Copyright and Trademarks

This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as “Ivanti”), and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.ivanti.com.

Copyright © 2014 - 2017, Ivanti. All rights reserved.

Ivanti and its logos are registered trademarks or trademarks of Ivanti, Inc. and its affiliates in the United States and/or other countries. Other brands and names may be claimed as the property of others.

Document Information and Print History

Document number: N/A

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 2014</td>
<td>Initial version</td>
<td>Initial release of the Shavlik Patch for Microsoft System Center User’s Guide.</td>
</tr>
<tr>
<td>November 2014</td>
<td>Shavlik Patch 2.1</td>
<td>Add synchronization info for third-party updates. Update the system requirements. Add new info on Configuration Checker, composite filters, details pane, proxy configuration, supersedence, metadata, languages, and end of life.</td>
</tr>
<tr>
<td>January 2015</td>
<td>Shavlik Patch 2.1, Rev A of manual</td>
<td>Update WSUS Server screenshots to show use of SSL connection.</td>
</tr>
<tr>
<td>March 2016</td>
<td>Shavlik Patch 2.2</td>
<td>Add new 2.2 features, including ability to edit updates, publish as metadata-only, manage products, pre-download updates, and more.</td>
</tr>
<tr>
<td>October 2016</td>
<td>Shavlik Patch 2.3</td>
<td>Add support for third-party catalogs, bundles, detectoids and offline mode. Document the new licensing process and update the prerequisites.</td>
</tr>
<tr>
<td>April 2017</td>
<td>Ivanti Patch for SCCM 2.3, Update 1</td>
<td>Rebranded the guide to Ivanti. Removed reference to 100 category limit.</td>
</tr>
</tbody>
</table>
# Table of Contents

Welcome to Ivanti Patch for SCCM ........................................................................................... 5  
System Requirements ........................................................................................................... 5

Installation and Configuration .................................................................................................. 7  
Installing the Ivanti Patch for SCCM Add-in .......................................................................... 7  
Configuring Your Ivanti Patch for SCCM Settings ................................................................. 9  
WSUS Server Tab .................................................................................................................... 10  
  WSUS Server Information ................................................................................................... 10  
  Code Signing Certificate Information ............................................................................... 11  
Proxy Tab ................................................................................................................................ 11  
License Tab ............................................................................................................................ 12  
  How to Enter a License Key ......................................................................................... 13  
Offline Options Tab ............................................................................................................... 16  
  Local Source Folder ........................................................................................................ 16  
  Offline Mode .................................................................................................................. 17  
Languages Tab ....................................................................................................................... 18  
Catalogs Tab .......................................................................................................................... 19  
  Metadata Options ........................................................................................................... 20  
Verify Setup Tab ................................................................................................................... 21  
About Tab ............................................................................................................................... 22  
Schedule Tab .......................................................................................................................... 22

Preparing to Use Ivanti Patch for SCCM .................................................................................. 23  
  What Gets Added to Configuration Manager .................................................................... 23  
  Toolbar Buttons ................................................................................................................. 24  
Understanding the Information in the Grid .......................................................................... 26

Using the Filters ....................................................................................................................... 28  
  Predefined Filters ........................................................................................................... 28  
  Custom Filters ................................................................................................................ 29  
  Composite Filters ........................................................................................................... 30

Performing Actions on the Grid ................................................................................................ 31  
  Using the Search Tool .................................................................................................... 31  
  Show XML ....................................................................................................................... 31  
  Copy Contents ................................................................................................................ 32  
  Download One or More Updates to the Local Source Folder ........................................... 33  
  Edit Updates ................................................................................................................... 33  
  Unselect All Updates ...................................................................................................... 33

How to Publish Updates ......................................................................................................... 34  
  Manually Publishing Third-Party Updates .................................................................... 34  
  Automatically Publishing Updates Using a Recurring Scheduled Task ................................ 38  
  Viewing and Managing Scheduled Publications .................................................................. 40

Managing Products ................................................................................................................ 41  
  Vendor / Product Categories to Synchronize ................................................................... 41  
  Delete Vendor / Product Categories .............................................................................. 43  
  Performing Actions on the Manage Products Dialog ....................................................... 44
# Table of Contents

**Expiring Third-Party Updates** .............................................................................................................. 45

**How to Edit Updates** .......................................................................................................................... 46
  - Editing Tips ........................................................................................................................................ 47
  - Editing the Binary File Information ............................................................................................... 48
  - Editing the Localized Description ................................................................................................. 49
  - Editing Information ......................................................................................................................... 50
  - Editing Prerequisites ...................................................................................................................... 51
  - Editing Superseded Updates ......................................................................................................... 52
  - Editing Installable Rules and Installed Rules ............................................................................. 52

**Custom Installation Scripts** .............................................................................................................. 53
  - Pre-Install Script and Post-Install Script Tabs ............................................................................... 53
  - Custom Files Tab ........................................................................................................................... 54
  - Tips for Debugging Custom Scripts ............................................................................................. 55
    - Add Tracing ............................................................................................................................... 55
    - Review the Files Contained in the Sandbox Folder ................................................................. 55
  - Testing Your Edits ......................................................................................................................... 55
  - Publishing Your Edits .................................................................................................................... 56

**Working with Bundles and Detectoids** ............................................................................................ 57
  - What are Bundles and Detectoids? .............................................................................................. 57
    - Bundles .................................................................................................................................... 57
    - Detectoids ............................................................................................................................... 57
  - Working with Bundles .................................................................................................................. 57
  - Working with Detectoids ............................................................................................................... 59

**Support Information** ......................................................................................................................... 60
  - Supported Products ......................................................................................................................... 60
  - Technical Assistance ...................................................................................................................... 60
  - End of Life Notification .................................................................................................................. 60

**Appendix A: Creating and Distributing Certificates** ........................................................................ 61
  - Certificate Overview ..................................................................................................................... 61
  - Reference ..................................................................................................................................... 61
  - Certificate Requirements .............................................................................................................. 61
  - Creating a Code Signing Certificate ............................................................................................ 62
    - Creating a Code Signing Certificate Using a CA ................................................................. 62
      - Using Ivanti Patch for SCCM and WSUS to Create a Code Signing Certificate ............... 62
  - Importing a Certificate .................................................................................................................. 66
  - Exporting a Certificate ................................................................................................................... 67
  - Distributing the Certificate ............................................................................................................ 67
    - Using Group Policy to Distribute the Certificate ................................................................. 67
    - Using MMC to Manually Distribute the Certificate ............................................................... 68
    - Renewing an Expiring Signing Certificate ........................................................................... 70
    - How to Re-sign and Deploy Updates After Renewing a Certificate .................................... 70
      - Enabling Your Clients to Download Re-Signed Updates .................................................. 71

**Index** ............................................................................................................................................... 72
Welcome to Ivanti Patch for SCCM

Welcome to Ivanti Patch for SCCM, an add-in that extends Microsoft’s System Center Configuration Manager capabilities by enabling you to publish third-party updates and legacy products no longer supported by Configuration Manager. With Ivanti Patch for SCCM you leverage a single Configuration Manager workflow for publishing updates for both Microsoft and non-Microsoft products.

Ivanti Patch for SCCM consists of two components:

- **Update catalog:** The Ivanti catalog contains the detection and deployment logic used to patch non-Microsoft products and legacy Microsoft products. The catalog consists of a large number of update files from a number of different software vendors including Adobe, Apple, Firefox, Sun, and others. Support for additional catalogs is also provided.

- **Add-in to the Configuration Manager console:** Used to select updates from the catalog, publish them to your WSUS servers, synchronize updates with Configuration Manager, and to expire published updates. This allows you to patch your legacy Microsoft products and your non-Microsoft products using the same Configuration Manager workflow used to patch Microsoft products.

System Requirements

Here are the requirements for installing and using Ivanti Patch for SCCM:

- **Ivanti Patch for SCCM installs as an add-in to an existing Configuration Manager 2012 SP1 or later console or a Configuration Manager 2012 R2 SP1 or later console. The Configuration Manager console must be installed on one of these Windows operating systems:**
  - Windows Server 2012 or later
  - Windows Server 2008 R2 SP1 or later
  - Windows 10 or later, Pro or Enterprise Edition
  - Windows 8 or later
  - Windows 7 SP1 or later

- **.NET Framework 4.6.1 or later**
  If you are missing this requirement, .NET Framework 4.6.2 will be installed for you during the installation of Ivanti Patch for SCCM.

- **Microsoft Visual C++ 2015 Redistributable (x86 and x64)**
  If you are missing these requirements, they will be installed for you during the installation of Ivanti Patch for SCCM.

- **Windows Server Update Services (WSUS) client requirements:**
  - If Ivanti Patch for SCCM is installed on the primary WSUS server and you are using Windows Server 2012 or Windows 8, then the WSUS API and the PowerShell cmdlets features must be enabled.
  - If WSUS is on a remote Windows 8 or Windows 8.1 machine, then the remote admin tools feature must be installed on that machine. The version of the remote
Welcome to Ivanti Patch for SCCM

admin tools and the version of WSUS must match or you will not be able to publish updates.

- If the primary WSUS server is running WSUS 3.0 SP2, then the WSUS 3.0 SP2 Administration Console must be installed on the same machine as Ivanti Patch for SCCM. Patches KB2720211 and KB2734608 must be applied to both the WSUS server and the Configuration Manager Console machines.

- The Microsoft Task Scheduler service must be enabled and the user must have the rights necessary to create scheduled tasks.

- The user running Ivanti Patch for SCCM must:
  - Be a member of the **WSUS Administrators group** on the WSUS server
  - Have **Log on as a batch job** rights
  - Be assigned to the **All instances of the objects that are related to the assigned security roles** security scope

  In addition, if the WSUS Server is remote, the user must be a member of the local administrators group on the WSUS Server.

- Federal Information Processing Standard (FIPS) environments

  When operating in a FIPS environment, the console must be configured as a FIPS-compliant machine before you install Ivanti Patch for SCCM. If FIPS is enabled after the installation, you must reinstall Ivanti Patch for SCCM.

- Client machine requirements:

  Each of your client machines must meet the following requirements in order to deploy non-Microsoft updates distributed by a WSUS server:
  - Must contain a copy of the code signing certificate in the appropriate certificate stores
  - Must have enabled the **Allow signed updates from an intranet Microsoft update service location** policy setting
Installation and Configuration

Installing the Ivanti Patch for SCCM Add-In

Show Me!
To view a video tutorial on this topic, click the video icon on the left.

Note: You must be running as Administrator in order to install the add-in.

