Software Vulnerability Manager 2018 (Cloud Edition)

Quick Start Guide

Legal Information

Book Name: Software Vulnerability Manager 2018 (Cloud Edition) Quick Start Guide

Part Number: SVM-2018-QSG02

Product Release Date: November 2018

Copyright Notice

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see https://www.flexera.com/producer/company/about/intellectual-property/. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.

Contents

1

Software Vulnerability Manager 2018 (Cloud Edition) Quick Start Guide

Flexera's Software Vulnerability Manager 2018 is a Vulnerability and Patch Management Software Solution that facilitates a customized Patch Management process. It combines Vulnerability Intelligence, Vulnerability Scanning, and Patch Creation with Patch Deployment Tool Integration to enable targeted, reliable, and cost-efficient Patch Management.

Vulnerability and Patch Management are critical components of any security infrastructure because it enables proactive detection and remediation of vulnerabilities before they are actively exploited and your security compromised. With Software Vulnerability Manager 2018, IT Operations and Security Teams are empowered to prevent vulnerability threats from both Microsoft and non-Microsoft (third-party) product vulnerabilities, covering Microsoft Windows, Mac OS, and Red Hat Enterprise Linux.

Software Vulnerability Manager 2018 integrates seamlessly with Microsoft® WSUS and System Center Configuration Manager.

Table 1-1 • Software Vulnerability Manager 2018 (Cloud Edition) Quick Start Guide

Topic	Content
Getting Started	The following topics provide further information for getting started with Software Vulnerability Manager 2018: • System Requirements • Permissions • Software Vulnerability Manager 2018 with Scanning and Patching Capabilities • Download and Install the Software Vulnerability Manager 2018 Internet Explorer Plug-in • Download and Install the Software Vulnerability Manager 2018 Daemon • Download and Install the System Center Plug-in

Table 1-1 • Software Vulnerability Manager 2018 (Cloud Edition) Quick Start Guide (cont.)

Topic	Content
Scanning	This following topics describe the various Software Vulnerability Manager 2018 scanning methods: ● Remote Scanning Via Software Vulnerability Manager 2018 (Agent-less Scan) ● Quick Scan ● Scan Groups ● Scanning Via Local Agents ● System Center Inventory Import ● System Center Import Schedules (Requires the Software Vulnerability Manager 2018 Daemon)
Reporting	Software Vulnerability Manager 2018 includes a report function to document your scanning results. ● To configure your reports and to schedule your report generation, see Report Configuration. ● To create and configure reminders, notifications, and alerts for a Smart Group, see Smart Group Notifications.
Patching	The following topics describe how to configure and deploy Software Vulnerability Manager 2018's patching function. ● Patch Configuration ● Creating the WSUS-CSI GPO Manually ● Creating a Patch with the Flexera Software Package System (SPS) ● Deploying the Update Package Using WSUS ● Deploying the Update Package Using System Center
Appendix A - Certificates	This appendix describes the types of certificates to obtain to deploy patches and how to verify and validate the certificate. ● WSUS Self-Signed Certificate (Microsoft) ● Using Your Own Certification Authority (CA) Certificate ● CA Verification and Validation

Using Help

Help is available from the Software Vulnerability Manager 2018 (Cloud Edition) interface help icon located at the top right of the screen or click the fields labeled with a "(?)" to access the contextual help.

Online Help

For online help, see https://helpnet.flexerasoftware.com/csi/Default.htm

Release Notes

For the latest product release notes, see https://helpnet.flexerasoftware.com/?product=Software%20Vulnerability%20Manager%202018%20Cloud%20Edition&version=2018

For earlier product release notes, see https://helpnet.flexerasoftware.com/?product=Software%20Vulnerability%20Manager%202018%20Cloud%20Edition&version=Previous

Contact Us

Flexera is headquartered in Itasca, Illinois, and has offices worldwide. To contact us or to learn more about our products, visit our website at: https://www.flexera.com/

Product Feedback

Have a suggestion for how we can improve this product? Please come share direct feedback with the product team and vote on ideas submitted by other users in our online community at: Customer Community feedback page for Software Vulnerability Manager.

2

Getting Started

Flexera's Software Vulnerability Manager 2018 solution is accessible via https://csi7.secunia.com.

You will be prompted for authentication with your username/password. Please use the credentials supplied by Flexera personnel. The initial password issued by Flexera is a one-time only password that must be changed upon the first logon. The new password must contain a minimum of eight characters, or comply with the criteria defined in your custom Password Policy Configuration.

The following topics provide further information for getting started with Software Vulnerability Manager 2018:

- System Requirements
- Permissions
- Software Vulnerability Manager 2018 with Scanning and Patching Capabilities
- Download and Install the Software Vulnerability Manager 2018 Internet Explorer Plug-in
- Download and Install the Software Vulnerability Manager 2018 Daemon
- Download and Install the System Center Plug-in

System Requirements

To use the Software Vulnerability Manager 2018 console, your system should meet the following requirements:

- Minimum resolution: 1280x1024
- Internet Explorer 11 or higher (Scan results can also be viewed from other browsers)
- Internet connection capable of connecting to https://csi7.secunia.com
- The following addresses should be white-listed in the Firewall/Proxy configuration:
  - crl.verisign.net
  - crl.thawte.com
  - http://crl3.digicert.com

- http://crl4.digicert.com
- http://*.ws.symantec.com
- https://*.secunia.com/
- http://*.symcb.com
- http://*.symcd.com

- First-Party cookie settings at least to Prompt (in Internet Explorer)
- Allow session cookies
- A PDF reader

Permissions

- Connect and Select permissions to the user (or service account) at the SQL Server Host of your System Center database. See Download and Install the Software Vulnerability Manager 2018 Daemon.
- WSUS Administrator Group privileges (located locally on your WSUS Server)
- (Optional) Domain Administrator privileges for Group Policy Object creation - however the Group Policy Object can be created manually. This is a one-time configuration so the rights are not required on a permanent basis.

Software Vulnerability Manager 2018 with Scanning and Patching Capabilities

Task ***To successfully scan and create updates, the following should also be present when using Software Vulnerability Manager 2018:***

1. Internet Explorer 11 or higher with Software Vulnerability Manager 2018 Plug-in installed (in order for Software Vulnerability Manager 2018 to connect to WSUS and to create packages successfully, IE must be run as administrator in most cases. Right-click and select **Run as administrator**).
2. In IE **Tools > Internet options > Advanced**, ensure **Use TLS 1.1** and **Use TLS 1.2** are selected.
3. WSUS Administration Console matching your WSUS server's version.
4. Visual C++ Redistributable for Visual Studio 2012.
5. Microsoft .NET Framework runtime 4 or later.
6. If the WSUS Self-Signed Certificate is going to be used, and the user wishes to provision the certificate through the **Patching > WSUS/System Center > Deployment** function, Remote Registry service must be enabled on the clients.
7. Select the target hosts where the certificate is to be installed (CTRL+ mouse click for multiple selection). Right-click and select **Verify and Install Certificate**.

Task ***To successfully run patching on Windows 8.1 and Server 2012 R2:***

1. On the Windows Server machine, from the Server Manager, go to **Add Roles & Features > Features**.
2. Select the Appropriate Installation Type (Role-Based & Feature Based as opposed to Remote Desktop Services Installation).
3. Select the local server as the Destination Server for the installation.
4. Click **Next** to bypass the Server Roles menu and go to the Features menu.
5. Within the Features menu, scroll down the list and find the Remote Server Administration Tools (RSAT).
6. Expand the RSAT feature menu and locate the Role Administration Tools list of features.
7. Expand the list and find Windows Server Update Services Tools.
8. Enable this feature and all additional subfeatures listed underneath it (API and PowerShell cmdlets and User Interface Management Console).
9. Proceed to the end of the Add Roles and Features Wizard by clicking **Next** and then **Install**.
10. Restart Windows and launch Software Vulnerability Manager 2018 from a web browser (for example IE).

Download and Install the Software Vulnerability Manager 2018 Internet Explorer Plug-in

The first time you log on to Software Vulnerability Manager 2018, click the link on the bottom of the page and follow the on-screen instructions to download and install the Software Vulnerability Manager 2018 Plug-in to enable scanning and patching. Please note that the plug-in is only compatible with Internet Explorer version 11 or higher.

Software Vulnerability Manager 2018 Plug-in is installed locally and must be installed on the machine you are running the Software Vulnerability Manager 2018 console from. Once the Software Vulnerability Manager 2018 Plug-in has been installed, the download link is removed from the page.

If Internet Explorer is blocking the ActiveX Plug-in, follow the steps below to allow it to load:

- Open Internet Explorer's **Internet options**
- Go to the **Security** tab
- Select **Trusted Sites**
- Add your server's IP or hostname to the Trusted Sites
- Go back to the Security tab and click **Custom level**
- Scroll down to *Initialize and script ActiveX controls not marked as safe for scripting* and change the setting from Disable to **Prompt** or **Enable**

Download and Install the Software Vulnerability Manager 2018 Daemon

The Software Vulnerability Manager 2018 Daemon is a stand-alone executable that executes various schedules configured in the Software Vulnerability Manager 2018 console. It runs as a background service with no user interaction. You can download the Daemon from: https//secuniaresearch.flexerasoftware.com/support/download/

The Daemon integrates a number of local data sources in your network with the Flexera Cloud. It should be deployed to a node in the network that has high availability (for example, the server running the System Center or SQL server).

