WSUS server with the upstream server
Run the Synchronize Server task to synchronize the selected WSUS server with the upstream server. You can review the server synchronization information in the SCCM console on the Server Settings tab located at 3rd Party Updates > Administration > Update Servers > your_WSUS_Server_view.

SolarWinds recommends that you schedule ongoing 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 SCCM console.

1. Log in to the SCCM console.
2. In the navigation pane, click Software Library.
3. In the Software Library navigation pane, expand 3rd Party Updates > Administration and select Update Servers.
4. In the center pane, select the WSUS server you want to synchronize.
5. In the toolbar, click Synchronize Server.
6. Complete the Task Options Wizard to schedule and execute the synchronization task for the
selected WSUS server.

See Task Options Wizard for additional information.

Clean up the WSUS server using the SCCM console

Run the Server Cleanup Wizard to delete expired updates and update revisions from the WSUS server.

This cleanup method is more efficient compared to the native cleanup task in the WSUS console. For example, you can configure a threshold for the number of days the WSUS server saves non-reporting computers in the console. You can also schedule the task to run daily or weekly on an ongoing basis, which is recommended.

The Server Cleanup Wizard provides several actions you can run simultaneously or individually on the WSUS server.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unused updates and update revisions</td>
<td>Deletes expired updates and revisions that remain unapproved for longer than three months.</td>
</tr>
<tr>
<td>Computers not contacting the server</td>
<td>Deletes computers that have not contacted the Update Server within the computer deletion threshold.</td>
</tr>
<tr>
<td>Configure the computer deletion threshold</td>
<td>Configures the number of days that the computer remains out of contact with the server before it is deleted.</td>
</tr>
<tr>
<td>Unneeded update files</td>
<td>Deletes update files that were declined or not required by the downstream servers.</td>
</tr>
<tr>
<td>Expired Updates</td>
<td>Declines unapproved, expired updates from Microsoft.</td>
</tr>
<tr>
<td>Superceded Updates</td>
<td>Declines unapproved updates that were superseded with approved updates. The system declines superseded updates that remain unapproved for 30 days or longer.</td>
</tr>
</tbody>
</table>

To schedule or execute a WSUS server cleanup task:

1. Log in to the SCCM console.
2. In the navigation pane, click Software Library.
3. In the Software Library navigation pane, expand 3rd Party Updates > Administration and select Update Servers.
4. In the center pane, select the WSUS server you want to clean up.
5. In the toolbar, click Server Cleanup Wizard.
6. Select one or more of cleanup options, and click OK.

7. Complete the Task Options Wizard to schedule and execute the cleanup task for the selected WSUS server.

See Task Options Wizard for details.

**Repair and maintain the Windows Update Agent**

Use the Windows Update Agent Maintenance and Repair task in the SCCM console 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.

1. Log in to the SCCM console.
2. In the navigation pane, click Assets and Compliance.
3. In the Assets and Compliance navigation pane, navigate to the computer you want to repair.
4. Right-click the computer and select RealTime Computer Info.
5. In the Computer Explorer window, click the Actions tab and then click Repair Windows Update Agent.
6. Select the applicable options as described in Repairing and Maintaining the Windows Update Agent.
7. Click OK.
8. Complete the Task Options Wizard to schedule and execute the task for one or more remote systems.

See Task Options Wizard for details.

**Manage the Windows Update Agent Local Policy**

Use the Windows Update Local Policy Management task in the SCCM console to manage the Windows Update Agent policy using Local Policy on one or more remote systems. This policy can help you manage computers in non-Active-Directory environments or when you prefer not to use Group Policy.

For details about the policies in this task, see the Windows Server Update Services 3.0 SP2 Deployment Guide located on the Microsoft TechNet website.

This task requires WMI connectivity with your remote systems. For details about enabling WMI connectivity between the Patch Manager server and the remote systems, see Manage Client WMI connectivity for details.
To manage Windows Update Agent policy on a remote system:

1. Log in to the SCCM console.
2. In the navigation pane, click Assets and Compliance.
3. In the Assets and Compliance navigation pane, select the computer you want to update.
4. Right-click the computer and select RealTime Computer Info.
5. In the Computer Explorer window, click the Actions tab and then click Windows Update Local Policy.
6. In the Windows Update Local Policy Settings window, click the check box next to each setting to toggle between Not Configured, Disabled, and Enabled states.
7. After you configure the desired settings, click Save.
8. In the Windows Update Local Policy Settings Template window, enter a name for the new template, and then click Save.