1. Using a Web browser, go to: www.shavlik.com/downloads/.
2. Click the Ivanti Patch for SCCM Free Trial link.
4. Close System Center Configuration Manager.
5. Begin the Ivanti Patch for SCCM installation by double-clicking the file named SCCMPatchSetup.exe.
   • If .NET Framework 4.6.1 or later is not installed on the Configuration Manager machine, you will be prompted to install .NET Framework 4.6.2 before continuing with the installation. Follow the on-screen instructions for installing this prerequisite.
   • If all prerequisites are installed, the license agreement is displayed. You must accept the terms of the license agreement in order to install the program.
6. Enable the check box to accept the license agreement and then click Install.
   After the files have been installed the Completed dialog is displayed.
Installation and Configuration

7. Click **Finish**.

Your next steps should be to access the program and configure your settings.
Configuring Your Ivanti Patch for SCCM Settings

Installing the Ivanti Patch for SCCM add-in will add two new list items to the Software Library > Software Updates folder. The new list items are named Ivanti Patch and Published Third-Party Updates. The first time you try to access either of these two new list items the setup wizard will be launched.

The wizard will step you through the tabs involved in the setup process. Ivanti Patch for SCCM is ready to use immediately after you complete the setup and save your settings. You can return to these settings at any time using the Settings button on the Home tab.

After reviewing the information on the Welcome tab, click Next.

The first setup tab is the WSUS Server tab.
WSUS Server Tab

The **WSUS Server** tab is used to configure how the add-in will communicate with your WSUS Server. It is also used to define the certificate that will be used to digitally sign the content that is published to the WSUS server.

**WSUS Server Information**

- **Name**: Confirm the name or IP address of your WSUS Server. This information will normally be detected and automatically populated.

- **Port**: Confirm the port number used when making a connection to your WSUS Server. The default value for unsecured connections is either 80 or 8530. For secured connections you will typically use either 443 or 8531.

- **Use Secure Sockets Layer (SSL) to connect to this server**: If your WSUS Server has been configured to use a secure connection, enable this check box. A secure connection is mandatory if you need to import a signing certificate. See [Importing a Certificate](#) for more information.

- **Test connection**: If you want to test your ability to access the WSUS Server, click **Test connection**.
Code Signing Certificate Information

A code signing certificate is required in order to publish updates to the WSUS server. If you already have a signing certificate in place it will be shown in the Current Certificate area.

You can perform the following certificate tasks:

- **Export**: Exports the current certificate from within Ivanti Patch for SCCM. For security, the certificate is exported without the private key. After exporting the certificate you will distribute it to your clients and to your infrastructure machines (e.g. other machines that run the Ivanti Patch for SCCM add-in, downstream WSUS servers, and Windows Update clients). This is necessary in order for the machines to receive locally published updates.

- **Import**: Imports a code signing certificate that was created by a Certificate Authority (CA). A secure connection is required in order to import a certificate.

- **Create a self-signed certificate**: Creates a code signing certificate for your enterprise. This process uses the services of WSUS to create the certificate.

For detailed information on exporting, importing, creating and renewing certificates, see Appendix A: Creating and Using Certificates.

Proxy Tab

The Proxy tab allows you to modify the proxy settings used by Ivanti Patch for SCCM when accessing the Internet using your Web browser. In general, Ivanti Patch for SCCM checks the proxy settings in Internet Explorer and conducts an Internet connectivity test to determine whether or not proxy server settings are necessary. If Ivanti Patch for SCCM is unable to access the Internet using these settings, or if you are required to enter a user name and password each time you launch your browser and browse the Internet, you will need to configure the proxy options.
Installation and Configuration

- **Do I need proxy information?**: To see if Ivanti Patch for SCCM can use your current Internet Explorer proxy settings to access the Internet and perform other operations, click this button. If the test is successful then nothing further is required. If the test fails it typically means your organization utilizes authentication and you need to modify your proxy settings by specifying credentials (a user name/password).

- **Use proxy**: If enabled, indicates that you will supply proxy credentials. If you clear the check box after specifying credentials, the credentials will be saved but not used.

- **User name**: Type the credential user name. It may be necessary to specify a domain as part of your user name (for example: mydomain\my.name).

- **Password**: Type the credential password.

- **Verify Proxy**: To test the proxy credentials, click this button.

**License Tab**

The **License** tab provides detailed information about your current product license key. If no information is being shown it means you have not licensed the program and you should use the **Enter / refresh license key** button to activate your license. You can also use the **Enter / refresh license key** button to provide an upgraded license key and to refresh and expiring key. See the sections below for instructions on how to enter your license key.

Once you have entered a valid license, the program will immediately access and download the full Ivanti Patch catalog. After that, the program will automatically check for a new catalog on a periodic basis.

The program will notify you if your license key has expired or is set to expire within the next 60 days.
How to Enter a License Key

Until you activate Ivanti Patch for SCCM, you will be very limited in the actions you are allowed to perform. To activate Ivanti Patch for SCCM, follow the instructions in the section below that represents your environment.

If You Have an Internet Connection

1. If you have an electronic copy of your license key(s), copy it to your computer’s clipboard.
2. On the Ivanti Patch for SCCM Settings dialog, click Enter/refresh license key.

The License Activation dialog is displayed.

3. Select an activation mode.
   - **Product license**: Selecting this option enables you to specify one or more activation keys. If you receive multiple keys, be sure to paste them all in the Enter your activation key(s) box. Each key may represent a different set of features, an add-on, or license seat count. The keys are additive so the resulting product license will be a compilation of all features and seat counts provided by the individual keys.
   - **Trial mode**: Enables you to test all the capabilities of Ivanti Patch for SCCM, but only for 60 days. With a trial license, you can publish as many updates as you wish but only for five different products in the catalog. When the trial license expires, most of the program features will no longer be available.
Installation and Configuration

4. (Optional) If you didn't copy the key to your computer's clipboard until after you launched this dialog, click the paste icon. This will paste the key into the **Enter your activation key(s)** box. You can also manually type your activation key if you prefer.

5. (Conditional) If your organization uses a proxy server, click **Configure proxy** and provide the credentials necessary for the activation process to reach the activation server.

   **Tip:** If you are required to enter a user name and password each time you launch a browser to access the Internet, it typically means you are using a proxy server.

6. If your machine has an Internet connection, in the **Select an activation method** box choose **Online**.

   **Important:** If your machine is on a disconnected network and you do not have an Internet connection, choose **Manual**, skip the remainder of this section and follow the instructions in the section titled *If You Do Not have an Internet Connection.*

7. Click **Activate online now**.

   If the activation is successful, the message **Ivanti Patch for SCCM product activation successfully completed** is displayed near the bottom of the dialog.

8. Click **Close**.

### If You Do Not Have an Internet Connection

**Note:** This procedure will not work if you are at a secure site that does not allow files to be transferred out of the secure environment. For this case, see the section below titled *If You are Activating from Within a Secure Disconnected Network.*

1. If you have an electronic copy of your license key(s), copy it to your computer's clipboard.

2. On the **Ivanti Patch for SCCM Settings** dialog, click **Enter/refresh license key**.

3. In the **Select an activation method** box, choose **Manual**.

4. Click **Create request**.

   Two files are generated and saved to the desktop of your console computer: an XML file named **LicenseInfo.xml** and a text file named **DisconnectedLicenseInfo.txt**. The XML file is used in this procedure; the text file can be ignored.

5. Move the XML activation request file to a computer that has an Internet connection.

6. On the Internet-connected computer, open a browser and go to [https://license.shavlik.com/OfflineActivation](https://license.shavlik.com/OfflineActivation).

7. Upload the LicenseInfo.xml activation request file.

   The web portal will process the license information and generate a license file.

8. Download the processed license file and move it to the console computer.

9. Within Ivanti Patch for SCCM, select **Settings > License > Enter/refresh license key**.

10. On the **Ivanti Patch for SCCM License Activation** dialog, click **Import manual license**.
11. Go to the location of the processed license file and then click **Open**.

12. Ivanti Patch for SCCM will process the file and the program will be activated.

**If You are Activating from Within a Secure Disconnected Network**

Use this activation procedure if you are at a secure site that does not allow files to be transferred out of the secure environment.

1. If you have an electronic copy of your license key(s), copy it to your computer's clipboard.
2. On the **Ivanti Patch for SCCM Settings** dialog, click **Enter/refresh license key**.
3. Select an activation mode (either **Product license** or **Trial mode**).
4. Paste or type your key into the **Enter your activation key(s)** box.
5. In the **Select an activation method** box, choose **Manual**.
6. Click **Create request**.
   
   Two files are generated and saved to the desktop of your console computer: an XML file named **LicenseInfo.xml** and a text file named **DisconnectedLicenseInfo.txt**. The text file is used in this procedure; the XML file can be ignored.
7. Open the **DisconnectedLicenseInfo.txt** file and carefully copy the information contained in it to a piece of paper.
8. On an Internet-connected computer, open a browser and go to
   
   **https://license.shavlik.com/OfflineActivation**.
9. Manually enter the activation request data and then click **Submit**.
   
   The web portal will process the data and generate a license file.
10. Download the processed license file and move it to the console computer.
11. Within Ivanti Patch for SCCM, select **Settings > License > Enter/refresh license key**.
12. On the **Ivanti Patch for SCCM License Activation** dialog, click **Import manual license**.
13. Go to the location of the processed license file and then click **Open**.
   
   Ivanti Patch for SCCM will process the file and the program will be activated.
Offline Options Tab

The **Offline Options** tab is used for two related purposes:

- The **Local Source Folder** area provides an alternate location to specify software update content.
- The **Offline Mode** area supports environments that do not have an Internet connection.

Local Source Folder

The **Local Source Folder** area provides the option to define a local source folder that is used to store updates. There are several reasons you might want to define and use this folder:

- You can manually download updates to this folder prior to publication. During publication, the updates are retrieved from the local folder rather than from the vendor websites, speeding the process.
- If you have a secure, isolated network, you can download your updates from a machine on a connected network and then move the updates to this folder after they are approved for use.
- You can create an archive of all your published updates.
• **Use a local source folder:** If enabled, indicates that a local folder will be the first place the program looks for the source file whenever you attempt to publish an update. If the binary file is located in the local source folder and the digest is verified, then that binary file will be added to the published CAB file. If the binary file is not contained in the local source folder or if the digest is not verified, then the update file will be downloaded from the web.

• **Always check this folder for software update content before attempting to download from the update URL:** Specify the full path name to the local folder or network share that will be used to store the update files.

There are several ways to manually download an update to the local source folder. You can select the update and then click the Download button in the toolbar, or you can right-click the update and choose Download to the Local Source folder. You can also use the Verify download button on the Binary File tab of the update editor. See How to Edit Updates for more details.

• **Place all updates downloaded during publication into the local source folder:** If enabled, indicates that during publication, any update that does not already reside in the local source folder will be copied to that folder. This enables you to create a complete archive of all your published updates.

**Offline Mode**

This area provides the option to run Ivanti Patch for SCCM in offline mode. To set offline mode, enable the Run disconnected check box.

When Ivanti Patch for SCCM is in offline mode, it means the console will not attempt to download newer catalog and update files. This mode is typically used by sites that require the use of fixed versions of data that have been approved for use. Offline mode is also useful if your security policy requires you to perform actions without downloading data files from the Web.