Once deployed, the Daemon will regularly scan the following data sources, based on the configuration created in Software Vulnerability Manager 2018:

- Active Directory
- Microsoft® System Center Configuration Manager ("System Center") Imports
- Scheduled Exports
- WSUS State Change

Important • *As the Daemon is connecting directly to the Flexera and System Center database servers unattended, Software Vulnerability Manager 2018's System Center Inventory Import page should be configured to include System Center SQL Host, SQL Port and SQL Database connection details prior to the installation of the Daemon to enable the latter to start executing unattended schedules correctly and on time.*

Important • *To pass authentication at the SQL server during an unattended scheduled Import, the Daemon has to be installed and configured with a user account that has been specifically assigned with Connect/Select permissions at the SQL Server Management Studio software prior to the installation of the Daemon.*

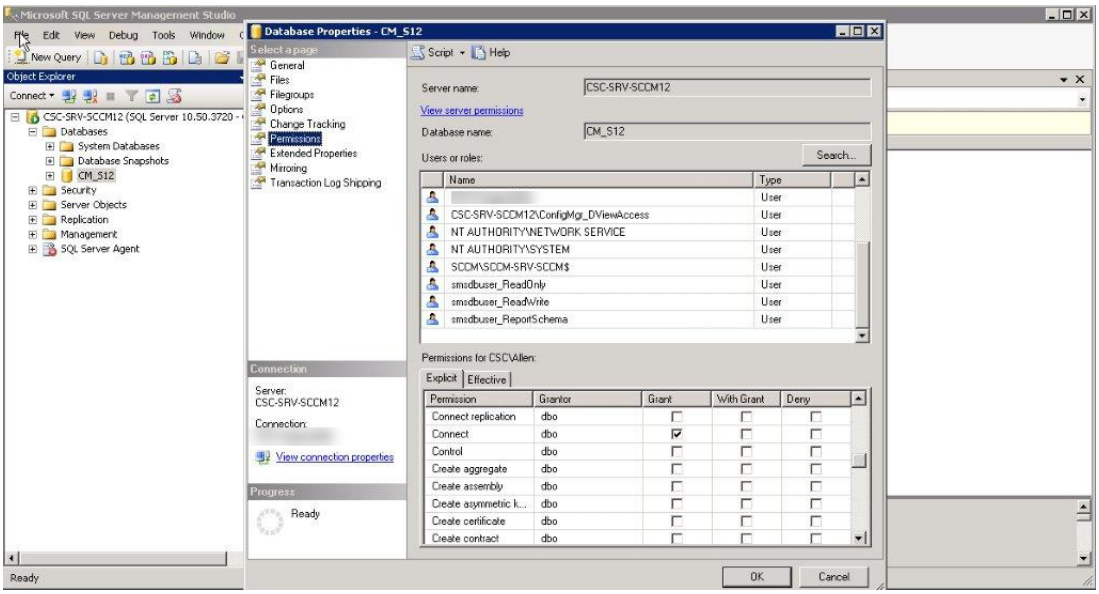
The Daemon should only be deployed once to avoid two instances competing to retrieve the schedules.

The user or service account that runs the Daemon must have:

- Run-as Service privileges
- Write permission on the location where the exports should be placed and a log file written for scheduled CSV file output and log file creation
- Membership to the local WSUS group "WSUS Administrators"
- LDAP query privileges
- SQL DataReader privileges
- System Center Configuration Manager Read only Analyst privileges

Task ***To assign Connect and Select permissions to the user (or service account) that will be used to run the Daemon service:***

1. Open the SQL Server Management Studio software at the SQL Server Host.
2. Expand the Databases and find the name of your System Center database.
3. Right-click the database name and select **Properties**.
4. Enter the Permissions section from the left-hand side menu.
5. Find the account that will be used to install the Daemon and click on it.
6. While highlighted, review the **Explicit** permissions of the account below and find and select the **Connect** and **Select** check boxes.
7. Save the configuration and exit the SQL Server Management Studio.



Task ***To install the Daemon:***

1. Double-click the Daemon installer icon and follow the wizard instructions.
2. Accept the End User License Agreement and click **Next**.
3. Enter the Daemon Proxy Settings (host name, port, user name and password), if required. The values in populated fields are fetched from the current user's Internet Explorer proxy settings. Click **Next**.
4. Enter the User Name and Password of your Software Vulnerability Manager 2018 account and click **Install**.

Important • *The Daemon executes scheduled tasks configured in Software Vulnerability Manager 2018. Therefore, the Software Vulnerability Manager 2018 user account used during the Daemon installation must be the same account which set up the scheduled tasks in Software Vulnerability Manager 2018. It can be a user account or an administrator account in Software Vulnerability Manager 2018.*

5. Enter the credentials for the user account (or service account) that was set up beforehand to grant access for the Daemon to the SQL Server Host. The user name must be entered in the <username>@<AD domain> format. Click **Next**.

6. Click **Finish** to close the Daemon setup.

For reference, the Daemon now outputs reports to a user-configured path. This path is set when the Daemon is installed, and there is a page in the installer to configure the path. The file created at that path gets the data and time appended to its name. For example, if the user sets the name to *all_hosts.csv* in Software Vulnerability Manager 2018, then the resulting file will actually be named *all_hosts_2016-03-03_13-00_01.csv*, or whatever the date and time were when the file was created.

Also note that from Daemon version 2.0.0.6 onwards, if the user leaves the path empty when installing the Daemon, then exporting reports will not work at all. To fix this later, the user will have to reinstall the Daemon and set the path in the installer.

The Daemon uses the System Center SQL Database Settings that are specified in the Configure dialog. If those settings have not been specified when the Daemon has been run, then the Daemon will check again for the settings in 10 minutes and every 10 minutes afterwards until the Daemon receives the settings.

The Daemon checks with Flexera every 10 minutes to download new schedules or fetch changes to existing schedules as long as it is not in the process of processing scans. The results are displayed in Software Vulnerability Manager 2018's Completed Scans page.

Log on with your Software Vulnerability Manager 2018 Account credentials (User name/Password).

The machine should have access to https://*.secunia.com.

Download and Install the System Center Plug-in

The System Center Plug-in should be installed on the same machine that the System Center Configuration Manager console is installed. You can use the Plug-in on the System Center Configuration Manager Server or on a client machine where the console is installed.

Download the installer from https://secuniaresearch.flexerasoftware.com/support/download/.

Double-click the installer icon and follow the wizard instructions.

Launch the System Center console. The Plug-in can be found under the **Software Library > Flexera Software** folder.

Tip *• You can define the sorting of both lines and columns in any grid view to create the layout that best suits your needs. Click the right-hand side of any of the column headings to view the available display options. The column's position can be modified by dragging and dropping the selected column to the desired position.*

Tip *• You can click* ***Export*** *in any grid view to save the displayed information as a CSV file. You can configure the file by hiding columns in the grids prior to export.*

3

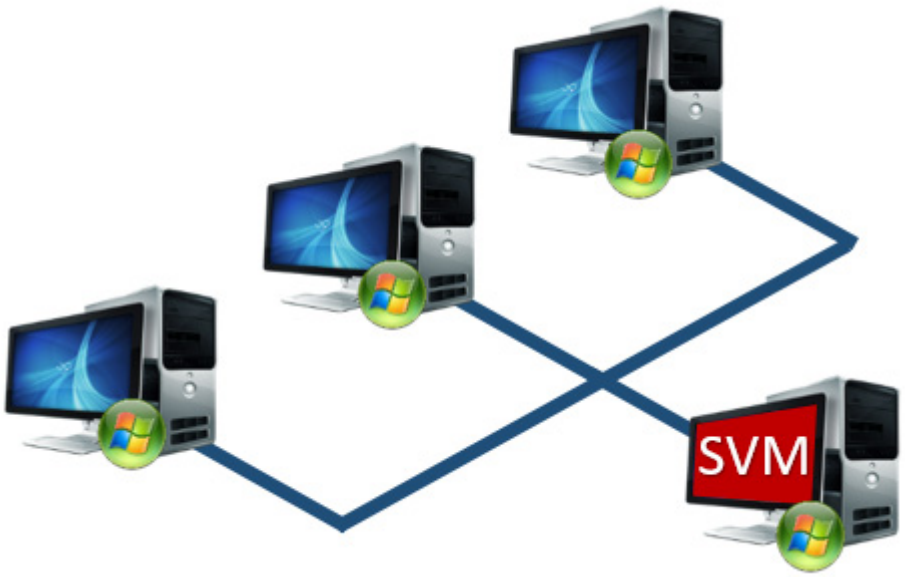
Scanning

This following topics describe the various Software Vulnerability Manager 2018 scanning methods:

- Remote Scanning Via Software Vulnerability Manager 2018 (Agent-less Scan)
- Quick Scan
- Scan Groups
- Scanning Via Local Agents
- System Center Inventory Import
- System Center Import Schedules (Requires the Software Vulnerability Manager 2018 Daemon)

Remote Scanning Via Software Vulnerability Manager 2018 (Agent-less Scan)

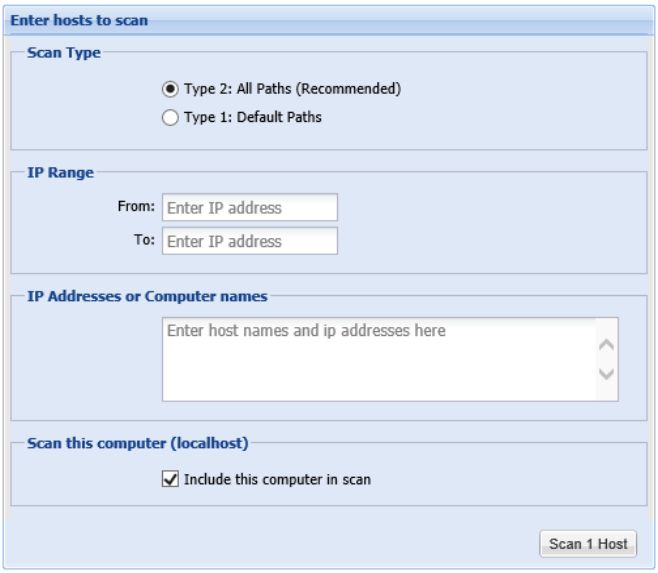
These scans are performed in an Agent-less manner, and the credentials used by Software Vulnerability Manager 2018 to authenticate on the target hosts are the same as those of the user that launched the Software Vulnerability Manager 2018 console.



Important • *Please consider the system requirements for the Scan Groups/Agent-less scans, described in Agent-based Scan Requirements (Windows).*

Quick Scan

Use this page to conduct quick, on-demand, scans from your Software Vulnerability Manager 2018 console against remote hosts on your network or your local PC. Enter the scan type and IP address range for the hosts you wish to scan in the **Enter hosts to scan** screen and click **Scan Hosts**.

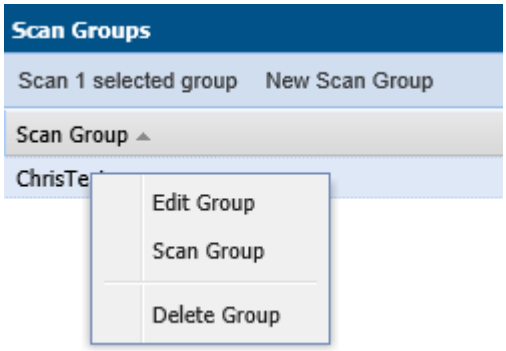


So that you are able to remote scan the target host, please ensure that all the system requirements for the remote scan are in place.

The progress can be seen under **Scan Progress**.

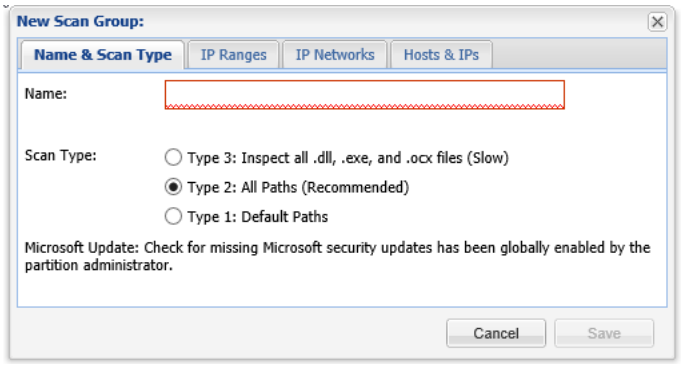
Scan Groups

This page displays a list of Scan Groups you have created. To start a scan, right-click the group name and select **Scan Group**.