   ![If you want to load an existing template, click Load, and then browse to the template you want to load.](image)

9. Click OK.
10. Complete the Task Options Wizard to schedule and execute the task for one or more remote systems.

   See [Task Options Wizard](#) for details.

### Provision the WMI Providers using the SCCM console

During the initial configuration steps, the Patch Manager installer provides the option to automatically provision WMI Providers to all managed clients as required. If you did not select automatic provisioning or you want to deploy WMI Providers, complete the following procedure.

1. Log in to the SCCM console.
2. In the navigation pane, click Assets and Compliance.
3. In the Assets and Compliance navigation pane, select the computer you want to update.
4. Right-click the computer and select RealTime Computer Info.
5. In the Computer Explorer window, click the Action tab and then click Check Computer Access.
6. In the Computer Management window, select Install the WMI Providers if not already installed, and then click OK.
7. Complete the Task Options Wizard to specify the target systems and schedule and execute the task.

See Task Options Wizard for details.

Resolve WMI connectivity issues using the SCCM console

If you recognize an issue with WMI connectivity to a remote system, use the Check Computer Access task to resolve the issue. This launches the same dialog you use to provision the WMI providers to remote systems.

1. Log in to the SCCM console.
2. In the navigation pane, click Assets and Compliance.
3. In the Assets and Compliance navigation pane, locate and select the computer you want to update.
4. Right-click the computer and select Realtime Computer Info.
5. In the Computer Explorer window, click the Actions tab and then click Check Computer Access.
6. In the Computer Access Management window, complete the following dialog boxes:
   - SolarWinds WMI Providers actions
   - Additional options
7. Complete the Task Options Wizard to specify the target systems and schedule and execute the task.

See Task Options Wizard for details.

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 options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check if WMI Providers are installed</td>
<td>Checks the WMI Providers on the remote system. You can view the results from this check in the Patch Manager Task History, or configure the task to email you the results.</td>
</tr>
<tr>
<td>Install the WMI Providers if not already installed</td>
<td>Installs the WMI Providers when required. This option also allows you to reinstall the WMI Providers.</td>
</tr>
<tr>
<td>Uninstall the WMI Providers</td>
<td>Uninstalls the WMI Providers from the remote system.</td>
</tr>
</tbody>
</table>
Additional options in the Computer Management window

The Computer Access Management window includes additional options to configure remote systems that allow WMI connections. The following table lists the available settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable DCOM if disabled</td>
<td>Enables Distributed COM (DCOM) on the remote system. This is a requirement for Patch Manager to use WMI to connect to remote systems.</td>
</tr>
<tr>
<td>Configure DCOM permissions to include 'Administrators' group if needed</td>
<td>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.</td>
</tr>
<tr>
<td>Enable the Remote Administration firewall rule (Windows Firewall/Advanced Firewall only)</td>
<td>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.</td>
</tr>
<tr>
<td>Enable Windows Installer service if disabled</td>
<td>Re-enables the Windows Installer service on the remote system. Patch Manager requires this service to install the WMI Providers.</td>
</tr>
<tr>
<td>Enable MSI Logging</td>
<td>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.</td>
</tr>
</tbody>
</table>

Verify WMI connectivity using the SCCM console

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.

1. In the navigation pane, click Assets and Compliance.
2. In the Assets and Compliance navigation pane, locate and select the computer you want to update.
3. Right-click the computer and select RealTime Computer Info.
4. In the Computer Explorer window, click Quick Inventory on the Actions tab.
5. On the Inventory Options window, select Inventory – verify access only.
6. Click OK.
7. Complete the Task Options Wizard to specify the target systems and schedule and/or execute the task.

   See Task Options Wizard for details.

   You can view the results from this check in the Patch Manager Task History, or configure the task to email you the results.

## Troubleshoot Patch Manager in SCCM

This section provides basic troubleshooting procedures for integrating Patch Manager with the Microsoft System Center Configuration Manager (SCCM).