There are certain restrictions when operating in offline mode:

• You cannot download updates directly using the Download button or by right-clicking an update

• You cannot publish updates that have not been manually downloaded and moved to the Local Source folder

When in offline mode, you must download your catalog file(s) and your update binary files from an Internet-connected machine and then move the files to your console machine. A utility is available to help you with the download process. For information, see Using the File Downloader User’s Guide.
Languages Tab

Often, a single update may be applied to any language version of a product. Some updates, however, have a different update package for each language that the product supports. The Languages tab lets you choose which languages you are interested in for these language-specific updates. The languages you choose controls which language versions will be displayed in the Ivanti Patch grid.

- **All languages**: Ivanti Patch for SCCM will display all available language packages for each update.
- **Languages configured in WSUS**: Ivanti Patch for SCCM will only display packages for the languages that are currently configured for downloading on the WSUS server. This is the default option. (To review or change the WSUS language settings, start Update Services on the WSUS server, click on Options, then on Update Files and Languages, and select the Update Languages tab.)
- **Languages selected below**: Ivanti Patch for SCCM will only display packages for the languages that you select in the table. You must select at least one language.
  - **WSUS column**: Indicates if the language is currently configured on your WSUS server. You cannot modify any of the check boxes in this column.
  - **Display column**: Enable the check box for each language you want to be displayed in the Ivanti Patch grid. You can select a language even if it is not currently configured in WSUS.
Catalogs Tab

The Catalogs tab allows you to select which update catalogs should be used by the program. The Ivanti catalog, which is the primary catalog, will always be available. Catalogs from other vendors may also be provided by Ivanti and appear in this list. You can also add your own custom catalogs.

The Ivanti catalog does not need to be imported. To import a different catalog, select the name in the top pane and then click **Import/ Update Data**. The catalog will not be displayed within the program until you mark the catalog as active.

Any active catalogs that are provided by Ivanti will be automatically updated when new versions become available. Custom catalogs (those that you provide) are not automatically updated. To retrieve updates for a custom catalog, select it and then click **Import/ Update Data**.

- **Import / Update Data**: Select a catalog and then click this button to import the latest version of the catalog. The catalog will be downloaded from the URL shown in the middle pane. The catalog will be saved to the current user's **Ivanti Patch for SCCM** directory. When the import is complete the **Status** column will show **Up to date**. The catalog will not be shown in the user interface until you enable the **Active** check box.
Installation and Configuration

- **Delete Imported Data:** Deletes all data for the selected catalog. If you delete the imported data, you will need to re-import the data before publishing additional updates from this catalog.

  **Note:** You cannot delete data for the Ivanti catalog.

- **Add:** Use this button to add a new third-party catalog to the list in the top pane. In the User Updates Catalog dialog, you must provide a valid URL or URI path to the catalog file (usually a .cab or .zip file) as well as a name and a description for the catalog.

- **Edit:** Enables you to edit the URL, name and description of the selected catalog. You can only edit those custom catalogs that you have added; catalogs defined in the product manifest cannot be edited.

- **Remove:** Removes the selected catalog from the list in the top pane. You can only remove those custom catalogs that you have added; catalogs provided by Ivanti cannot be removed, but they can be deactivated and the data files can be deleted using **Delete Imported Data.**

**Metadata Options**

- **Prompt me when metadata revisions are available:** If new metadata becomes available for updates that you have previously published, a dialog will be displayed that provides you with the option to either immediately revise the updates in WSUS or ignore the new metadata. For example:

  ![Publish Revisions dialog](image)

  Ivanti Patch for SCCM will look for metadata revisions whenever a new copy of the catalog is downloaded. The recommended course of action in most cases is to publish the revisions.

  If you enable the **Remember my choice and do not prompt again** check box and then click **Yes**, the metadata option on the Account tab will change to **Update WSUS metadata without prompting me.**

  If you enable the **Remember my choice and do not prompt again** check box and then click **No**, the metadata option on the Account tab will change to **Do not prompt me and do not update WSUS.**

- **Update WSUS metadata without prompting me:** Automatically updates your published updates with the revised metadata without notifying you.

- **Do not prompt me and do not update WSUS:** No action is taken when revised metadata is available. You can use the *Revised metadata* filter to determine when metadata revisions are available.
Verify Setup Tab

This tab is used to launch the Configuration Checker. This utility is typically run once immediately after Ivanti Patch for SCCM is first installed.

Configuration Checker is used to determine if you meet all the requirements for using Ivanti Patch for SCCM. You can run Configuration Checker by clicking the Launch Configuration Checker button on the Verify Setup tab. You can also run it from the command line: C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\bin\ST.SCCM.ConfigurationChecker.exe. You must run Configuration Checker with full Administrator privileges, but you can use it to evaluate accounts that do not have full Administrator privileges.

Most of the information on this dialog will be pre-populated for you but it can be modified as necessary.

- **WSUS Server FQDN:** Type the fully qualified domain name of your WSUS server.
- **Port:** Select the port used to access the WSUS server.
- **User account (domain/user):** Type the domain and user name of the account that you want to evaluate.
- **Account password:** Type the password associated with the user account. This field can be left blank if you are evaluating the account that you are using to run this tool.
- **Use proxy:** If enabled, indicates that proxy server credentials are required in order to run the Configuration Checker test. If you clear the check box after specifying credentials, the credentials will be saved but not used. This box will initially mirror what is configured on the Proxy tab but can be temporarily overridden here.
- **Proxy user name:** Type the user name for an account on the proxy server. This box will be automatically populated with the user name provided on the Proxy tab but it can be overridden. It may be necessary to specify a domain as part of your user name (for example: mydomain\my.name).
- **Proxy password:** Type the password for the proxy server account.
Installation and Configuration

The utility checks for the following:

- Ability to connect to the WSUS server using a fully qualified domain name and port number
- Ability to connect to Protect Cloud using a user name and password
- Ability to retrieve the Ivanti catalog
- User account has **Log on as a batch job** privileges
- User account is a member of the **Administrators** group and the **WSUS Administrators** group on the WSUS server
- WSUS signing certificate is contained in the Trusted Root and Trusted Publisher stores and is current (not expired)

If any of the tests fail, you should correct the issue before using Ivanti Patch for SCCM.

**About Tab**

The **About** tab displays product and catalog version information, and it provides notification if the version in use is reaching its end of life. It is the last tab displayed by the setup wizard. To save your settings and exit the wizard, click **Finish**.

**Schedule Tab**

The **Schedule** tab is not available until after you have completed the setup wizard and saved your settings. The tab is used to publish updates using a recurring scheduled task. For more information on this tab, see the section titled **Automatically Publishing Updates Using a Recurring Scheduled Task**.
Preparing to Use Ivanti Patch for SCCM

What Gets Added to Configuration Manager

Installing the Ivanti Patch for SCCM add-in will add two new list items to the **Software Library > Software Updates** folder. It will also add a number of toolbar buttons to the Configuration Manager Home tab when either of the two new list items are selected.

- **Ivanti Patch**: Contains all the updates available in the active catalogs. You will use this list to locate and publish updates. Filters can be used to limit which updates are displayed; see [Using the Filters](#) for more information.

![Screenshot of Ivanti Patch for SCCM](image-url)
Preparing to Use Ivanti Patch for SCCM

- **Published Third-Party Updates:** Contains all the third-party updates that have been published to WSUS. The updates may have been published using Ivanti Patch for SCCM or by another mechanism. You will use this list to review and manage the updates.

![Screenshot of Ivanti Patch for SCCM interface]

**Toolbar Buttons**

Several toolbar buttons are available on the **Home** tab when **Ivanti Patch** or **Published Third-Party Updates** is selected.

- **Available from both Ivanti Patch and Published Third-Party Updates:**
  - **Synchronize Software Updates:** Used to initiate a site-wide synchronization of software updates. This option is also available by right-clicking the **Ivanti Patch** or the **Published Third-Party Updates** list item.
  - **Edit:** Used to modify an individual update’s metadata and to create and attach custom install scripts to the update. This option is also available by right-clicking an update in the **Ivanti Patch** or the **Published Third-Party Updates** list.
  - **Settings:** Used to modify your Ivanti Patch for SCCM settings or schedule a recurring publication task. This option is also available by right-clicking the **Ivanti Patch** or the **Published Third-Party Updates** list item.
### Used to view and modify which third-party vendors and product categories are being synchronized with the WSUS server. This option is also available by right-clicking the **Ivanti Patch** or the **Published Third-Party Updates** list item.

### Used to access the user documentation and training videos that are available on the Ivanti website. This option is also available by right-clicking the **Ivanti Patch** or the **Published Third-Party Updates** list item.

- **Also available when **Ivanti Patch** is selected:**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="download-icon" alt="Download" /></td>
<td>Used to download the selected update(s) to the folder specified on the <strong>Local Source</strong> tab of the <strong>Settings</strong> dialog. This button is unavailable if you have not specified a local source folder. You can also perform a download by right-clicking an update in the <strong>Ivanti Patch</strong> list.</td>
</tr>
<tr>
<td><img src="publish-icon" alt="Publish" /></td>
<td>Used to manually publish one or more third-party updates.</td>
</tr>
<tr>
<td><img src="unselect-all-icon" alt="Unselect All" /></td>
<td>Used to unselect all updates that are currently selected in the Ivanti Patch grid. This option is also available by right-clicking an update in the <strong>Ivanti Patch</strong> list.</td>
</tr>
<tr>
<td><img src="catalogs-icon" alt="Catalogs" /></td>
<td>Used to choose which of your <strong>active update catalogs</strong> will be displayed within the grid.</td>
</tr>
</tbody>
</table>

- **Also available when **Published Third-Party Updates** is selected:**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="expire-icon" alt="Expire" /></td>
<td>Used to expire third-party updates.</td>
</tr>
<tr>
<td><img src="re-publish-icon" alt="Republish" /></td>
<td>Used to publish updates that were previously published. For example, you might publish the full-content version of an update that was previously published as metadata-only. This will always publish the unedited version of the update that is in the current catalog. This is also useful if you expire an update and you want to get it back.</td>
</tr>
<tr>
<td><img src="re-sign-icon" alt="Re-sign" /></td>
<td>Used to re-sign updates if your signing certificate has changed or has been renewed. See <strong>How to Re-Sign and Deploy Updates</strong> for more details.</td>
</tr>
<tr>
<td><img src="delete-icon" alt="Delete" /></td>
<td>Used to delete an update from all deployments, deployment packages, Software Update Groups, and WSUS. The update will be expired as part of the deletion process.</td>
</tr>
</tbody>
</table>
Understanding the Information in the Grid

The **Ivanti Patch** and the **Published Third-Party Updates** grids each consist of two panes. Each pane displays unique information and provides unique functionality.

- The top pane displays all of the updates for the selected list item. This pane contains a large number of columns that provide high level information about each update. You can also select the updates that you want to perform an action on.
- The bottom pane displays detailed information about the update that is selected in the top pane. This pane is not available if more than one update is selected in the top pane.

There are several ways to customize how information is displayed within the top pane of a grid. You can:

- Apply filters to search for specific updates.
- Reorder the columns by clicking and dragging the column headers to new locations. Only the **Selected** column cannot be moved.
- Click within a column header to sort the column in ascending or descending order.
- Right-click within a column header to resize the columns and choose which grid lines to show. You can also choose which columns to display within the grid.