If you are scanning remote hosts, your current logon credentials or the ones you supplied via “Run as...” will be used to authenticate against the remote hosts when conducting the scan.

Click **New Scan Group** to create and configure a group of hosts to be scanned.

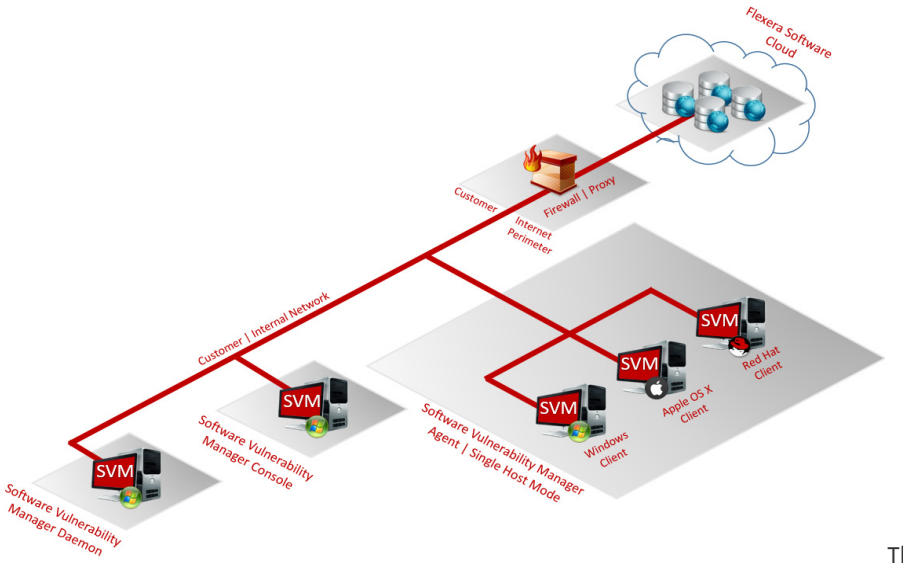


After navigating through the different tabs: **Name & Scan Type**, **IP Ranges**, **IP Networks** and **Hosts & IPs**, click **Save** to create the scan group.

Scanning Via Local Agents

Software Vulnerability Manager 2018 provides different scan approaches, enabling you to select the one that best suits your environment. The Agent-based deployment is more robust and flexible for segmented networks or networks with mobile clients (for example, laptops). Once installed, the Agent will run silently in the background.

This is the recommended scanning approach due to its flexibility, usage convenience, and performance.



The following sections provide more information for using an Agent-based deployment:

- Agent-based Scan Requirements (Windows)
- Single Host Agents
- Download Local Agent
- Agent Deployment

Agent-based Scan Requirements (Windows)

The flexibility offered by Software Vulnerability Manager 2018 ensures that it can be easily adapted to your environment.

If you choose to scan using the installable Agent (Agent-based scans), as described in Agent-based Scan Requirements (Windows), the following requirements should be present in the target hosts:

- Administrative privileges (to install the Software Vulnerability Manager 2018 Agent – csia.exe)
- Microsoft Windows XP, 2003, 2008, Vista, 7, 8, 10 or 2012
- Internet Connection – SSL 443/TCP to https://*.secunia.com/
- Windows Update Agent 2.0 or later

Single Host Agents

Use this page to manage configurations and schedule scans for the hosts where the Agent is installed as a service in Single Host mode.

Double-click a host to manage the configuration of the selected Agent and change its settings (Inspection type, Check-in frequency, Days between scans).

Right-click a host name and select **Edit Site Configuration** to manage the configuration for all the hosts in that Site.

The hosts scanned with the `csia.exe` will be grouped by Site. By default, the domain name will be used as a Site name.

You can also specify a Site name when installing the Agent by using the **-g** parameter or by specifying a site name in the additional parameters when creating the Agent deployment package described in Agent Deployment.

Download Local Agent

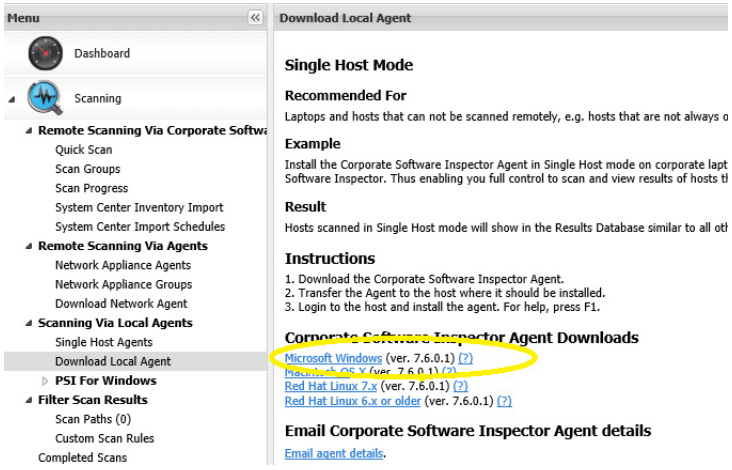
Use this page to download the `csia.exe` file, as well as read an explanation on how to install the Agent in Single Host mode.

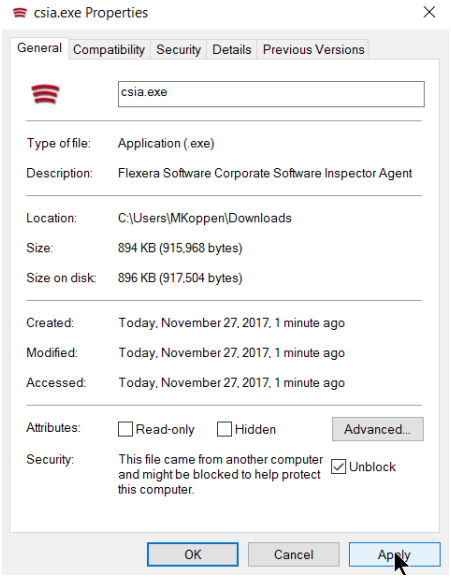
If your intention is to deploy the Software Vulnerability Manager 2018 Agent through the WSUS/System Center, please refer to Agent Deployment for further information.

Important • *Ensure that the Agent (csia.exe) is available in a local folder on the target PC before installing.*

Example:

Install the `csia.exe` (Agent) in Single Host mode; download the Agent from the Software Vulnerability Manager 2018 console under **Scanning > Scanning via Local Agents > Download Local Agent**.





Note • *Make sure to right click on the .exe in the deployment share to "Unblock" it. Click* ***Apply > OK****.*

Once the Agent is installed, every time, for example, the laptop goes online (Internet connection) it will verify if a new scan should be conducted.

After scanning, the result will be displayed in **Scanning > Completed Scans** in the Software Vulnerability Manager 2018 console.

Important • *When the Agent is installed a unique identifier is generated so that each Agent has its own unique ID. For this reason, the Agent should not be included in OS images. Doing so will result in having several instances of the same Agent and in the inability to correlate the scan results with the scanned hosts.*

Result:

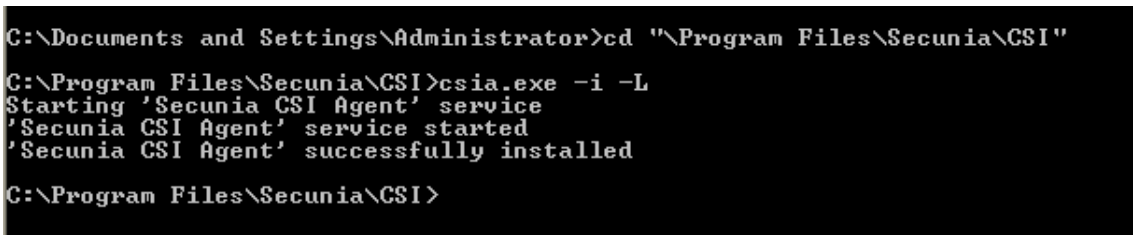
Hosts scanned with the Agent in Single Host mode will be displayed in **Results > Host Smart Groups**.

When and how the hosts are scanned can be controlled from the Software Vulnerability Manager 2018 console under **Single Host Agents**. Right-click a host name and select **Edit Configuration** to change the Agent settings.

Install the Agent from the command prompt with the Local Admin account using:

```
csia.exe -i -L
```

Example of an installation:



By using the **-L** parameter, the Agent will be installed as a service running under the LocalService user account. For further information, refer to: http://msdn.microsoft.com/en-us/library/windows/desktop/ms684190%28v=vs.85%29.aspx

If you are a member of a domain and you do not use the **-L** switch, the service will be installed under the user account performing this action, granting the 'logon as a service' privilege.

However, this privilege is usually removed in the next GPO background refresh since domain policies will not allow it. As a consequence, the Agent will stop working after the privilege has been removed.

Refer to Agent Deployment to deploy the csia.exe through WSUS/System Center for further information of how to deploy the csia.exe via Group Policy.

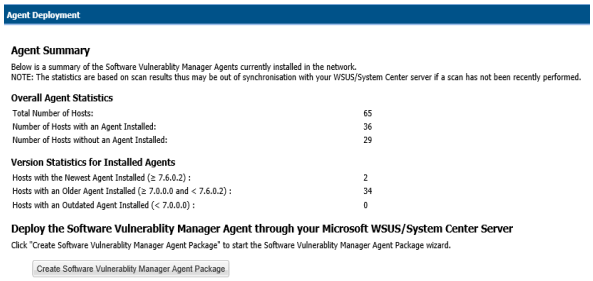
Important • *The csia.exe file is a customized executable, unique and private for your Software Vulnerability Manager 2018 account. This means that the csia.exe automatically links all scan results to your Software Vulnerability Manager 2018 account.*

Once the Agent is installed it will automatically scan after ten minutes. You can also initiate an on-demand scan by executing **csia.exe –c**.

Agent Deployment

If you choose to scan the target host by using the Software Vulnerability Manager 2018 Agent in Single Host mode (recommended), you can easily distribute and install the Agent by deploying it through the WSUS/System Center.

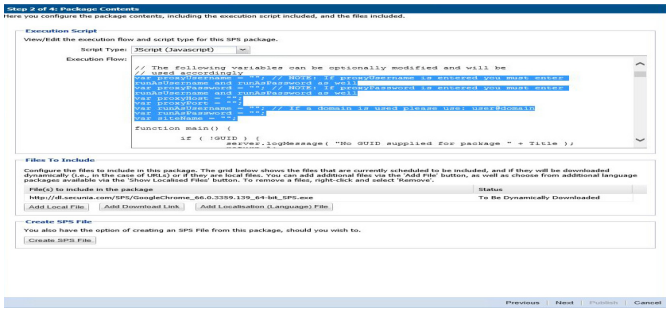
Click **Create CSI Agent Package** under **Agent Deployment** to start the Software Vulnerability Manager 2018 Agent Package wizard.