<table>
<thead>
<tr>
<th>Issue</th>
<th>How to troubleshoot and resolve</th>
</tr>
</thead>
</table>
| SCCM does not synchronize with WSUS/SUP updates | This issue can be caused by:  
  - Not creating a custom search folder for the updates  
  - Not creating a full synchronization  
  - WSUS and SCCM are not synchronized  
  See SCCM does not synchronize with WSUS/SUP updates for troubleshooting. |
| You cannot push software updates to the SCCM software update group | See Unable to push software updates to the SCCM software group for troubleshooting. |
| You cannot view third party packages in the SCCM Console. | See Third party packages do not display in the SCCM Console for troubleshooting. |
Reference

This section contains additional information you can use to customize your Patch Manager deployment.

Patch Manager server settings

Patch Manager consists of three server roles:

- Automation Server
- Application Server
- Management Server

By default, the server that hosts Patch Manager is the Primary Application Server. The remaining servers provide additional functionality for your deployment. All Patch Manager servers include the Automation Server role.

You can configure the Automation Server, Application Server, and Management Server settings in the Patch Manager Administrator Console.

💡 Based on your deployment needs, you can install a secondary application server (SAS). This server can independently download third-party packages from the SolarWinds third-party catalog and control separate Windows Server Update Services (WSUS) servers that are not configured to work with the PAS.

Automation Server settings

You can access the Automation Server settings in the Patch Manager Administrator Console. These settings allow you to configure the Automation Server hosted on a Patch Manager server.

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Value</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent client cache timeout (in seconds)</td>
<td>30</td>
<td>Agent Subsystem Settings</td>
</tr>
<tr>
<td>Automation Server Security Audit Failure Event Logging Enabled</td>
<td>Enabled</td>
<td>Event Logging</td>
</tr>
<tr>
<td>Automation Server Security Audit Success Event Logging Enabled</td>
<td>Enabled</td>
<td>Event Logging</td>
</tr>
<tr>
<td>Automation Server Error Event Logging Enabled</td>
<td>Enabled</td>
<td>Event Logging</td>
</tr>
<tr>
<td>Global Catalog full replication timeout (in minutes)</td>
<td>240</td>
<td>Agent Subsystem Settings</td>
</tr>
<tr>
<td>Automation Server Information Event Logging Enabled</td>
<td>Enabled</td>
<td>Event Logging</td>
</tr>
</tbody>
</table>

To access the Automation Server settings:
1. Log in to the Patch Manager Administrator Console as an administrator.

2. In the navigation pane, expand Patch Manager System Configuration and select Patch Manager Servers.

3. In the center pane, select the Automation Server and then select the Automation Server Settings tab.

The following sections describe the settings for each category.

Event Logging

The Event Logging settings control how the Automation Server logs incidents 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

The Event Logging settings on the Automation Server Settings tab overwrite the corresponding settings on both the Application Server Settings and Management Server Settings tabs.

General

The General settings define the general options for the Application Server.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation Server Enabled</td>
<td>Enables the Automation Server on a Patch Manager server.</td>
</tr>
</tbody>
</table>

Logging

The Logging settings define how Patch Manager generates detailed debug logging. By default, logging is turned on.

SolarWinds recommends enabling this level of logging when engaging in advanced troubleshooting and working with SolarWinds Technical Support.
## Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>Enables debug logging. Patch Manager writes these logs to the following folder: %programdata%\Solarwinds\PM\Log</td>
</tr>
</tbody>
</table>

Logging impacts server performance and can consume significant disk space if you leave it enabled for an extended period of time.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Level</td>
<td>Defines the logging level when logging is enabled.</td>
</tr>
<tr>
<td></td>
<td>Select one of the following levels:</td>
</tr>
<tr>
<td></td>
<td>- 1 (Normal logging): Enables logging for any program code object that is</td>
</tr>
<tr>
<td></td>
<td>configured to provide normal logging.</td>
</tr>
<tr>
<td></td>
<td>- 2 (Verbose logging only): Enables logging for any program code object</td>
</tr>
<tr>
<td></td>
<td>that is configured to provide verbose logging.</td>
</tr>
<tr>
<td></td>
<td>- 3 (Normal and verbose logging): Enables both normal and verbose logging</td>
</tr>
<tr>
<td></td>
<td>for all applicable program code objects.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Output</td>
<td>Defines the output type when logging is enabled.</td>
</tr>
<tr>
<td></td>
<td>Select one of the following output types:</td>
</tr>
<tr>
<td></td>
<td>- 1 (Output file): Writes debug logs to the logging folder with a log.txt</td>
</tr>
<tr>
<td></td>
<td>extension.</td>
</tr>
<tr>
<td></td>
<td>- 2 (Debug stream): Writes debug logs to a debug stream. Use this option</td>
</tr>
<tr>
<td></td>
<td>when using a debugger, such as the Microsoft DebugView utility.</td>
</tr>
<tr>
<td></td>
<td>- 3 (Hybrid output): Writes debug logs to both an output file and debug</td>
</tr>
<tr>
<td></td>
<td>stream.</td>
</tr>
</tbody>
</table>

## Worker Process Settings

The Worker Process Settings define how Patch Manager servers in the Automation Server role execute their worker processes. Worker processes manage tasks assigned to an Automation Server. When required, they execute on demand.