The **Ivanti Patch** grid contains a number of unique columns that help you identify the status of each update.

- **Bundled count**: Indicates the number of updates contained within a bundle. The value will be blank if you select an update that is not part of a bundle.
- **Catalog**: Indicates which catalog the update is contained in.
- **Detectoid**: Indicates if the selected item is a detectoid. A detectoid is a piece of logic that determines if an update is installable.
- **Published**: Indicates if the update has been published to WSUS.

- **Published Revision**: This number is incremented each time a revision to that update is published. All published updates will have a number greater than zero.

- **Revised**: Indicates if the update is a revision to an update that was previously published. If so, the check box in the Selected column will be enabled. Publishing such an update will create a new revision and will increment the Published Revision number.

A revision update alters only the metadata and not the update package. A revision is posted to the Ivanti catalog whenever any of the following need updating:

- The detection logic that determines if a patch applies to a system and if it is already installed
- Any text related to the update

- **Languages**: Identifies the different language versions that are available for each update. You can limit which languages are displayed by using the Languages tab of the Ivanti Patch for SCCM Settings dialog. If the Languages column entry is blank it means that the update applies to all languages that the product supports.

- **Metadata Only**: Indicates if detection logic has been published for the update but not the actual software binaries used to install the update.

- **Is Superseded**: Indicates if the update has been superseded by another update. An update that has been superseded is not the most current update available. To view the supersedence chain for an update, select the update and the superseded information is displayed in the bottom pane. The default filter, *Latest not-published*, will not display any superseded updates that have not already been published. To view all updates, including superseded updates, select the filter named *All*.

For example:
Using the Filters

Information displayed in the **Ivanti Patch** list and the **Published Third-Party Updates** list can be filtered to search for specific updates. You can also use a filter when scheduling a recurring task. There are three types of filters:

- **Predefined Filters**
- **Custom Filters**
- **Composite Filters**

**Predefined Filters**

The predefined filters are identified by a leading asterisk. Predefined filters cannot be modified or deleted. The predefined filters include the following:

**Ivanti Patch List**

- ***All***: All updates are displayed.
- ***Bundles***: Only bundles are displayed.
- ***Detectoids***: Only detectoids are displayed.
- ***Latest not-Published***: Only those updates that are not superseded and that have not been published to WSUS are displayed. This is the default filter.
- ***Not-Published***: Only the updates that have not been published to WSUS are displayed.
- ***Published***: Only the updates that have been published to WSUS are displayed.
- ***Revised metadata***: Only those updates that have been published to WSUS and that have metadata revisions in the current catalog are displayed. Re-publishing these updates will update the metadata in WSUS.
- ***Selected***: Only the updates you select in the grid are displayed. You can use this filter to verify your selections before publishing updates to WSUS.

**Note:** For updates that have different packages for each language, there is an implicit language filter in place in the Ivanti Patch grid. The only updates displayed will be those that apply to all languages (where the **Languages** column is blank) and where **Languages** includes at least one of the languages selected on the **Settings** dialog.

**Published Third-Party Updates List**

- ***All***: All updates are displayed.
- ***Selected***: Only the updates you select in the grid are displayed.
Custom Filters

You can create your own custom filters. The SmartFilter tool enables you to specify exactly which updates are displayed. Each custom filter is comprised of one or more rules. You can define as many rules in a filter as needed.

To create a new filter:

1. Click the New SmartFilter icon ( ).

   The Smart Filter dialog is displayed.

2. Type a name for the filter.

3. Specify which rules in the filter must be matched.
   - **All**: Only those updates that match all the rules in the filter will be displayed
   - **Any**: Updates that match at least one rule in the filter will be displayed

4. Define one or more rules.

   To define a rule, select an option in each of the first two logic boxes and then type the criteria in the third box. To add another rule simply click Add rule.

   **Note**: If you define a rule that does not make sense (for example: “Bulletin is less than 3”) the rule will be ignored.

5. Click Save.

Example

Assume you want to see a list of all critical updates for Adobe Acrobat. You simply create the following filter:
Composite Filters

Ivanti Patch for SCCM provides the ability to define composite filters. A composite filter consists of two or more filters that are linked and that run in series. This advanced filtering feature enables you to repeatedly narrow or expand your search of the updates within a grid by automatically running two or more filters back-to-back. It enables you to perform searches that involve both or and and logic.

To create a new composite filter:

1. Click the New Composite Filter icon ( ).
   The Composite Filter dialog is displayed.

2. Type a name for the composite filter.
3. Choose a starting filter.
4. Add one or more levels of filtering.
   To define a level, choose an action (Add, Remove, or Filter again) and then the additional filter that you want to apply. To add another level, click Add filter.
5. Click Save.

Example

Assume you want to see a list of all critical updates for Adobe and Google products. You simply create the following composite filter:
Performing Actions on the Grid

Using the Search Tool

You can easily search for updates contained in the top pane. All searches are performed using the Search tool. To initiate a search you type the text you want to find and then press Enter or click the search icon ( ). Only those updates matching the search criteria are displayed; all other updates are hidden.

Tips for Using the Search Tool

- The Search tool works only on the information currently visible in the top pane. You can right-click on the column headers to add or remove columns to be searched.
- If a filter is applied, only updates matching both the search criteria and the filter criteria are displayed.
- All partial matches are displayed.
- The search is not case sensitive.
- The following operators are available:
  - & (and)
  - | (or)
  - ^ (not)
- The use of wildcards is not allowed.

Show XML

You can right-click any update in the top pane and show the XML that defines the update. You can show the XML as it appears in the Ivanti catalog or as it appears in its published state on WSUS (for updates that have been published). This is intended as a debug tool and is not something you will typically need to use.
Performing Actions on the Grid

Copy Contents

You can copy the content in the top and bottom panes to your computer's clipboard. You might do this in order to paste content into an email message, into a spreadsheet program, etc.

Copy contents in the top pane

<table>
<thead>
<tr>
<th>Selected</th>
<th>Bulletin</th>
<th>Severity</th>
<th>Title</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>7-Zip 9.20 x64</td>
<td>7-Zip</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7-Zip</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Show catalog XML</td>
<td>7-Zip</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Show published XML</td>
<td>7-Zip</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7-Zip</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7-Zip</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7-Zip</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7-Zip</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7-Zip</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7-Zip</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Adobe Systems, Inc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Download to the Local Source folder</td>
<td>Adobe Systems, Inc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Edit</td>
<td>Adobe Systems, Inc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Unselect all</td>
<td>Adobe Systems, Inc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Adobe AIR 3.8.0.870</td>
<td>Adobe Systems, Inc.</td>
</tr>
</tbody>
</table>

- **Copy visible columns**: For the selected updates, this will copy the column information currently displayed in the grid.
- **Copy all columns**: For the selected updates, this will copy all column information, including columns that are not currently being displayed in the grid.

Copy contents in the bottom pane

You have a variety of options.

- To copy all contents: Right-click the section header and then select **Copy**.
- To copy supersedence information: Right-click the **Supersedence** table and then select **Copy**.
- To copy selected rows: Use ctrl- or shift-click to select the desired rows, and then right-click and select **Copy**.

- To copy a URL: Right-click the URL and then select **Copy**. You can then paste the URL directly into a browser.
Download One or More Updates to the Local Source Folder

You can download selected updates to a local source folder. Downloading updates in advance will help speed the publication process. This feature is also useful if you need a way to manually download updates and then move them to a secure, isolated network. This option is only available if the **Use a local source folder** option is enabled on the **Ivanti Patch for SCCM Settings** dialog. For details about the local source folder, see the **Offline Options Tab**.

Edit Updates

You can edit many details about an update either before or after it is published. For details, see **How to Edit Updates**.

Unselect All Updates

Use this option to quickly unselect all updates that are currently selected in the Ivanti Patch grid.
How to Publish Updates

Manually Publishing Third-Party Updates

You can manually publish one or more third-party updates. The updates can be published immediately or be scheduled for publication at some point in the future. The Microsoft Task Scheduler is used to schedule the publication. The publication always runs as a separate task, but can be monitored while it is running.

1. Within the Configuration Manager Software Library workspace, expand the Software Updates folder and click on Ivanti Patch.
2. Enable the Selected check box for each update that you want to publish.
   The Selected check box will be disabled if the latest revision of the update has already been published or has recently been scheduled for publication.

   To locate the desired updates you can:
   • Use a filter
   • Use the Group by vendor check box
   • Sort the columns by clicking in the column headers
3. Click Publish.
   The Publish selected updates dialog is displayed.
4. Specify when and how you want to publish the update(s).
   - **Now**: The publishing process will begin as soon as you click **OK**.
   - **Once**: Schedule the publication process to occur at some time in the future.
   - **Run the publication task offline**: If enabled, the publication task will be run in offline mode. This means the console will not attempt to download the selected update files. In order for the publication to be successful, the update(s) must already reside in the **Local Source folder**.

     **Note**: This check box is automatically enabled if **Run disconnected** is enabled on the **Offline Options** tab.

   - **Publish metadata only**: If enabled, this will publish detection logic for the update but not the actual software update binaries. You might do this if you want to detect if an update is needed by your clients but ensure that the update cannot be installed. This is useful only in very specific scenarios and server configurations.

     If you edit an update that is published as metadata-only, the original update will be deleted and the edited update republished as metadata-only. This means the revision number for these updates will always be 1. An update that is published as metadata-only cannot be re-signed because there is no content to sign. An attempt to re-sign it will result in a warning message in the log file.
How to Publish Updates

- **Accept all metadata updates in the catalog**: If you want to automatically update WSUS with any metadata revisions that are available for updates that have been previously published, enable this check box.

- **Synchronize after publishing selected updates**: If you want Configuration Manager to automatically synchronize itself with the WSUS database as part of this task, enable this check box. This will cause an incremental synchronization to be performed. If you do not enable this check box, the published update(s) will not be available for deployment until your regularly scheduled synchronization process occurs. Synchronization can also be started by selecting the **Home** tab and then clicking **Synchronize Software Updates**.

- **Logged on user**: If enabled, specifies that you will use the credentials of the currently logged on user to add the publishing task to Microsoft Scheduler. The **User** box is automatically populated so you only need to type the account password.

- **Different user**: If enabled, specifies that you want to use a different user account when adding the publishing task to Microsoft Scheduler. For example, you might specify a service account whose password does not expire.

  The account must:
  - Have **Log on as a batch job** rights
  - Be a member of the WSUS Administrators group on the WSUS server
  - Be a member of the local administrators group on the WSUS Server if the WSUS Server is remote

  When specifying a different user, you must indicate if credentials are required to authenticate to a proxy server.

  - **Proxy authentication is required - use these credentials**: If enabled, indicates that proxy server credentials are required when using the user account. If you then choose **Same as above**, the user account credentials will be used as the proxy credentials. If you choose **Credentials below**, you can provide a separate set of proxy credentials.

    - **User name**: Type the user name for an account on the proxy server. It may be necessary to specify a domain as part of your user name (for example: mydomain\my.name).
    - **Password**: Type the password for the proxy server account.
    - **Verify password**: Retype the same password.