The Software Vulnerability Manager 2018 Agent Package can be created and managed just like any other SPS package. For example, you can Add Proxy Settings.

Add Proxy Settings

You can add proxy settings to the installation script in the SPS wizard when creating the Agent deployment package. In **Step 2 of 4: Package Contents**, modify the variables in the Execution Flow field.



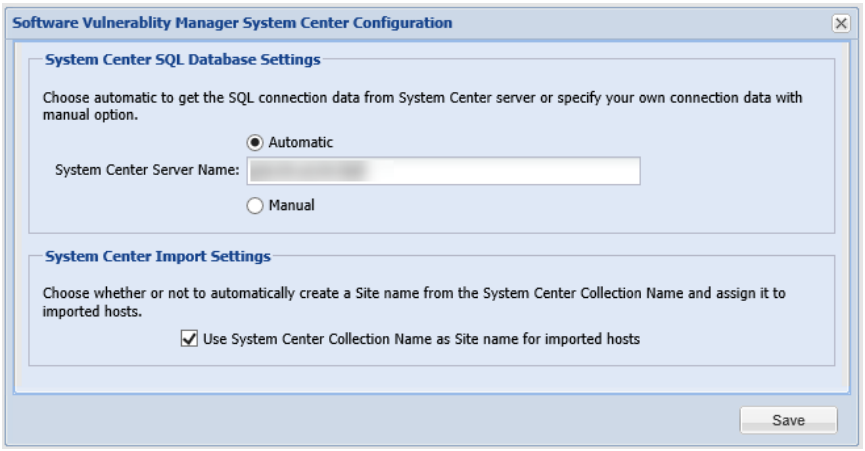
System Center Inventory Import

Scan results are obtained from the data collected by the System Center software inventory agent, which avoids the need to install the Software Vulnerability Manager 2018 Agent on each client.

System Center integration requires the following prerequisites:

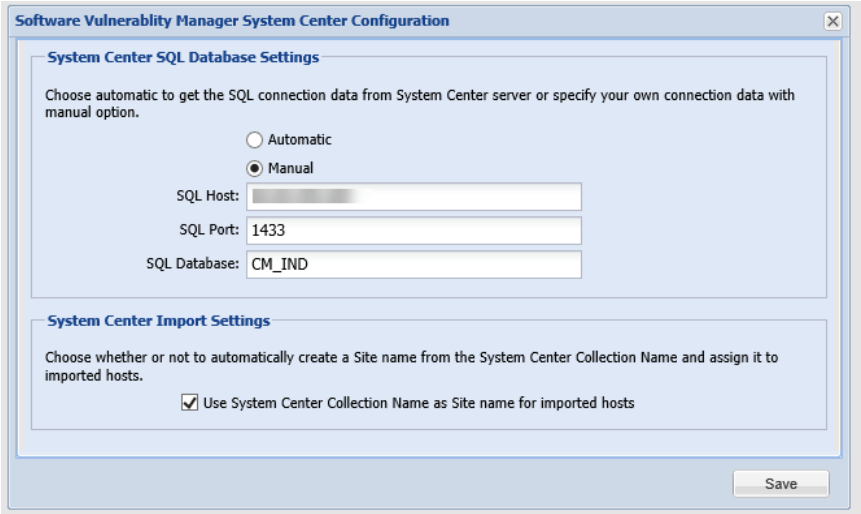
- **Setting up authentication**. The user running the Software Vulnerability Manager 2018 console must have access to the database containing the data of the System Center. For System Center Configuration Manager, the database is named **CM_<site_code>** and for System Center Configuration Manager 2007 it is named **SMS_<site_code>**. To add permissions, open SQL Server Management Studio, right-click the appropriate database, navigate to permissions, and add Connect and Select.
- **Setting up the software inventory agent**. Assuming that the System Center site has been set up, open the System Center console and ensure that the System Center client (agent) is installed on the hosts to be scanned. In System Center Configuration Manager, go to **Devices** and right-click **Install client**. Then go to **Administration > Client Settings > Properties > Software Inventory**. To configure the broadest possible pattern, select **File Detail: full** and add the patterns *.dll, *.exe, *.ocx. Do not exclude the Windows directory. Less data will be generated by specifying a narrower pattern. However, the quality of the scan result will suffer.
- In addition, you might want to consider increasing the software inventory file size from the default of 5 MB to 12 MB. To accomplish this, change the following registry key on the System Center Server:
  HKLM\Software\Microsoft\SMS\Components\SMS_SOFTWARE_INVENTORY_PROCESSOR\Max File Size

Click **Configure System Center**. In the Software Vulnerability Manager 2018 System Center Configuration page, enter the **System Center Server Name** and click **Save**.



If you select **Manual**, enter the SQL Host, SQL Port and SQL Database connection data and click **Save**.

In the System Center Inventory Import page, click **Import Selected Collections**.

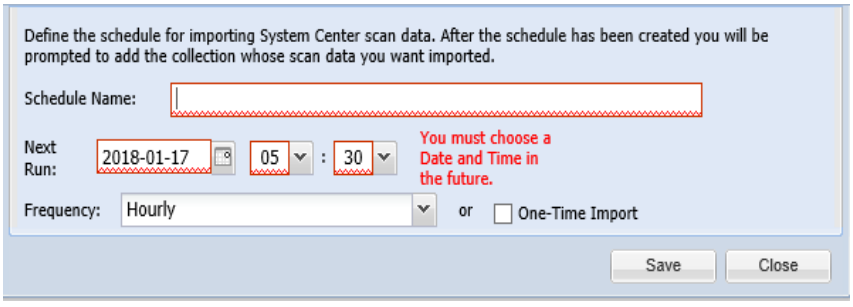


Important • *The scan result is based on the data collected by the software inventory agent, which may not be of the same quality as that of the Software Vulnerability Manager 2018 Agent (csia). This means that there could be discrepancies between a scan performed by the System Center integration and the csia. It may also result in some products not being detected correctly. For higher quality scan results Flexera recommends using the csia.*

System Center Import Schedules (Requires the Software Vulnerability Manager 2018 Daemon)

Click **New System Center Import Schedule** and enter:

- The **Schedule Name**.
- The **Next Run** date and time.
- The **Frequency** (Hourly, Daily, Weekly or Monthly) that the import will be performed or select the **One-Time Import** check box.



Click **Add Collections** and enter the Collections to include in the Import Schedule.

Right-click an Import Schedule in the grid to edit or delete the schedule.

4

Reporting

Software Vulnerability Manager 2018 includes a report function to document your scanning results.

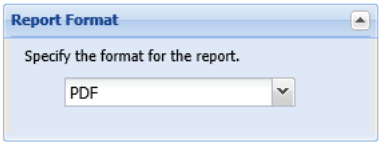
- To configure your reports and to schedule your report generation, see Report Configuration.
- To create and configure reminders, notifications, and alerts for a Smart Group, see Smart Group Notifications.

Report Configuration

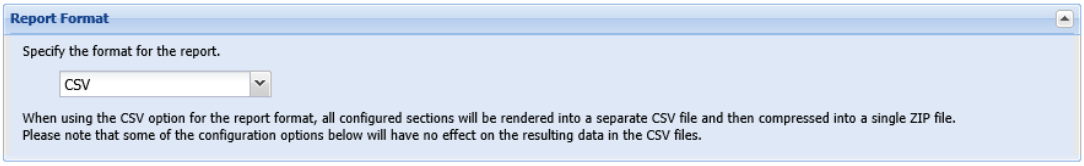
Use this page to view a list of reports that have been configured and scheduled for generation. You can configure a new report by clicking **Generate New Report** or right-click an existing report to view, edit or delete it. The Software Vulnerability Manager 2018 reporting capabilities allow the user to schedule and fully customize the intended report.

Task ***To configure a report:***

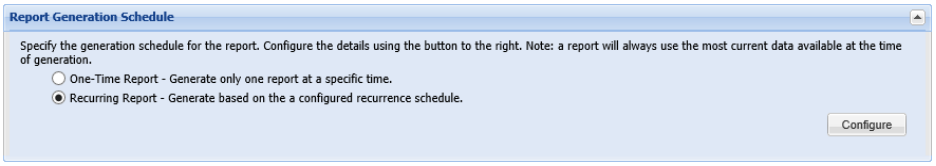
1. Choose between PDF and CSV as the format for the report.



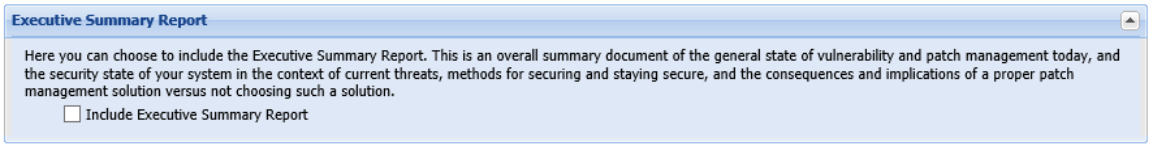
2. When using the CSV option for the report format, all configured sections will be rendered into a separate CSV file and then compressed into a single ZIP file. Please note that some of the configuration options below will have no effect on the resulting data in the CSV files.



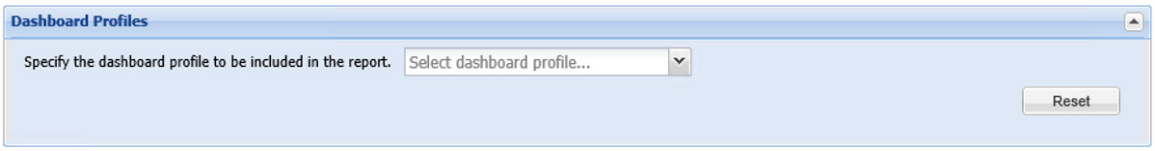
3. Choose between a One-time only report or a recurring one (daily, weekly, monthly).



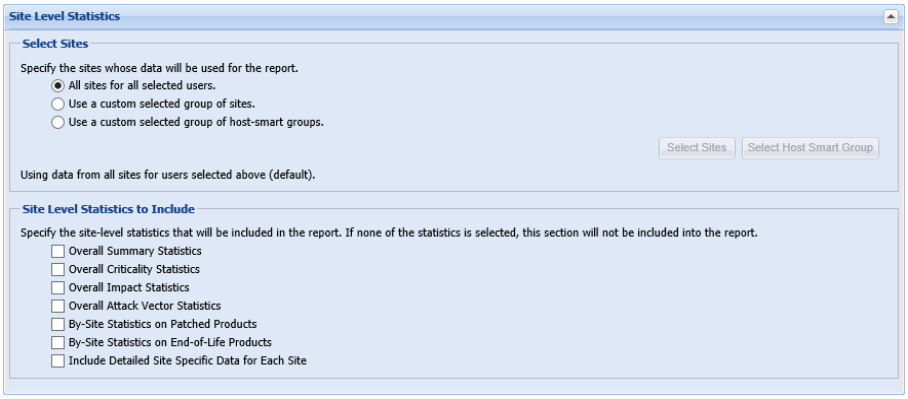
4. Choose to include the Executive Summary Report, which provides an overall summary with the general state of vulnerability and patch management.