The following settings define when to queue worker processes if Patch Manager requests several tasks at the same time.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Worker Processes</td>
<td>Defines the maximum number of worker processes the Automation Server can run at once.</td>
</tr>
<tr>
<td>Maximum Thread Pool Size per Worker Process</td>
<td>Defines the maximum number of threads each worker process can execute at once.</td>
</tr>
<tr>
<td>Enable Worker Process Memory Usage Quota</td>
<td>Defines a memory usage quota for the worker processes.</td>
</tr>
<tr>
<td>Shutdown Worker Process after being idle for (in minutes)</td>
<td>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.</td>
</tr>
<tr>
<td>Worker Process Memory Usage Quota</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum retry count for Worker Process Job</td>
<td>Defines the maximum number of times a worker process will retry a failed job.</td>
</tr>
<tr>
<td>Worker Process startup time limit (in seconds)</td>
<td>Defines the maximum start-up time for the worker processes. Specify the number of seconds Patch Manager should wait before terminating a worker process that does not start immediately.</td>
</tr>
</tbody>
</table>

**Application Server settings**

You can access the Application Server settings in the Patch Manager Administrator Console. These settings allow you to configure the Application Server hosted on a Patch Manager server.
1. Log in to the Patch Manager Administrator Console as an administrator.

2. In the navigation pane, expand Patch Manager System Configuration > Patch Manager Servers.


4. In the center pane, select the Management Server and then select the Application Server Settings tab.

The following sections describe the settings for each category.

**Application Server Communication Settings**

These settings control how the Application role server handles communication failures with remote systems.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of retries to attempt on communication failure</td>
<td>Defines the frequency that the Application Server attempts to communicate with a remote system if a task is unable to connect. Select a value from 0 to 10.</td>
</tr>
<tr>
<td>Retry delay on communications failure (in seconds)</td>
<td>Defines the retry interval handling communication failures. Select the number of seconds Patch Manager should wait between retry attempts. Select a value from 0 to 60.</td>
</tr>
</tbody>
</table>

**Application Server Job Pool Settings**

These settings control the number of concurrent jobs Patch Manager allows.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Concurrent Jobs</td>
<td>Defines the total number of jobs that can run at the same time across all Management Server roles. Each Management Server role includes this setting to limit the concurrent jobs by each server.  Select a value from 4 to 16.</td>
</tr>
</tbody>
</table>

**Email Configuration**

The Email Configuration settings define the email and Simple Mail Transfer Protocol (SMTP) server settings for email notifications Patch Manager sends from the Application Server role.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Configuration: Sender email Address</td>
<td>Defines the sender e-mail address Patch Manager uses when sending email notifications from the Application Server.</td>
</tr>
<tr>
<td>Email Configuration: Sender email Name</td>
<td>Defines the sender e-mail name Patch Manager uses when sending email notifications from the Application Server.</td>
</tr>
<tr>
<td>Email Configuration: SMTP Server Name (Outgoing)</td>
<td>Defines the SMTP server Patch Manager uses when sending email notifications from the Application Server.</td>
</tr>
<tr>
<td>Email Configuration: SMTP Server Port Number</td>
<td>Defines the SMTP port number Patch Manager uses when sending email notifications from the Application Server.</td>
</tr>
<tr>
<td>Email Configuration: SMTP Server requires authentication</td>
<td>Defines whether the SMTP server requires authentication to send email.</td>
</tr>
<tr>
<td>Email Configuration: SMTP Server logon user password</td>
<td>Defines the user password Patch Manager uses when sending email notifications from the Application Server using an authenticated mail server.</td>
</tr>
<tr>
<td>Email Configuration: SMTP Server uses encrypted SSL connection</td>
<td>Defines whether the SMTP server uses an encrypted Secure Socket Layer (SSL) connection.</td>
</tr>
<tr>
<td>Email Configuration: SMTP Server uses encrypted TLS connection</td>
<td>Defines whether the SMTP server uses an encrypted Transport Layer Security (TLS) connection.</td>
</tr>
</tbody>
</table>
### Event Logging

The Event Logging settings 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

ℹ️ In the Automation Server Settings tab, these category settings overwrite the corresponding settings in the Application Server Settings and Management Server Settings tabs.