5. Click **OK**.

   A status message will indicate if the publication task was successfully scheduled.

6. During the publication process the **Published** column status will show **Scheduled**.

   You may need to click the refresh button ( ) to update the data in the grid.
7. (Optional) Use the Configuration Manager Trace Log Tool to open the AutoPublish.log file and monitor the publication process.

AutoPublish.log is written by all one-time or recurring scheduled jobs that publish to WSUS.

Here is an example of the AutoPublish.log file:

```
<table>
<thead>
<tr>
<th>Log Text</th>
<th>Component</th>
<th>Date/Time</th>
<th>Thread</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Adobe Acrobat XI 1.1.1</td>
<td>AutoPublish</td>
<td>02/07/2014 00:10:00</td>
<td>1 (Dx1)</td>
</tr>
<tr>
<td>Publishing Adobe Acrobat XI 1.1.1</td>
<td>AutoPublish</td>
<td>02/07/2014 00:10:00</td>
<td>1 (Dx1)</td>
</tr>
<tr>
<td>Successfully published Adobe Acrobat XI 1.1.1</td>
<td>AutoPublish</td>
<td>02/07/2014 00:10:00</td>
<td>1 (Dx1)</td>
</tr>
</tbody>
</table>
```

8. When the update is successfully published the **Published** column status will change to **Yes** the next time the grid is refreshed.

   Note that the check box in the **Selected** column will be disabled if the latest revision of an update has been published.

   You can sort the **Published** column to see the list of updates that have been published, or you can use the **Published** filter.
Automatically Publishing Updates Using a Recurring Scheduled Task

You can automatically publish updates on a recurring basis by creating a scheduled task. You can only have one scheduled recurring task at a given time.

1. Within the Configuration Manager **Software Library** workspace, expand the **Software Updates** folder and click on **Ivanti Patch**.
2. On the **Home** tab, click **Settings** (or right-click Ivanti Patch and click **Settings**).

The **Ivanti Patch for SCCM Settings** dialog is displayed.
3. On the Schedule tab, specify when the scheduled task should run and what action(s) should occur.

- **Schedule Download and/or Publication**: Specify when you want the recurring task to run.

- **Run the scheduled task offline**: If enabled, the scheduled publication task will be run in offline mode. This means the console will not attempt to download the selected update files. In order for the publication to be successful, the update(s) must already reside in the Local Source folder.

  **Note**: This check box is automatically enabled if Run disconnected is enabled on the Offline Options tab.

- **Publish the packages selected by this filter**: Enables you to specify which updates you want to publish on a recurring basis. You can choose either the predefined filter named *Latest not-published* or any of your custom filters.

  **Example 1**: To publish all updates that have not been previously published and that are not superseded, select the *Latest not-published* filter. This is an easy way to automatically publish new updates on a recurring basis.

  **Example 2**: Assume you have previously created a custom filter that identifies all unpublished critical updates for the products you use in your organization. Simply select that filter here to publish just those updates on a recurring basis.

  **Note**: If an update contains different packages for different languages, only the language versions specified on the Languages tab will be published.

- **Accept all metadata updates in the catalog**: If you want to automatically update WSUS with any metadata revisions that are available for updates that have been previously published, enable this check box.

- **Synchronize updates**: If you want Configuration Manager to automatically synchronize itself with the WSUS database as part of this task, enable this check box. This will cause an incremental synchronization to be performed. If you do not enable this check box, the published updates will not be available for deployment until your regularly scheduled synchronization process occurs. Synchronization can also be started by selecting the Home tab and then clicking Synchronize Software Updates.

- **Logged on user**: If enabled, specifies that you will use the credentials of the currently logged on user to add the publishing task to Microsoft Scheduler. The User box is automatically populated so you only need to type the account password.

- **Different user**: If enabled, specifies that you want to use a different user account when adding the publishing task to Microsoft Scheduler. For example, you might specify a service account whose password does not expire.

  The account must:
  
  o Have **Log on as a batch job** rights
  
  o Be a member of the WSUS Administrators group on the WSUS server
  
  o Be a member of the local administrators group on the WSUS Server if the WSUS Server is remote

  When specifying a different user, you must indicate if credentials are required to authenticate to a proxy server.
How to Publish Updates

- **Proxy authentication is required - use these credentials**: If enabled, indicates that proxy server credentials are required when using the user account. If you then choose **Same as above**, the user account credentials will be used as the proxy credentials. If you choose **Credentials below**, you can provide a separate set of proxy credentials.

- **User name**: Type the user name for an account on the proxy server. It may be necessary to specify a domain as part of your user name (for example: `mydomain\my.name`).

- **Password**: Type the password for the proxy server account.

- **Verify password**: Retype the same password.

4. (Optional) Use the Configuration Manager Trace Log Tool to open the AutoPublish.log file and monitor the publication process.

   The AutoPublish.log file is written by any one-time or recurring scheduled jobs that publish to WSUS.

   You can use the Auto-Publish feature of Ivanti Patch for SCCM in conjunction with Automatic Deployment rules in Configuration Manager to keep clients up to date with the latest third-party updates.

**Viewing and Managing Scheduled Publications**

You can use the Microsoft Task Scheduler to view and manage your scheduled publications. To access Ivanti Patch for SCCM scheduled tasks, select **Start > Administrator Tools > Task Scheduler > Task Scheduler Library > Ivanti Patch for SCCM**.

- One-time tasks can be run, deleted, disabled, or rescheduled using the Microsoft Task Scheduler.

  ![Task Scheduler](image)

- After a one-time publishing task completes, the task will continue to be displayed in the Microsoft Task Scheduler for one to two days.

- If you alter a recurring auto-publish schedule using the Ivanti Patch for SCCM **Settings** dialog, the task will be automatically rescheduled.

- If you clear the **Schedule download and / or publication** check box in the **Settings** dialog and click **OK**, the recurring task will be deleted from the Microsoft Task Scheduler.
Managing Products

Show Me!
To view a video tutorial on this topic, click the video icon on the left.

You use the **Manage Products** dialog for several purposes. You can:

- View and edit which third-party vendor and product categories are being synchronized with the WSUS server and are deployable
- Select the categories you want to be synchronized with Configuration Manager
- Initiate a synchronization with WSUS
- Delete product and vendor categories

To begin, click the **Manage Products** icon. Please see the following topics:

- **Vendor / Product Categories to Synchronize**
- **Delete Vendor / Product Categories**
- **Performing Actions on the Manage Products Dialog**

**Note:** The **Manage Products** dialog is similar to the **Products** tab on the **Software Update Point Component Properties** dialog in Configuration Manager, but it provides additional functionality.

**Vendor / Product Categories to Synchronize**

To view which third-party vendors and products have been published and which ones are currently being synchronized with WSUS, select the **Vendor / Product Categories to Synchronize** tab. This is an important tab to monitor and manage. A new category is created each time you publish an update for a new third-party product. You will need to approve each new vendor or product category if you want updates in that category to be synchronized.
You can subscribe or unsubscribe to any of the categories in the list.

- If a category is contained in the list it means an update for a product in that category has been published and a synchronization with WSUS has occurred.

- If a category check box is enabled it means that it will be synchronized with WSUS. A product category will not be deployable until you have approved the category and performed a synchronization with Configuration Manager.

- If a category check box is clear (not checked) it means it is not being synchronized with WSUS and the product category is not deployable.

- If a category is displayed in red, it means an update for a product in that category has been published since the last synchronization with WSUS. Categories in red are unavailable for selection until either a background Configuration Manager task detects the change (this typically occurs once an hour) or a synchronization with WSUS is performed.

To change which categories in the list are being synchronized with WSUS, enable or clear the desired check boxes and then click **Apply Changes**. A confirmation dialog will be displayed to let you know that the change has been made, and it will give you the option to start a synchronization with WSUS. You will not be able to deploy published updates for newly selected categories until a synchronization occurs.
Delete Vendor / Product Categories

To delete one or more categories from the list, select the Delete Vendor / Product Categories tab. It is a good idea to delete a category when you no longer support a product in your environment, or when the updates in a category no longer apply to the product versions you support. By default, none of the check boxes on this tab are enabled.

Note: In order to delete categories, the user running Ivanti Patch for SCCM must be a full administrator with the security scope assigned to All instances of the objects that are related to the assigned security roles.

To delete a product or vendor category:

1. Enable the desired check box(es).
2. Click Delete Categories.
   A confirmation dialog is displayed.
   
   ![Confirmation Dialog]
   
   All updates associated with the selected vendors and/or products will be deleted from WSUS and from all deployments that they belong to. Do you want to continue?

3. To confirm the deletion, click Yes. To cancel the request, click No.

When you delete a product category, the following actions are performed:

- All published updates for that product are expired
- The updates are removed from all deployments and deployment packages in Configuration Manager
- The updates are removed from all Software Update Groups in Configuration Manager
- The updates are deleted from WSUS
Managing Products

If you delete all of the products for a vendor, the vendor category will also be deleted. The deletion operation is performed by a separate background process that begins immediately. The operation will continue even if you close Ivanti Patch for SCCM. The updates will be removed from the Published Third-Party Updates list as soon as they are deleted. You can monitor the progress of the operation by using the Configuration Manager Trace Log Tool to open the AutoPublish.log file.

The new state of the updates will not appear in the All Software Updates list in SCCM until the next synchronization is performed. After a synchronization, the updates will show as expired and are no longer deployable. The updates will remain in the All Software Updates list for several days until a background SCCM task removes them.

Note: To get a deleted product category to reappear in the Manage Products dialog, you must publish one or more updates for that product. See How to Publish Updates.

Performing Actions on the Manage Products Dialog

You can use the buttons located at the bottom of the dialog to perform the following actions.

- **Start synchronization:** Initiates a synchronization with WSUS. An incremental synchronization will be performed if no changes were made to the categories to be synchronized. If you have made changes to the category selections, Configuration Manager will automatically turn this into a full synchronization. Be careful if this is done during peak hours, as this can be an expensive operation if you have many published updates.

  This button is the same as clicking the Synchronize Software Updates button on the toolbar. The advantage of starting the synchronization here is that status of the synchronization is displayed as long as the dialog remains open. You can leave the dialog open and continue to use Configuration Manager. To bring the dialog to the top, click on the Ivanti icon in the task bar or click on the Manage Products button in the toolbar.

  Initiating a synchronization is also one way to make new product categories selectable. New categories are displayed in red in the category list and are unavailable for selection until either a synchronization occurs or a background Configuration Manager task detects the change.

- **Refresh:** Refreshes the information in the dialog.

- **Close:** Closes the dialog.
Expiring Third-Party Updates

You can expire third-party updates that have been invalidated by the product vendor or that have been superseded by other updates. Expired software updates cannot be deployed. The updates you set as expired can then be deleted using the WSUS cleanup tool.

To expire an update

1. Within the Configuration Manager Software Library workspace, expand the Software Updates folder and click on Published Third-Party Updates.
2. Select the updates that you want to expire.
3. Click Expire.