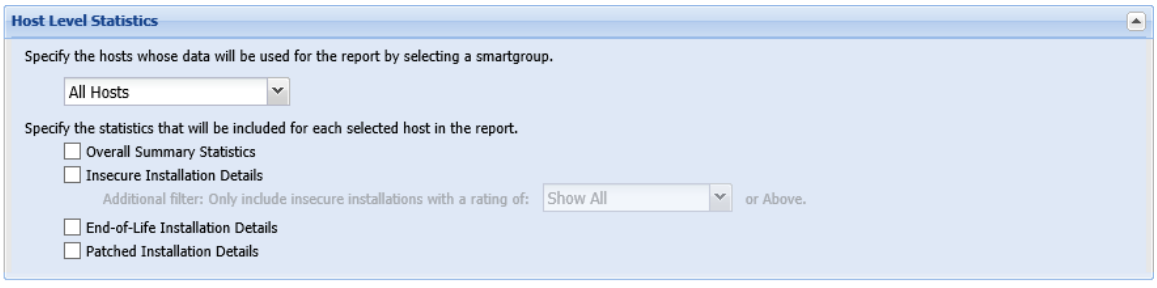
5. Choose a dashboard profile to be included in the report.



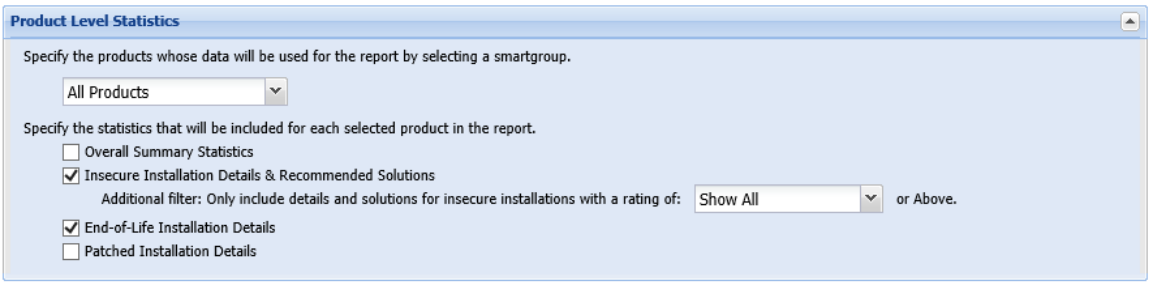
6. Choose which sites should be included together with which statistics to include.



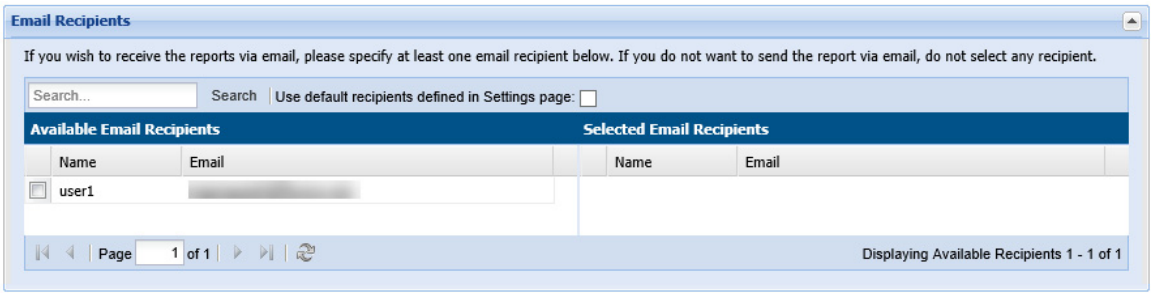
7. Choose a Host Smart Group to be included together with which statistics to include.



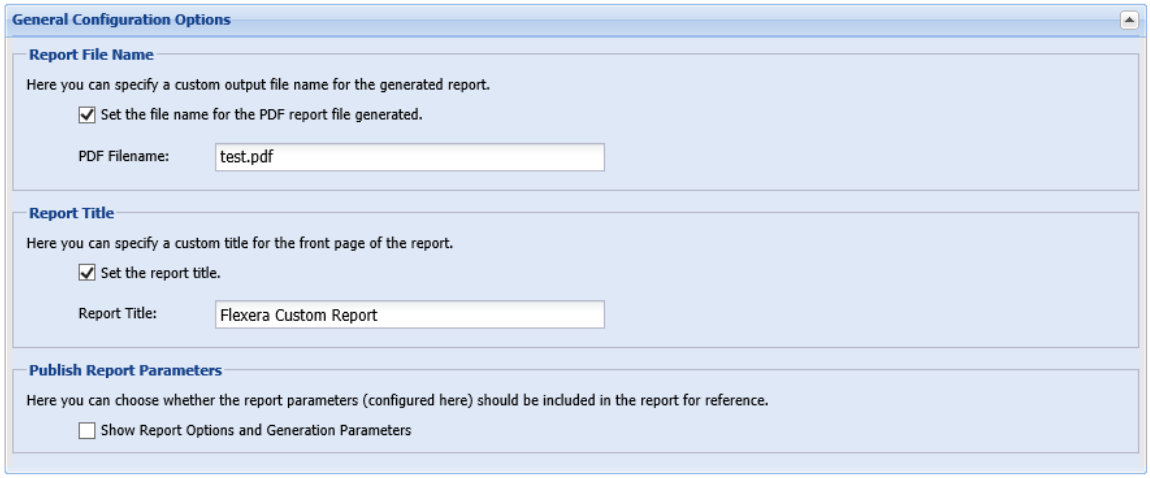
8. Choose a Product Smart Group to be included together with which statistics to include.



9. Choose the email address of the person(s) receiving the report or, if you do not want to send the report via email, do not select any recipients.



10. Choose the name for the PDF file, set the report title, and specify if you would like to include the report parameters in the report itself. All the reports available through this feature are provided in .PDF format and will be emailed to the defined email addresses in accordance with the schedule and recurrence specified. Once generated, a report can also be downloaded directly from the main page.

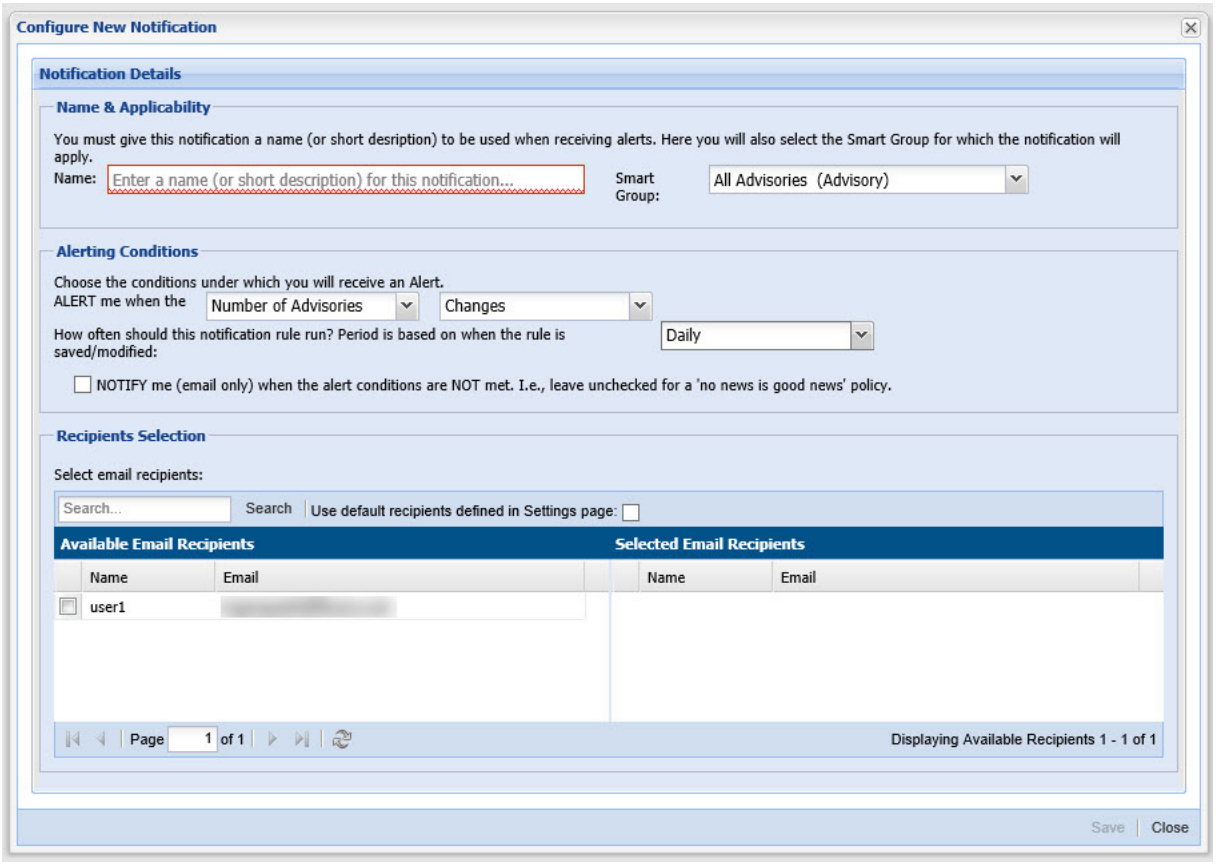


Important • *The emails containing the .PDF reports will be sent from the Flexera Data Cloud - no-reply@flexerasoftware.com. Be aware that the email server from the recipient may block/filter the email. For example, the size of the attachment may exceed a certain pre-defined threshold. If no email is being received, please check the email Spam filter and/or the Junk folder in the email client.*

Smart Group Notifications

Use this page to create and configure reminders, notifications, and alerts for a Smart Group based on the current state or changes to a group.

Click **Configure New Notification**, enter the required information, and then click **Save**.



5

Patching

After scanning your system and analyzing the appropriate vulnerabilities to patch, the next step is to patch your system. The following topics describe how to configure and deploy Software Vulnerability Manager 2018's patching function.