### General

The General settings define the general options for the Application Server role.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically archive Task History Days</td>
<td>Defines the retention period for old Task History items. Select the number of days Patch Manager should wait before deleting old Task History items.</td>
</tr>
<tr>
<td>Automatically archive Task History Enabled</td>
<td>Enables Patch Manager to delete old Task History items after a specific period of time.</td>
</tr>
</tbody>
</table>

### Patch Manager Update

The Patch Manager Update settings define when and how the Application Server connects to and synchronizes with the SolarWinds third party updates library.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically Purge Synchronization History</td>
<td>Enables Patch Manager to automatically delete synchronization history items after a specific period of time.</td>
</tr>
<tr>
<td>Automatically Purge Synchronization History Threshold in Days</td>
<td>Defines the purge threshold for synchronization history items. Specify the number of days Patch Manager should wait before deleting synchronization history items.</td>
</tr>
<tr>
<td>Catalog Settings</td>
<td>Selects the third party updates library that the Application 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.</td>
</tr>
<tr>
<td>Enabled Patch Manager Update Notification emails</td>
<td>Enables the Application Server to send email notifications when it synchronizes new, expired, or revised updates.</td>
</tr>
<tr>
<td>Patch Manager Update Notification recipients</td>
<td>Defines the recipients who receive synchronization email notifications. Enter the email addresses separated by a comma with no spaces.</td>
</tr>
<tr>
<td>Frequency in hours of how often to synchronize</td>
<td>Defines the synchronization frequency for the Application Server. Enter the frequency (in hours) that the server should synchronize with the SolarWinds third-party updates library.</td>
</tr>
<tr>
<td>Proxy Port Number</td>
<td>Defines the port number the Application Server should use to connect to the Internet using a proxy server.</td>
</tr>
<tr>
<td>Proxy Domain</td>
<td>Defines the user logon domain the Application Server should use when connecting to the Internet using an authenticated proxy.</td>
</tr>
<tr>
<td>Proxy User Name</td>
<td>Defines the user logon name the Application Server should use when connecting to the Internet using an authenticated proxy.</td>
</tr>
<tr>
<td>Proxy Server Name</td>
<td>Defines the proxy server the Application role server should use when connecting to the Internet.</td>
</tr>
<tr>
<td>Subscription</td>
<td>Defines the Application third party catalog subscriptions using an XML value. To modify this setting, use the Synchronization Settings action in the Software Publishing node.</td>
</tr>
<tr>
<td>Synchronization Start Time</td>
<td>Defines the time when the Application Server synchronizes with the SolarWinds third party updates library. Select the time for the first update by selecting the number of minutes after midnight you want it to start.</td>
</tr>
</tbody>
</table>
### Setting | Description
--- | ---
**Synchronization Type** | Enables the Application 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 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
The Scheduled Task Scheduler settings define how the Application Server role handles scheduled tasks.

| Setting | Description |
--- | --- |
**Maximum concurrent executing schedule tasks** | Defines the total number of scheduled tasks the Application Server can execute at once. Select a value from 1 to 50.

### Management Server settings
You can access the Management Server settings in the Patch Manager Administrator Console. These settings allow you to configure the [Management Server](#) hosted on a Patch Manager server.

1. Log in to the Patch Manager Administrator Console as an administrator.

2. In the navigation pane, expand Patch Manager System Configuration > Patch Manager Servers.

4. In the center pane, select the Management Server and then select the Management Server Settings tab in the lower center pane.

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.

The following sections describe the tab settings for each category.