To view expired updates

- Within the Published Third-Party Updates list, sort the list using the Expired column. Note that the check boxes in the Selected column will be disabled. For example:

- Within the All Software Updates list, after a synchronization occurs, expired updates are represented by the expired icon ( ). For example:
How to Edit Updates

Ivanti Patch for SCCM provides the ability to edit an individual update. It allows advanced users to modify an update’s metadata and to specify pre-installation and post-installation commands. You can edit an update before or after it is published.

**WARNING!** Editing an update can be risky and the edit tool is not for everyone. Only qualified administrators should attempt to modify an update.

There are two distinct types of modifications that can be made to an update:

- **Modifications to the update’s metadata only**: Changes made on any of the editor’s tabs except the **Custom Install Script** tab will modify only an update’s metadata. Modifying the metadata does not create a new installation file or a new update ID. After making your changes, if the update was previously published, a revision will be published to the WSUS server. If you have previously deployed the update, it is not necessary to alter the deployments after editing the metadata. The client machines that have not installed the update will receive the updated metadata.

- **Modifications to the installation file**: Any changes made on the **Custom Install Script** tab will result in a new update being generated that supersedes the update being edited. After the new update is published, you will need to deploy it in order for your clients to get the changes.

Updates can be edited from either the **Ivanti Patch** list item or the **Published Third-Party Updates** list item.

- Updates in the **Ivanti Patch** list may or may not have already been published. When accessing an update from this location, the starting point for the update will always be the current catalog update. If an update has been edited with metadata changes only and published, you will be notified and those edits will not appear in the editor.

- When using the editor to open an update in the **Published Third-Party Updates** list, any previous edits you may have applied will be available.

- If you attempt to edit an update that has been superseded by another published updated (for example, one created by publishing the update with custom scripts), you will only be able to edit that update’s metadata. The controls on the **Custom Install Script** tab will be disabled.

To access the update editor: Select the individual update that you want to modify and then either click the **Edit** button in the toolbar or right-click the update and choose **Edit**.
Editing Tips

With the update editor you can:

- Edit an update’s information. For example, you can change an update’s title, description, severity, etc.
- Add command line options when relevant.
- Edit the Is Installed and the Is Installable rules.
- Change which CPU architectures and operating system languages will be patched.
- Edit the list of superseded updates.
- Add pre-install and post-install commands. These commands can invoke other scripts, command files, or executables that you provide and which will become part of the update.

The editor does not allow you to:

- Create completely new updates
- Replace the original binary update
- Modify the vendor, product, bulletin, KB article, CVE IDs, or JAVA IDs
- Make arbitrary changes to the software distribution package XML

Identifying Edited Updates

When you publish an edited update, the title and description of the update are automatically altered to indicate that changes were made. If only the metadata is changed, the term (Edited) is appended to the title. If a custom install script was added, the term (Custom) is appended to the title. In either case the following items are appended to the description: (Edited) <timestamp> <user name of editor>.

Saving Your Work

You can save your work at any point in the editing process. Periodically saving your changes is considered a good practice. You should save your work if you need to exit the update editor before finishing your edits or if you want to perform a review before publishing the changes.

To save your changes, click the Save icon ( ) and then specify a file name and a location to save the edited file. Your changes are reviewed by the program and checked for errors. You will not be able to save the file if any errors are found.

If you have exited the editor and want to retrieve your changes, select the correct update, restart the editor and then click the Open icon ( ). Locate the correct saved file, click Open and the edited version of the update will be loaded into the editor. An error will occur if you accidentally attempt to load an edited version of a different update.
How to Edit Updates

Editing the Binary File Information

The **Binary File** tab enables you to view information about the update binary file, to verify your ability to download the update, and to define command-line switches and return codes.

- **Static binary file information**: Displays information about the binary file that cannot be changed.
- **Verify download**: Downloads the update from the specified URL to a temporary location and verifies that the digest in the update matches the digest in the metadata. If the digest is approved and a local source folder is specified on the **Local Source** tab of the **Settings** dialog, the update will also be copied to that location and will not need to be downloaded again when the update is published. When the process is complete the file is deleted from its temporary location.
- **Command line**: Specifies command-line switches to use when the update is installed. For example, you might add switches that disable auto-update, that direct the update not to install the desktop shortcut, etc.
  
  **Note**: Certain updates will show setup.bat as the command line and none of the fields on this tab will be editable. This occurs if an update in the Ivanti catalog requires special non-standard installation procedures or if an update has been previously edited to include a custom install script. For these updates, it is not possible to alter the command-line options.
- **Success return codes**: Specifies the integer codes that the update returns if it is successfully installed and does not require a restart. This box is not displayed for .msi or .msp updates.
- **Success pending reboot return codes**: Specifies the integer codes that the update returns if it is successfully installed but requires a restart. This box is not displayed for .msi or .msp updates.
Editing the Localized Description

The Localized Description tab enables you to view and modify the title and description text that is provided for each update. You can provide unique text for any of the supported languages.

- **Language**: Enables you to choose which language you want to view and modify. The updates in the Ivanti catalog generally only provide English titles and descriptions. If you have users running non-English versions of an operating system, you may wish to provide text in other languages.

- **Clear**: Removes all text from the **Title** and **Description** boxes for the selected language.

- **Undo**: Restores the original text for the selected language. If you switch to a different language you will no longer be able to revert changes made to other languages.

- **Title**: Shows the text currently being used as the title for the update. When you publish the update the term *(Edited)* or *(Custom)* is appended to the title.

- **Description**: Shows the text currently being used to describe this update. When you publish the update the following items are appended to the description: *(Edited)* <timestamp> <user name of editor>.
How to Edit Updates

**Editing Information**

The **Information** tab enables you to view and modify general information about the update.

- **Static update information:** Displays general information about the update that cannot be changed.
- **More information URL:** Specifies a URL you can go to that contains additional information about the update. This is a required field and must contain a valid URL.
- **Support URL:** Specifies the URL address to use if you need assistance with this update. This is not a required field, but if a URL is specified it must use a valid URL syntax.
- **Severity:** Enables you to assign one of five severity levels based on the perceived threat of the vulnerability related to the update.
- **Impact:** This field has no effect on how the update is detected or installed; it is for information purposes only.
- **Reboot behavior:** This field has no effect on how the update is detected or installed; it is for information purposes only.
Editing Prerequisites

The **Prerequisites** tab enables you to specify requirements that must be met in order for an update to be considered installable.

- **Available detectoids**: A detectoid is a rule or prerequisite that determines if an update is installable. Multiple detectoids can be defined for an individual update. This list shows the detectoids that are available for selection. There are two types of detectoids: **CPU architecture** detectoids specify the computer architecture that is required, and **OS Language** detectoids specify the operating system language that is required on the target machine.

  You can use the search box to quickly locate a specific detectoid in this list.

**Tip**: When defining your prerequisites, first use the **Add Group** button to create your prerequisite groups and then use the **Add Prerequisite** button to add additional prerequisites to those groups.

- **Add Prerequisite**: Adds the selected detectoid(s) to the **Prerequisites** list. The detectoid(s) will be added to the group that is currently selected in the **Prerequisites** list. If there are no existing groups, the detectoid(s) will added as a new group.
- **Remove Prerequisite**: Removes the detectoid selected in the **Prerequisites** list.
- **Add Group**: Adds the selected detectoid(s) as a new group in the **Prerequisites** list. Use the **Add Prerequisite** button to add additional detectoids to a group. In order for the prerequisites to be met, at least one of the detectoids in each group must be satisfied.
- **Remove Group**: Removes the group selected in the **Prerequisites** list.
How to Edit Updates

Editing Superseded Updates

The Superseded Updates tab enables you to specify which updates are superseded by this update. An update that has been superseded is not the most current update available.

**Tip:** To view the complete supersedence chain for an update, select the update in the Ivanti Patch grid and the superseded information is displayed in the bottom pane.

- **Available software updates:** This list shows all updates in the Ivanti catalog that are available from the vendor of the update that is being edited. In addition, the list will contain custom updates for that vendor that were previously created using the update editor.

  You can use the search box to quickly locate a specific update in this list.

- **Add Selected Updates:** To add a superseded update, select the desired update in the Available software updates list and then click Add Selected Updates.

- **Remove Selected Updates:** To remove updates, select them in the superseded list and then click this button.

Editing Installable Rules and Installed Rules

The Installable Rules and the Installed Rules tabs allow you to edit the rules used to determine if an update is applicable to a target machine and if an update is currently installed on a target machine. The rules can be edited for MSI and EXE updates but not for MSP updates. Both tabs contain the same editing tools.
How to Edit Updates

- **Copy all to clipboard ( )**: Copies the existing rules to your computer’s clipboard. This enables you to use a more powerful external XML editor if you prefer.

- **Replace all from clipboard ( )**: Replace the existing rules with the rules contained on your computer’s clipboard.

- **Check for well-formed XML ( )**: Enables you to check periodically for well-formed XML as you develop your rules. You will not be allowed to leave this tab if the rules contain poorly-formed XML. A check will always be done whenever you attempt to leave this tab.

- **Word wrap**: Toggles word wrap on and off.

- **Font and font size**: Enables you to change the font and font size used to display the rules.

- **Line and Column**: Displays the current location of your cursor. This is useful if you need to find a line and column location that is displayed in an error message.

## Custom Installation Scripts

The **Custom Installation Script** tab enables you to insert Windows batch file commands directly into the installation script. The commands can be executed before or after the update is installed. If any files are required in order to execute your custom commands, they can be added to the update package.

For example, you could use this feature if you want to stop and restart services, remove conflicting software, or perform custom logging.

### Pre-Install Script and Post-Install Script Tabs

You can define custom batch commands that will be executed before or after the update is installed. The process is the same for both tabs.
How to Edit Updates

You can define the batch file commands by typing them in the space provided, or you can use the 
icons to copy and paste commands to and from your computer’s clipboard.

The following environment variables are available for use in the commands:

- `%PATHTOFIXES%` : Contains the full path to the current folder, with a trailing backslash.
- `%LSFN%` : The Language-Specific File Name variable provides a reference to the update file name and extension; the full path to the file is not included.

Custom Files Tab

The **Custom Files** tab is used to specify the location of any files required by your custom scripts. Files specified here will be added to the published package and will be written to the working directory of the target machines when the patch is installed.

To add a required file, specify the full path to the file and then click **Add**. You can also click **Browse** to locate the file.

Each file you specify must be located in a folder or share that is accessible to the account that is used to publish the update.
Tips for Debugging Custom Scripts

Add Tracing

If you run into problems while testing a custom installation script, you might consider inserting tracing steps into various points of your script. One possibility is to use echo commands to write out tracing messages to a text file. For example:

```bash
@echo beginning pre-install script >>.	race.txt
.
<your script commands>
.
@echo exiting pre-install script >>.	race.txt
@echo beginning post-install script >>.	race.txt
.
<your script commands>
.
@echo exiting post-install script >>.	race.txt
```

In this example the trace messages are written to the trace.txt file during the installation of the custom update. You can review the text file to pinpoint exactly where your custom script encountered an error. The file will be located in the installation sandbox folder on the target machine. See Review the Sandbox Folder for more information.