- Patch Configuration
- Creating the WSUS-CSI GPO Manually
- Creating a Patch with the Flexera Software Package System (SPS)
- Deploying the Update Package Using WSUS
- Deploying the Update Package Using System Center

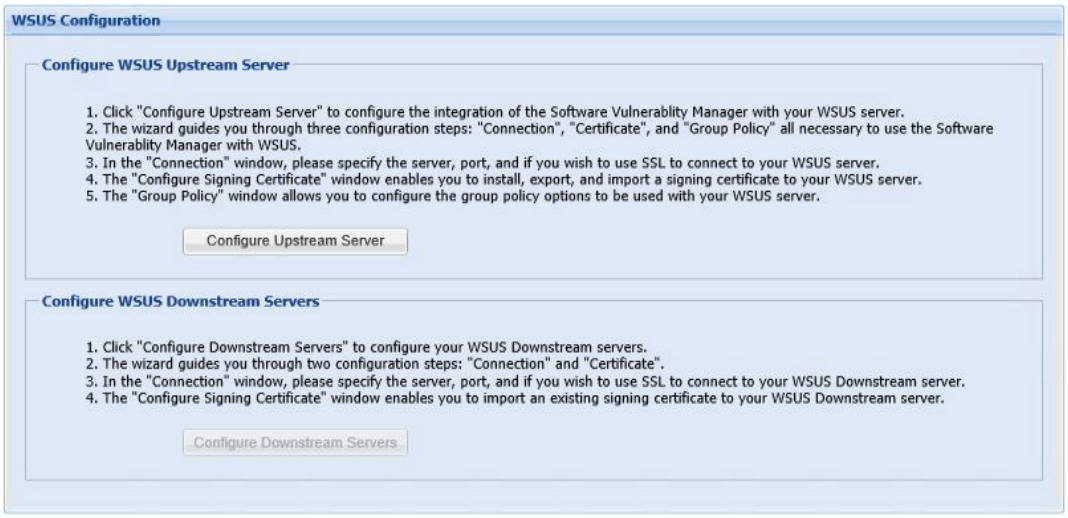
Patch Configuration

Flexera's Software Vulnerability Manager 2018 can be integrated with Microsoft's WSUS/System Center.

WSUS/System Center

Use this option to configure the integration of Software Vulnerability Manager 2018 with your WSUS server(s). If you have a single WSUS server, which is connected to the Microsoft Updates site, running the **Configure Upstream Server** wizard will be sufficient for setting up Software Vulnerability Manager 2018 with WSUS.

After clicking **Configure Upstream Server**, a configuration wizard will be initiated.



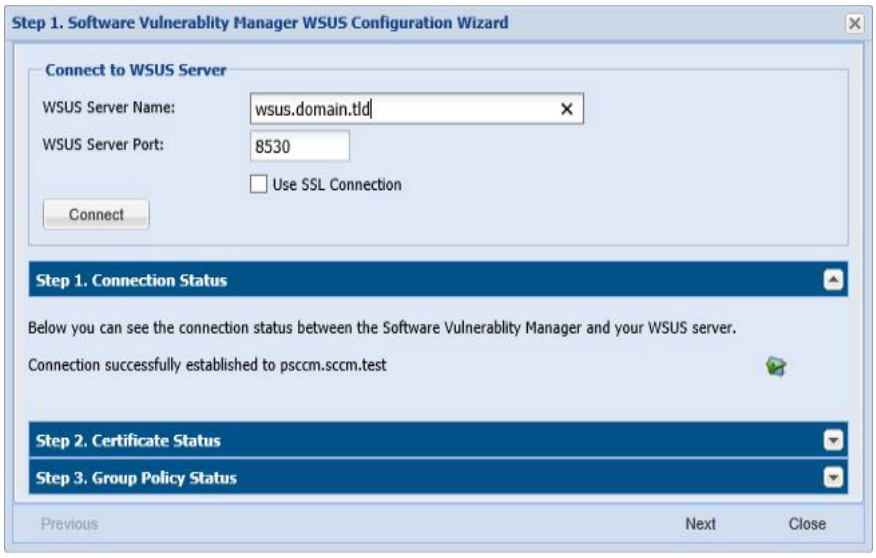
Follow the wizard steps to successfully integrate Software Vulnerability Manager 2018 with your Microsoft WSUS.

- Step 1 – Connection Status
- Step 2 - Certificate Status
- Step 3 – Group Policy Status

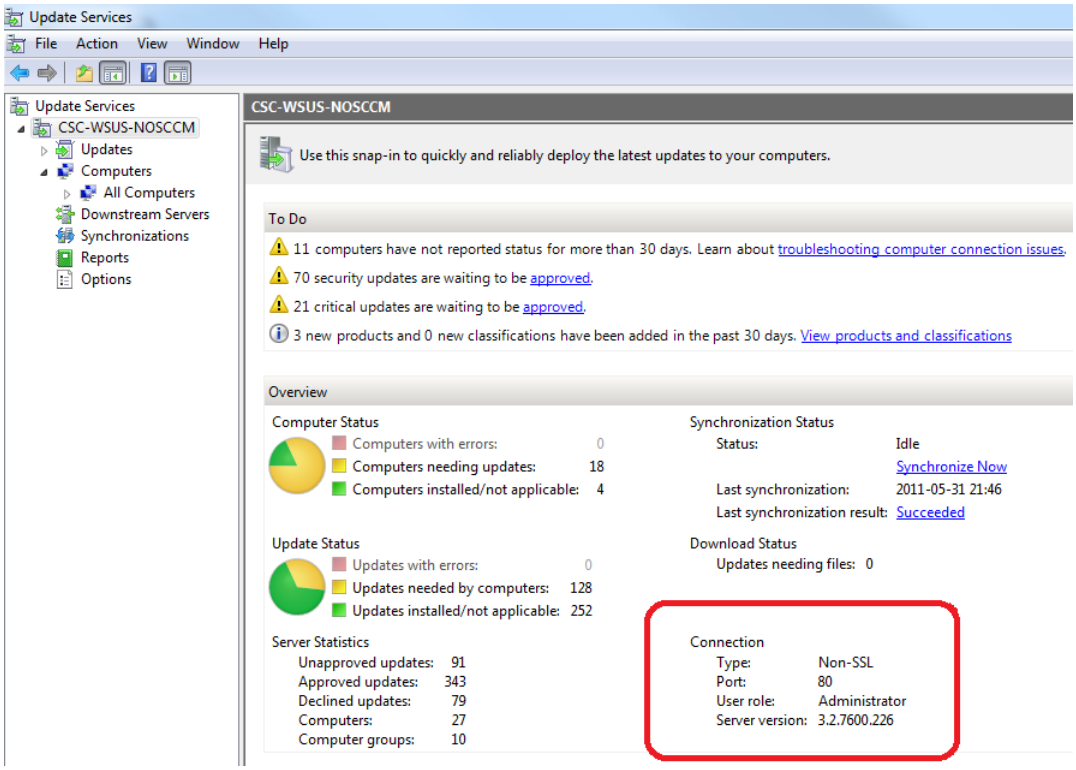
Step 1 – Connection Status

In Step 1 you should provide the relevant information (NetBIOS name and port number) for the main Upstream WSUS server. After inserting the required information, click **Connect**.

To check the status of the connection, expand **Step 1. Connection Status**.



If you are unsure of which port number to use, check your WSUS configuration as shown.



Important • *If you have a WSUS server hierarchy with one or more Downstream Replica WSUS server(s) connected to an Upstream WSUS server, please run the* ***Configure Downstream Servers*** *after running the* ***Configure Upstream Server*** *wizard.*

Important • *The port number used to connect to your WSUS depends on your settings. Ports 80 or 8530 are commonly used when SSL is not configured. Only select the* ***Use SSL Connection*** *check box if your WSUS is configured to accept SSL connections.*

Important • *Refer to http://technet.microsoft.com/en-us/library/bb633246.aspx for further information on how to configure WSUS to use SSL.*

Step 2 - Certificate Status

A code-signing certificate is needed to publish third-party updates to the WSUS/System Center, so the updates can be deployed as patches. In this step, Software Vulnerability Manager 2018 can request the WSUS to create and install the WSUS Self-Signed Certificate.

To create and install a WSUS Self-Signed Certificate in all appropriate certificate stores, click **Automatically create and install certificate**.

The WSUS Self-Signing Certificate must be installed/provisioned in the following systems:

- WSUS Server

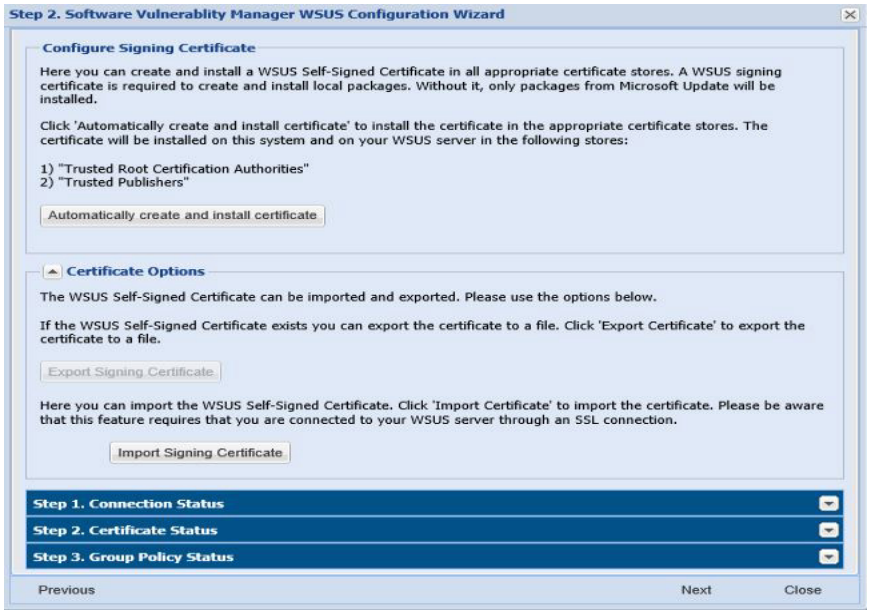
The system running Software Vulnerability Manager 2018 (note that the certificate must also be installed on the system running the Software Vulnerability Manager 2018 console)

- Clients receiving the Update

  The created certificate is required, and it will be used for all future publishing. Without the created certificate, only packages from Microsoft Update will be installed.

If you would like to use your own CA certificate instead of the Microsoft WSUS Self-Signing Certificate, click **Import Signing Certificate**.

At Step 3 – Group Policy Status, the certificate created/imported in this step will be provisioned to all clients through a GPO.



Important • *Be careful not to re-provision a signing certificate on a WSUS server that already has a signing certificate assigned. Doing so can cause issues with certificate validation at the WSUS server and target computers unless BOTH certificates (new and old) are left in the appropriate certificates stores (Trusted Publishers and Trusted Root Authorities). It can also cause issues with troubleshooting.*

Once a certificate is either inserted or created, it does not need to be recreated until it expires or needs to be replaced.

Click **Automatically create and install certificate**. The certificate will be installed on the WSUS server in the following stores:

- Trusted Root Certification Authorities
- Trusted Publishers
- WSUS – The certificate in this location must also contain the private key.