Event Logging

The Event Logging settings control how the Management Server logs to the Windows Event Log on the Patch Manager server. Enable or disable the following settings to define the events added to the log:

- 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

The Event Log settings in 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of retries on communication failure</td>
<td>Defines the frequency Patch Manager attempts to communicate with a remote system if a task is unable to connect. Select a value from 0 to 10.</td>
</tr>
<tr>
<td>Retry delay on communications failure (in seconds)</td>
<td>Defines the retry interval handling communication failures. Select the number of seconds Patch Manager should wait between retry attempts. Select a value from 0 to 60.</td>
</tr>
</tbody>
</table>

Management Server Job Pool settings

The Management Server Job Pool settings control the number of concurrent jobs allowed by the Management Server.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Concurrent Jobs</td>
<td>Defines the total number of jobs that can run at the same time across the Management Server. Each Application Server includes this setting to limit concurrent jobs across all Management Servers. Select a value from 4 to 16.</td>
</tr>
</tbody>
</table>

**Orion Web Console components**

The tables in this section list the SolarWinds Orion Platform services and programs installed by the Patch Manager Web Console installer. 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 Service V2</td>
<td>Processes advanced alerts for Orion Platform products</td>
<td></td>
</tr>
<tr>
<td>SolarWinds Collector Service</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 V2</td>
<td>Polls data from network devices and executes some management tasks</td>
<td></td>
</tr>
<tr>
<td>SolarWinds Orion Module Engine</td>
<td>Hosts and executes program functions</td>
<td>Yes</td>
</tr>
<tr>
<td>SolarWinds Syslog Service</td>
<td>Receives and processes syslog messages</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 Service</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 v2</td>
<td>Polls data from network devices and executes some management tasks</td>
<td></td>
</tr>
<tr>
<td>SolarWinds Orion Module Engine</td>
<td>A collection of Orion website services, which include:</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>- SolarWinds Job Engine v2</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 Recommendations</td>
<td>An optional service to collect and report usage statistics to SolarWinds, Inc.</td>
<td></td>
</tr>
<tr>
<td>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>Alerting, Reporting, and Mapping</td>
<td>Contains programs to create and manage Orion alerts, reports, and maps</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Supported</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Configuration Wizard</td>
<td>Opens the SolarWinds Configuration Wizard</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Discovery</td>
<td>Opens the Network Discovery program</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>
<tr>
<td>Syslog Viewer</td>
<td>Opens the Syslog Viewer</td>
<td></td>
</tr>
<tr>
<td>Trap Viewer</td>
<td>Opens the Trap Viewer</td>
<td></td>
</tr>
</tbody>
</table>

**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 /?
```

The following table lists the commands you can run in Patch Manager.

<table>
<thead>
<tr>
<th>To perform this task...</th>
<th>Run this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a Patch Manager server to the environment and automatically register with the PAS (obtain and install the required server certificates)</td>
<td><code>setuphelper /provisionserver /type primary</code></td>
</tr>
<tr>
<td>Add a Patch Manager server to the environment and locally install the required server certificates</td>
<td><code>setuphelper /provisionserver /type local</code></td>
</tr>
<tr>
<td>Add a service account to the environment</td>
<td><code>setuphelper /provisionserviceaccount &lt;fullname of service account&gt;</code></td>
</tr>
<tr>
<td>To perform this task...</td>
<td>Run this command...</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Create the first management group</td>
<td>setuphelper /createmgmtgroup &quot;Managed Enterprise&quot; /description &quot;The Managed Enterprise Management Group&quot; /addserver &lt;deviceid&gt;</td>
</tr>
<tr>
<td>Assign a server to a specific management group</td>
<td>setuphelper /assignservertomgmtgroup &lt;managementGroupID&gt; addserver &lt;deviceID&gt;</td>
</tr>
<tr>
<td>Remove the local server from the environment</td>
<td>setuphelper /unregisterserver</td>
</tr>
<tr>
<td>Reset the ACLs on a server</td>
<td>setuphelper /secureserver /rootdirectory &quot;C:\Program Files\EminentWare&quot; /serviceaccountname &lt;fullname of service account&gt; /sqlinstance THISMACHINE\EMINENTWARE</td>
</tr>
<tr>
<td>Reset the ACLs on a console-only installation</td>
<td>setuphelper /secureconsole /rootdirectory &quot;C:\Program Files\EminentWare&quot;</td>
</tr>
<tr>
<td>Re-provision the Patch Manager certificate</td>
<td>setuphelper /reprovisioncertificates</td>
</tr>
<tr>
<td>Uninstall Patch Manager</td>
<td>setuphelper /uninstall</td>
</tr>
<tr>
<td>Create a custom event log</td>
<td>setuphelper /createcustomeventlog</td>
</tr>
<tr>
<td>Remove the custom event log</td>
<td>setuphelper /deletecustomeventlog</td>
</tr>
</tbody>
</table>