Review the Files Contained in the Sandbox Folder

A unique sandbox folder is created each time a custom update is installed. The sandbox folder is located on the target machine here:

```
%ProgramData%\Shavlik\Installation\InstallationSandbox#date/timestamp
```

Contained within a sandbox folder will be several files you might find useful for debugging purposes. This includes all the files that were published in the CAB file as well as any files you specified on the Custom Files tab.

The sandbox folders are only temporary and will be automatically removed after a number of days. For this reason, if there is a sandbox folder you would like to preserve you should copy it to a different location.

Finally, custom updates are not the only updates that use sandbox folders. Sandbox folders are also created for updates that require special handling so be careful to select the correct sandbox folder during your debugging process.

Testing Your Edits

You run the risk of introducing errors anytime you modify an update package. For this reason, you should always test your changes by publishing a modified update to your WSUS server and then deploying it to a set of test machines. You should never deploy a modified update to your production machines until it is fully tested.

If your test deployment fails and you need to perform additional editing, select the update in the Published Third-Party Updates list and then click Edit. Make your new edits and then click Publish. If your additional edits alter only the metadata, a revision will be published but the update ID will be unchanged. If you make new or additional edits to the Custom Install Script tab, a new update will be published that supersedes the update being edited.

If you publish multiple iterations of a custom script during your development and testing cycle, it could result in a sequence of superseded updates that will never be used. You should delete the
How to Edit Updates

intermediate updates after publishing the final version. To do this, in the Published Third-Party Updates list, select all but the final version of the custom updates that you created and then click Delete. This will delete all your intermediate customized versions and any related deployments that you performed during the testing process.

If you want to delete all of your edits and publish the original catalog version of the update, do the following:

1. If you created any custom updates using the Custom Install Script options, select those updates in the Published Third-Party Updates list and then click Delete.
2. If you published the unedited update, select it in the Published Third-Party Updates list and then click Republish. If you never published the original update but wish to publish it now, select and publish it from the Ivanti Patch list.

Publishing Your Edits

When you complete your edits, click Publish to begin publishing the update. If you want to save your changes without publishing them, click the Save icon ( ), save your changes to a file, and then click Cancel. All detectable errors must be fixed before saving your changes. To resume editing, select the same update, restart the editor, click the Open icon ( ) and then select your saved file.

Depending on the circumstances, you may be able to publish edited updates as either metadata-only or full-content, or you may be required to publish them as full-content. When you publish an update as metadata-only, a revision is created for the update and the detection logic for the update is provided, but the actual software update binaries are not included. When you publish an update as full-content, a new ID is applied to the update.

You can publish an edited update as either metadata-only or full-content if:

- You make only metadata edits to an update that has not been previously published
- All but the last tab (the Custom Install Script tab) on the update editor affect only the metadata.
- You make only metadata edits to an update that is published as metadata-only

You must publish an edited update as full-content if:

- You add or edit a custom install script
- If you made changes on the Custom Install Script tab, then the update package has been modified and it will need to be republished as full-content.
- You edit an update that has been published as full-content
- In the very rare case where you do want to publish an update as metadata-only when the update has already been published with full content, you need to edit the original catalog update and publish that as metadata-only. Note that in this situation, Configuration Manager may have a problem properly synchronizing the update.

When you publish an update from the update editor, your changes are reviewed and checked for errors. You will not be able to publish the update if any errors are found. If an error does occur, you will be notified and will have the opportunity to correct the error. If no errors are detected, the Publish selected updates dialog is displayed and you will follow the normal publishing process.

If you use the update editor to publish an update that has not been modified, then no changes are made and the normal publishing process is performed.
What are Bundles and Detectoids?

Bundles and detectoids are two different update types that are supported by Microsoft System Center. While not rare, they are not used within every update catalog. For example, they are not currently contained within the primary Ivanti catalog, but they may apply to certain third-party catalogs.

**Bundles**

A bundle is a collection of one or more updates. A bundle consists only of the metadata used to reference the updates that are included in the bundle. The bundle does not contain actual content or binary data.

A common use of a bundle is to group together related updates. For example, a bundle might contain all of the updates for the drivers that are associated with a particular machine type. To publish the updates for the machine type you simply publish the bundle, rather than locating and publishing each individual update. Another advantage of a bundle is that, when publishing, you only need approval for a single item (the bundle) rather than for each update contained in the bundle.

When you publish a bundle, Ivanti Patch for SCCM will publish all the updates in the bundle that have not already been published. Bundles can get quite large and may consist of dozens of different updates, so the publishing process is typically longer for a bundle.

For information on how to work with bundles in Ivanti Patch for SCCM, see *Working with Bundles*.

**Detectoids**

A detectoid is a unique form of an update. It does not contain a payload, but it does contain a single “Installed” rule that verifies a particular condition. Detectoids are used as prerequisite checks for other updates. For example, one detectoid might specify the operating system that is required to install an update on a target machine, and a second detectoid might specify the computer architecture that is required by the update. An update may have many prerequisites detectoids, and a detectoid may have other prerequisite detectoids.

If a detectoid is required in order to publish an update, Ivanti Patch for SCCM will publish the detectoid automatically. This is true for all update catalogs that contain detectoids.

For information on how to work with detectoids in Ivanti Patch for SCCM, see *Working with Detectoids*.

**Working with Bundles**

If you are working with an update catalog that contains bundles, here is what you need to know:

- To view unpublished bundles in the **Ivanti Patch** workspace, use the *Bundles filter*.
- To view the number of updates contained within a bundle, use the **Bundled count column** in the top pane.
- To view the list of updates that are contained within a bundle, in the lower pane, locate the **Updates in this bundle** line item and then click **Expand**.
Working with Bundles and Detectoids

- To publish a bundle, follow the same process used to publish an update.
  When you publish a bundle, the updates contained within the bundle will be published first and the bundle itself will be the last item to be published. If you publish all of the individual updates within a bundle, the bundle will still not be published; it must be published explicitly on its own.

- To view published bundles, in the Published Third-Party Updates workspace, select the bundle.
  The lower pane will show which updates are contained in the bundle.

- To delete a published bundle, in the Published Third-Party Updates workspace, select the bundle and then click Delete.
  You will be prompted to delete either just the bundle, or the bundle and all of the updates contained within the bundle.
  Deleting just the bundle deletes only the bundle, not the updates within the bundle. If you delete the bundle itself, however, you can then delete the individual updates as long as they are not contained within another bundle. If you choose to delete both the bundle and the updates within the bundle, the bundle will always be deleted first and then the specified updates will be deleted.
  You cannot delete an update from one bundle if it is contained in another bundle. If any updates in the bundle being deleted are contained in other bundles, they will not be deleted and this will be noted in the log file.

- To re-sign all of the updates in a bundle, in the Published Third-Party Updates workspace, select the bundle and then click Re-sign.
  Be sure to perform a synchronization with WSUS after the re-sign process is complete.

- To expire a bundle, in the Published Third-Party Updates workspace, select the bundle and then click Expire.
  You will be prompted to expire either just the bundle, or the bundle and all of the updates contained within the bundle.

- You cannot edit a bundle using Ivanti Patch for SCCM.
Working with Detectoids

You do not typically need to be concerned with detectoids in Ivanti Patch for SCCM. If an update requires detectoids, Ivanti Patch for SCCM will automatically publish those detectoids when you publish the update. By default, detectoids are not displayed in the Ivanti Patch for SCCM interface. If you are working with an update catalog that contains detectoids, you can view and publish them as follows:

- To view detectoids in the **Ivanti Patch** workspace, use the *Detectoids filter*. You can also create a custom filter that references the **Detectoid** column.
- To see if an update contained in the top pane is a detectoid, use the **Detectoid column**.
- To view detailed information about a detectoid, select the detectoid in the top pane and view its details in the lower pane.
- To publish a detectoid, follow the same process used to **publish an update**. There is nothing to download for a detectoid so the publication process is usually very quick.
- You cannot view published detectoids in the **Published Third-Party Updates** workspace.
  - To see which detectoids have been published, in the Ivanti Patch workspace, use the *Detectoids filter* and then view the **Published column**.
- You cannot edit, expire or delete a detectoid using Ivanti Patch for SCCM.
Support Information

Supported Products

For a complete list of the products supported by Ivanti Patch for SCCM, see:
http://community.shavlik.com/docs/DOC-2285

Technical Assistance

For technical assistance with Ivanti Patch for SCCM, please refer to one of the following support options:

- Browse the Ivanti Patch for SCCM section of the community page at: http://community.shavlik.com. You will need to become a member of the community in order to gain full access to all available resources.
- Open a support request at http://support.shavlik.com/CaseLogging.aspx
- Phone Technical Support at (866) 407-5279
- View online video tutorials at www.shavlik.com/support/training-videos/patch

End of Life Notification

If the version of Ivanti Patch for SCCM that you are using is nearing its end of life date, an Update Available message will be displayed when you start Ivanti Patch for SCCM. The message will indicate when the version will expire and it will provide a link to get the latest version. You should never allow your version of the product to reach its end of life date because the update catalog that contains the detection and deployment logic will stop being refreshed. A sample notification message is shown here:

![Update Available Message](image-url)
Appendix A: Creating and Distributing Certificates

Certificate Overview

A code signing certificate is required when using Ivanti Patch for SCCM with Configuration Manager and WSUS to publish third-party updates. In general, you must:

1. Create a code signing certificate.
   You can do this using either an internal Certificate Authority (CA) or your WSUS server.

2. (Conditional) If you use an internal CA to create the code signing certificate, you must import the certificate into WSUS, which you can do using Ivanti Patch for SCCM.
   If you use WSUS to create the code signing certificate, the certificate will be automatically imported into WSUS.

3. Export the certificate.

4. Distribute the code signing certificate to the appropriate certificate stores on all your WSUS servers, your remote SCCM consoles and to your client machines.
   • Trusted Publishers certificate store
   • Trusted Root Certificate Authorities certificate store

This appendix provides details on how to accomplish each of these tasks.

Reference

For detailed certificate information beyond that presented in this appendix, please see the following articles.

• For information on establishing a trust relationship to support third-party patching:

• For information on why WSUS in Windows Server 2012 R2 no longer by default supports generating code signing certificates, and for a workaround:

Note: Ivanti Patch for SCCM will automatically invoke this workaround if you choose to create a self-signed certificate using the Settings dialog.

Certificate Requirements

The minimum requirements of the signing certificate are:

• The private key must be exportable
• The key size must be 2048 or greater
• It must be a code-signing certificate
Appendix A: Creating and Distributing Certificates

Creating a Code Signing Certificate

**Note:** You can skip this section if you already have a code signing certificate.

You have two options for creating a code signing certificate:

- **Use a code signing certificate that is created using an internal CA**
- **Use the Ivanti Patch for SCCM user interface to have the WSUS create a self-signed code signing certificate**

Creating a Code Signing Certificate Using a CA

Creating a certificate from a trusted CA offers a couple of advantages:

- Distribution: Eliminates the need to distribute the certificate to other machines in the same domain.
- Management: Simplifies management because the certificate can be managed the same way as other certificates in your environment.