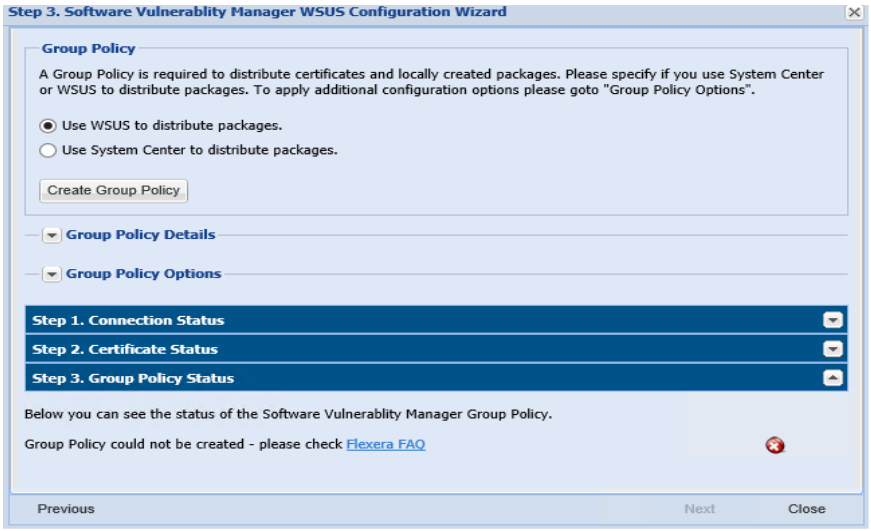
Expand the Certificate Options to access the import and export certificate features.

Important • *To import your own certificate through Software Vulnerability Manager 2018, the WSUS connection must be configured to accept SSL connections.*

Step 3 – Group Policy Status

A Group Policy is required to distribute certificates and locally created packages. Software Vulnerability Manager 2018 can easily create this GPO so the WSUS Signing Certificate is distributed to all clients. Please choose to use WSUS or System Center. Once this is completed, expand the Group Policy Options.

If you are creating the Software Vulnerability Manager 2018 WSUS Group Policy for the first time, proceed by selecting all the options, and then click **Create Group Policy**.

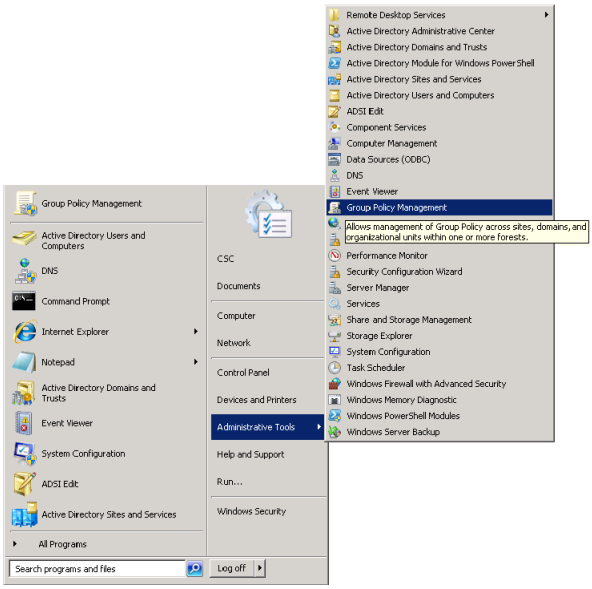


Important • *Besides distributing the certificate through the Software Vulnerability Manager 2018 WSUS GPO, it is also possible to provision certificate to the target computers by going to* ***Patching > WSUS/System Center > Deployment*** *and selecting the target hosts where the certificate is to be installed (CTRL+ mouse click for multiple selection). Then right-click and select* ***Verify and Install Certificate****.*

Creating the WSUS-CSI GPO Manually

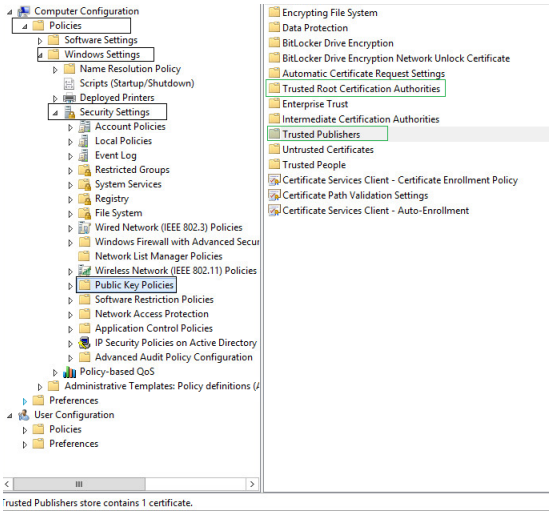
Task ***To create the WSUS-CSI GPO manually:***

1. Export the WSUS Self-Signed Certificate.
2. On the Domain Controller, click **Start > Administrative Tools > Group Policy Management**. Right-click your Domain name and select **Create a GPO in this domain, and Link it here**. Alternatively you can edit an existing GPO.

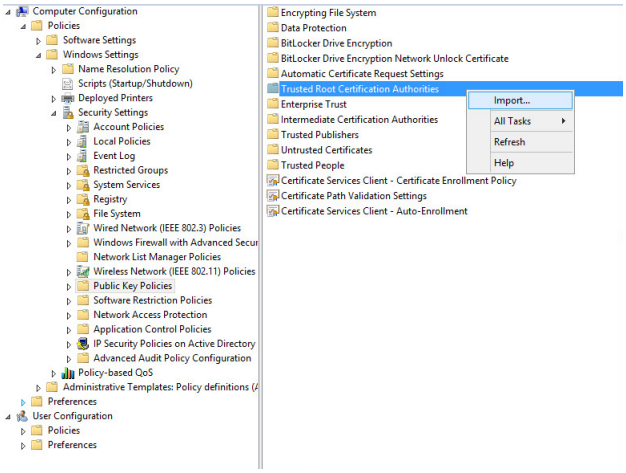


3. Right-click the GPO that you created/edited in the previous steps and select **Edit**.

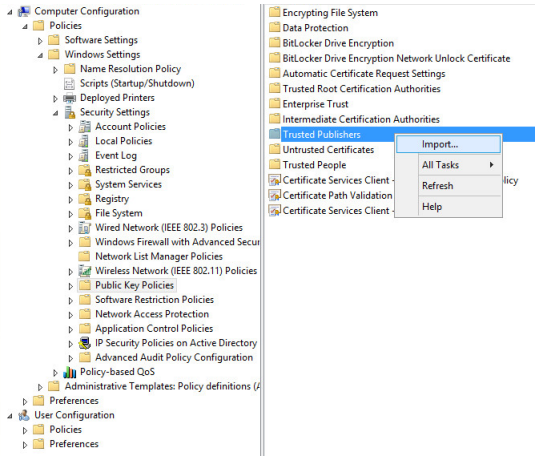
4. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.



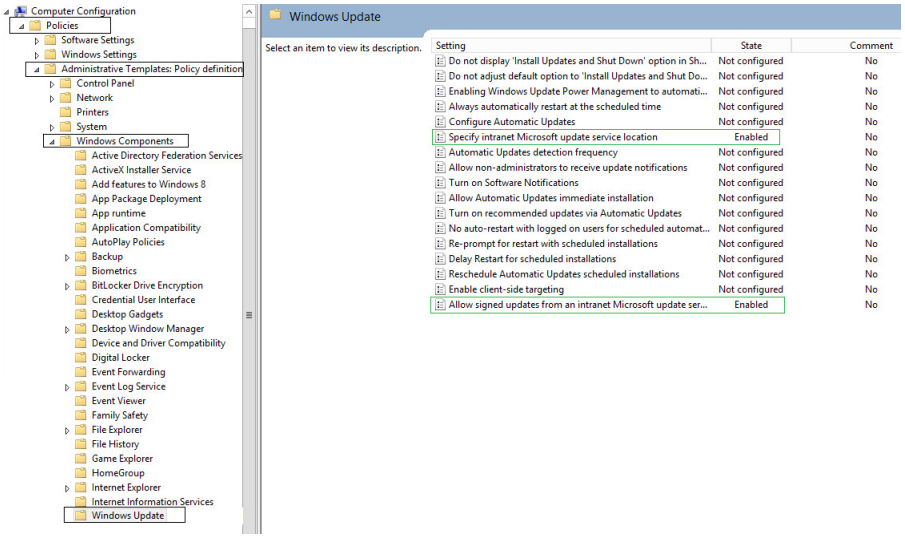
5. Right-click **Trusted Root Certification Authority** and select **Import**. Import the certificate that you exported in Step 1.



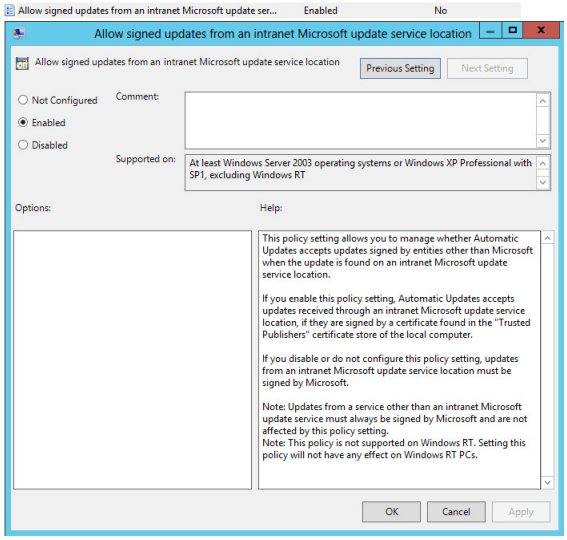
6. Repeat Step 4 and import the certificate for **Trusted Publishers**.



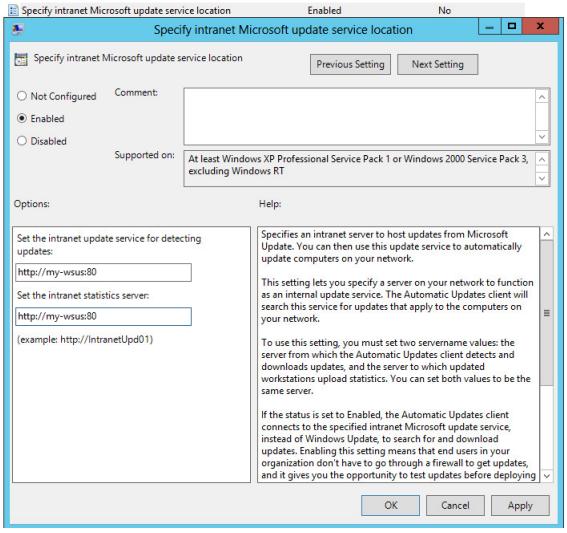
7. Navigate to **Computer Configuration > Administrative templates > Windows Component > Windows Update**.



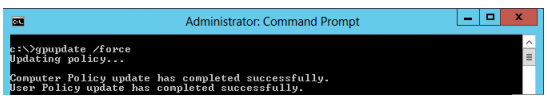
8. On the right side menu, double-click **Allow signed updates from an intranet Microsoft update service location**. Select **Enabled** and click **OK**.