Follow your normal process for creating a certificate from your internal CA. After you have created the certificate you must write it to the WSUS server. You can do this using the Import Certificate feature in Ivanti Patch for SCCM. See the section titled Importing a Certificate for more details.

Using Ivanti Patch for SCCM and WSUS to Create a Code Signing Certificate

**Note:** Your user account must be a member of the WSUS Administrators group in order to create a code signing certificate through the Ivanti Patch for SCCM interface.

Using the Ivanti Patch for SCCM interface, you can instruct WSUS to create a self-signed code signing certificate for your enterprise. Creating a code signing certificate is enabled by default on WSUS prior to Windows Server 2012 R2.

**Important!** If you are using WSUS on Windows Server 2012 R2, the ability to create self-signed code signing certificates has been deprecated and is disabled by default. You can, however, restore this capability by using the workaround described in this article:


If you choose to create a code signing certificate in Ivanti Patch for SCCM using a Software Update Point (WSUS server) on Windows Server 2012 R2 or later, this workaround will be applied automatically.

To create a self-signed code signing certificate using WSUS:

1. Within the Configuration Manager **Software Library** workspace, expand the **Software Updates** folder and click on **Ivanti Patch**.
2. On the Configuration Manager **Home** tab, click **Settings**.
3. On the **Ivanti Patch for SCCM Settings** dialog, select the **WSUS Server** tab.
Note: Verify that the **Use Secure Sockets Layer (SSL) to connect to this server** check box is enabled. A secure connection to the WSUS server is typically required when creating a self-signed certificate.

4. Click **Create a self-signed certificate**.

   If a certificate already exists a **Warning** dialog is displayed.

   ![Warning Dialog]

   Do not proceed unless you are certain you need a different certificate. The warning message explains what you will need to do if you are replacing or deleting an existing certificate.

   If you click **OK**, a second **Warning** dialog is displayed.
Appendix A: Creating and Distributing Certificates

5. Read the information and then click **OK**.

The dialog shows the requirements that must be met before using the certificate.

The new certificate is created on the WSUS server and is registered with WSUS. Details of the certificate are displayed in the **Current Certificate** area. For example:
If you are running Configuration Manager with **Run as Administrator** privileges, the certificate is also automatically installed for you in the following certificate stores on the local Configuration Manager console:

- Trusted Root Certification Authorities
- Trusted Publishers

If the automatic installation fails you will have to manually distribute the certificate to the stores.
Appendix A: Creating and Distributing Certificates

Importing a Certificate

This section applies only if you created your code signing certificate using an internal CA. Importing the certificate will write the certificate to the WSUS Server and to the appropriate certificate stores on your machine. You do not need to use the import process if you used WSUS to create a code signing certificate, as that certificate was automatically written to the proper locations.

**Note:** In order to import a certificate you must have a secure (SSL) connection to the WSUS server. This is accomplished in part by enabling the Secure Connection check box in the WSUS Server area of the WSUS Server tab. You must also configure your ISS to use SSL.

To import a certificate:

1. Within the Configuration Manager Software Library workspace, expand the Software Updates folder and click on Ivanti Patch.
2. On the Configuration Manager Home tab, click Settings.
3. On the Ivanti Patch for SCCM Settings dialog, select the WSUS Server tab.
4. Click Import.
5. Navigate to the certificate file and click OK.

The certificate file will contain a copy of the private key and will be identified by a .PFX extension.
Exporting a Certificate

The export process is used to export the signing certificate to an accessible location on your network.

**Note:** The export process will only export the public certificate; the private key is NOT exported.

1. Within the Configuration Manager **Software Library** workspace, expand the **Software Updates** folder and click on **Ivanti Patch**.
2. On the Configuration Manager **Home** tab, click **Settings**.
3. On the **Ivanti Patch for SCCM Settings** dialog, select the **WSUS Server** tab.
4. Click **Export**.
5. Specify the location and file name and then click **Save**.

   The file is typically a .CER file.

After exporting the certificate, you will need to distribute it to any other WSUS servers and to your client machines. This is necessary in order for the machines to receive locally published updates.

The distribution process is described in the next section.

Distributing the Certificate

You must distribute the code-signing certificate to all servers that house your Configuration Manager and WSUS consoles and to all of your client machines. Which certificate store(s) the certificate is copied to depends on how the code-signing certificate was created.

- If your code signing certificate was created by WSUS (and is therefore a self-signed code signing certificate), you will need to copy the certificate to the following locations on all your WSUS servers, your remote SCCM consoles and your client machines:
  - Trusted Publishers certificate store
  - Trusted Root Certificate Authorities certificate store
- If the code-signing certificate was issued by a CA whose root is already trusted by your clients, you only need to copy the certificate to the Trusted Publishers certificate store on your WSUS and client machines.

Using Group Policy to Distribute the Certificate

Using MMC to Manually Distribute the Certificate

Another method for distributing the code-signing certificate is to use MMC. This is an easy method for distributing the certificate to a handful of local machines but might prove impractical for distributing the certificate to many machines spread across your organization.

1. On the target machine, start Microsoft Management Console (MMC).
2. In the Certificates store, right-click **Trusted Publishers** and select **All Tasks > Import**.
3. On the **Welcome to the Certificate Import Wizard** dialog, click **Next**.
4. On the **File to Import** dialog, browse for your public key file and then click **Next**.
5. On the **Certificate Store** dialog, choose **Place all certificates in the following store** and then click **Next**.
6. On the **Completing the Certificate Import Wizard dialog**, click **Finish**.

7. On the confirmation dialog click **OK**.

8. (Conditional) If you created your certificate using WSUS, repeat Steps 2 – 7, only this time select **Trusted Root Certification Authorities** in Step 2.
Appendix A: Creating and Distributing Certificates

Renewing an Expiring Signing Certificate

If your signing certificate is within 90 days of its expiration date, a warning dialog will be displayed. For example:

![Certificate Warning]

Although you are able to delay this warning for a number of days, do not let this task slide. If you let your signing certificate expire you will be unable to publish third-party updates.

How to Re-sign and Deploy Updates After Renewing a Certificate

After renewing your signing certificate, you must re-sign and then deploy or re-deploy your updates. How you do this depends on the current state of your updates.

Scenario 1: You have updates that were published with an old certificate but have not been deployed.

1. Re-sign the updates.
2. Perform a synchronization with WSUS.

Your updates are now ready to be deployed.

Scenario 2: You have updates that were published with an old certificate and they have been deployed.

In this scenario you need to modify each deployment package that contains a re-signed update. You must delete each update that was signed with the old certificate and replace each one with the newly signed updates.

1. Re-sign the updates.
2. Perform a synchronization with WSUS.
3. Delete the updates from the deployment package(s).
   a. Within the Configuration Manager Software Library workspace, expand the Software Updates folder and click on Deployment Packages.
   b. Double-click a deployment package that contains a re-signed update.
      This will open the deployment package.
c. Within the deployment package, right-click the updates you re-signed and then choose **Delete**.

d. At the confirmation prompt, clear the **Refresh Distribution Points** check box and then click **OK**.
   If you receive a warning indicating that deployments will fail, click **OK**.

e. Repeat Steps b – d for each deployment package that contains a re-signed update.

4. Download the newly signed updates and add them back to the deployment package(s).
   a. Select the **All Software Updates** folder.
   b. Right-click an update you just deleted and then choose **Download**.
      The **Download Software Updates Wizard** is displayed.
   c. Choose **Select a deployment package** and then specify the deployment package you deleted the update from in Step 3.
   d. Complete the download by clicking **Summary** and then **Next**.
   e. Repeat Steps b – d for each update that you deleted.

**Tip:** If the updates belong to a software update group you can download the group instead of the individual updates.

### Enabling Your Clients to Download Re-Signed Updates

You may have clients that have already downloaded one or more updates that were signed with the old certificate. In this situation you must clear the old updates from the clients' cache so that the newly-signed updates can be downloaded by the client.

1. On each client, use Control Panel to locate and open the **Configuration Manager Properties** dialog.
2. On the **Cache** tab, click **Configure Settings**.
3. Click **Delete Files**.
4. Enable the **Delete persisted cache contents** check box.
5. Click **Yes** and then **OK**.
Index

A
About tab 22
Add-in 5
Automatically publishing updates 38
AutoPublish.log file 34

B
Binary file information 48

C
Catalogs tab 19
Certificate authority 62
Certificates 61
  Code signing 62
  Creating 62
  Distributing 67
  Exporting 67
  Importing 66
  Reference 61
  Renewing 70
  Requirements 61
Code signing certificate info 10
Composite filters 30
Configuration Checker 21
Configuring your settings 9
Copy contents 32
Custom files tab 54
Custom filters 29
Custom scripts
  Custom files 54
  Debugging 55
  Pre-install and post-install scripts 53

D
Debugging custom scripts 55
Delete Vendor / Product Categories 43
Detectoid 51
Download re-signed updates 71
Download to Local Source folder 33

E
Editing updates 46
  Custom files 54
  Debugging custom scripts 55
  Editing binary file information 48
  Editing installable rules 52

F
Filters 28
  Composite filters 30
  Custom filters 29
  Predefined filters 28
FIPS 5

G
Grid information 26
Group policy 67

I
Installed and installable rules 52
Installing Ivanti Patch 7

L
Languages tab 18
License tab 12
Local Source folder 16
Localized update description 49

M
Managing products 41
Manually publishing updates 34
Metadata revisions 19
Microsoft Management Console (MMC) 68

O
Offline Options tab 16
## Index

<table>
<thead>
<tr>
<th>Letter</th>
<th>Pages</th>
</tr>
</thead>
</table>
| **P**  | Predefined filters 28  
|        | Pre-install and post-install scripts 53  
|        | Prerequisites for updates 51  
|        | Proxy tab 11  
|        | Published Third-Party Updates list item 23  
|        | Publishing updates 34  
|        |  
|        |  
|        |  
|        | Automatically publishing updates 38  
|        | Manually publishing updates 34  
|        | Scheduled publications 40  
|        |  
| **R**  | Renewing a certificate 70  
|        | Requirements for certificates 61  
| **S**  | Sandbox folder 55  
|        | Schedule tab 22  
|        | Scheduled publications 40  
|        | Search tool 31  
|        | Show XML 31  
|        | SmartFilter 29  
|        | Superseded updates 52  
|        | Support information 60  
|        |  
|        |  
|        | End of life notification 60  
|        | Supported products 60  
| **T**  | Task Scheduler 40  
|        | Technical assistance 60  
|        | Testing your edits 55  
|        | Toolbar buttons 24  
|        | Tracing 55  
|        | Trusted publisher 68  
| **U**  | Unselect all updates 33  
|        | Update catalog 5  
|        | Update information 50  
| **V**  | Vendor / Product Categories to Synchronize 41  
|        | Verify Setup tab 21  
| **W**  | Welcome 5  
|        | What is added to Configuration Manager 23  
|        | WSUS Server tab 10  

Technical assistance 60  
Synchronize 44  
System requirements 5  

End of life notification 60  

Supported products 60