9. On the right side menu, double-click **Specify intranet Microsoft update service location**. Enable this setting and modify the existing empty fields with the intranet address of your WSUS Server. This step is only valid for WSUS integration and is not required for System Center Configuration Manager integration.



10. Link the created GPO to an Active Directory container appropriate for your environment.



The clients affected by the created GPO will install the certificate being distributed (either the WSUS Self-Signed Certificate or your own CA certificate) and acknowledge the Windows Update settings that you have specified in the GPO.

By default, Group Policy refreshes in the background every 90 minutes, with a random offset of 0 to 30 minutes. If you want to refresh Group Policy sooner, you can go to a command prompt on the client computer and type:

gpupdate /force.

For further information on how to configure Automatic Updates by Using Group Policy, see http://technet.microsoft.com/en-us/library/cc720539(WS.10).aspx.

Creating a Patch with the Flexera Software Package System (SPS)

The Flexera Software Package System (SPS) page displays a list of products that you can create updates for.

Click **Configure View** to customize the list and limit the types of products shown, as well as highlight products for which packages have or have not been created.

If highlighted, products for which SPS packages exist will be shown in green.

A product will be displayed in blue if the vendor provides unattended/silent installation parameters for its patches. Any product listed in blue is available to have an update created in a simple four-step process.

- Step 1 of 4: Package Configuration
- Step 2 of 4: Package Contents
- Step 3 of 4: Applicability Criteria - Paths
- Step 4 of 4: Applicability Criteria - Rules

Some products are presented in gray because the vendor of the product does not provide silent installation parameters. If you choose to patch one of these products, you must provide (import) the **.MSI/.MSP/.EXE** file together with the parameters for the unattended installation. Software Vulnerability Manager 2018 will then repackage and publish the update through the standard workflow. Packages cannot be automatically created by Software Vulnerability Manager 2018 for these products.

If you wish to create a new custom package that does not necessarily patch an existing product, for example to deploy new software, you can click **New Custom Package**. In this case you should provide the files/installer that will be executed on the target client together with the execution flow script.

With Software Vulnerability Manager 2018, you are able to create three different kinds of packages. Right-click a product and select one of the available options:

- Create Update Package
- Create Uninstall Package
- Create Custom Package

For the Update and Uninstall packages, a default execution flow script is provided in the SPS Package Creation Wizard (Step 2 of 4: Package Contents), which will fulfill most of the common needs.

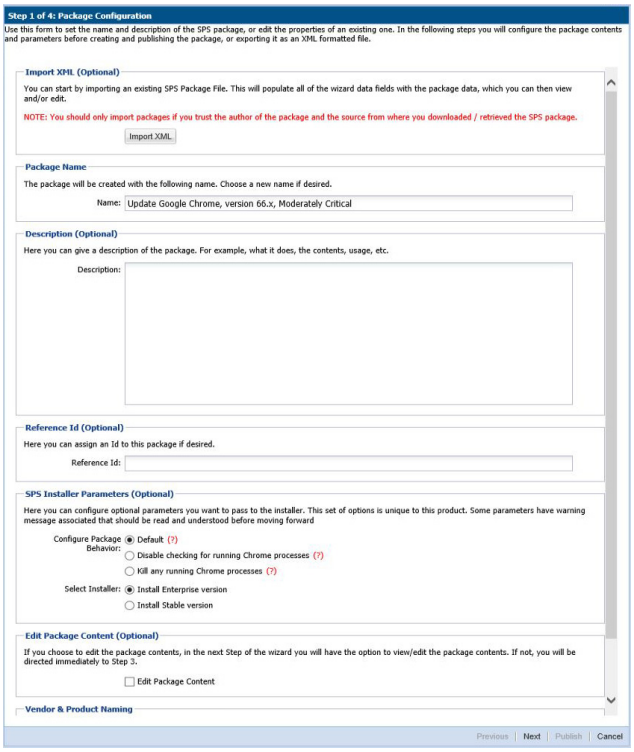
The execution flow script for an Update package can also be customized for additional functionality. You can also configure your patching package SPS Installer Parameters using dynamic check box options (where applicable) based on product functionality, including:

- Remove End User License Agreement
- Disable Automatic Updates

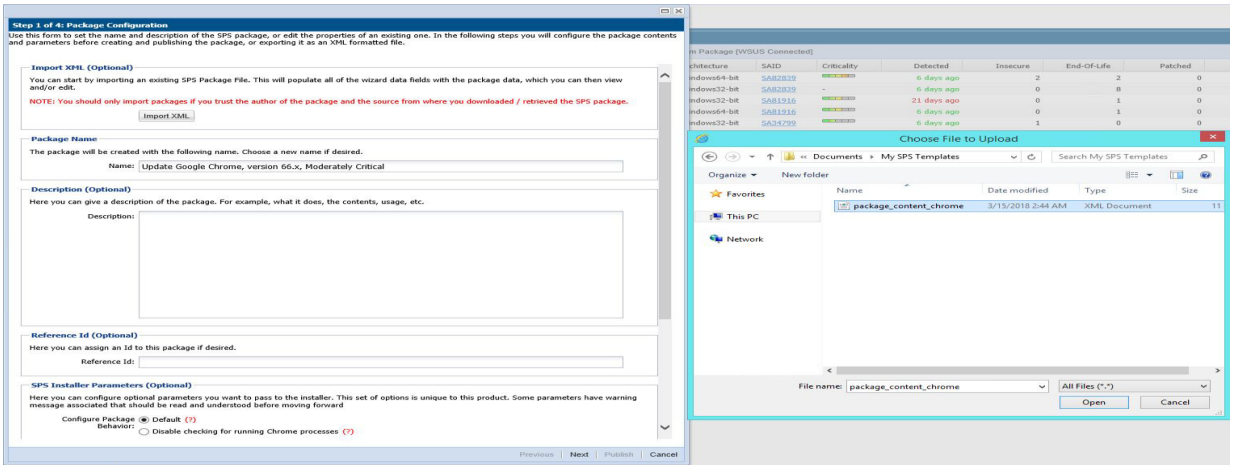
- Silent Install
- Update to lowest secure version
- No reboot necessary
- Cumulative updates in one package
- Set Security Level
- Remove system tray icon
- Restrict Java Applications
- Uninstall Prior to Installing
- Prevent Installation of Certain Components
- Prevent Collection of Anonymous Usage Statistics
- Remove Desktop Shortcut

Step 1 of 4: Package Configuration

In Step 1, no action is required if the selected product was in blue. You should only check **Edit Package Content (Optional)** if the product was in gray or there is a need to customize the update patch by selecting a different file(s) and/or defining a different execution flow script.



The **Import Package** feature allows you to import a SPS template in XML format that will automatically populate all the fields of the SPS Package Creation Wizard. This feature will be especially relevant when creating custom updates or when creating update packages for the products in gray.



In Step 4 of 4: Applicability Criteria - Rules, you will also have the option to export the XML template for the package being created.

After clicking **Next**, and if **Edit Package Content (Optional)** was not selected, you will go directly to Step 3 of 4: Applicability Criteria - Paths.

Step 2 of 4: Package Contents

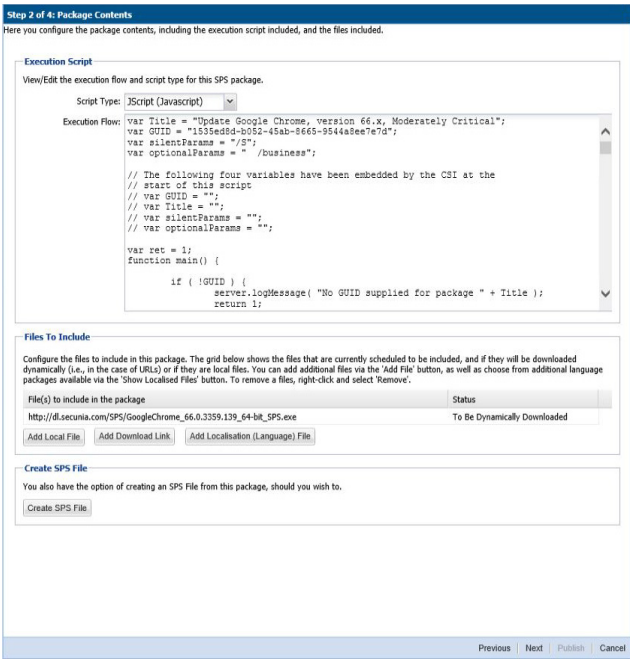
Step 2 becomes available when **Edit Package Content** is selected in Step 1 of 4: Package Configuration. The first section of Step 2 is the Execution Script where you select **JScript (Javascript)**, **VBScript** or **Powershell Script** and then review or create a customized execution flow.

Important • *When using Powershell Scripting as the execution controlling script of the package, you must ensure that Microsoft Visual C++ 2012 Redistributable (x86) is installed on the target hosts you are deploying the update package to.*

You are also able to change the files that are included in the SPS package, which can either be local files or links to be dynamically downloaded upon publishing of the package.

To test a newly created execution flow together with the added files click **Create SPS File**. A SPS.exe file is created that can be executed locally prior to being published into the WSUS server.

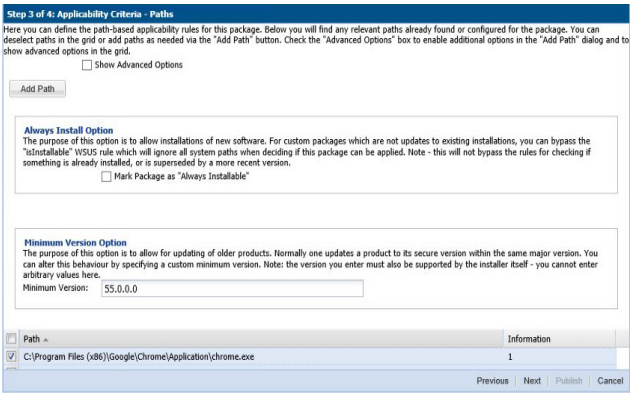
This SPS.exe file will include the execution flow script and the files to be included, but not the applicability rules.



Step 3 of 4: Applicability Criteria - Paths

In Step 3 you should select the paths/locations to which this package should be applied. These are usually populated by Software Vulnerability Manager 2018 based on the scans previously conducted.

Please be advised to only choose paths that are valid to avoid any update loops. You can also use paths with CSIDL and KNOWNFOLDERID if you select the **Show Advanced Options** check box. These variables should be used with their decimal value.



For packages that should not have any paths for applicability, select the **Mark Package as "Always Installable"** check box to ignore all paths. Paths for App-V and Mac OS X are filtered out since they are not supported for patching.

Use the **Minimum Version Option** to update older products. Normally, a product is updated to its secure version within the same major version. You can alter this behavior by specifying a custom minimum version.

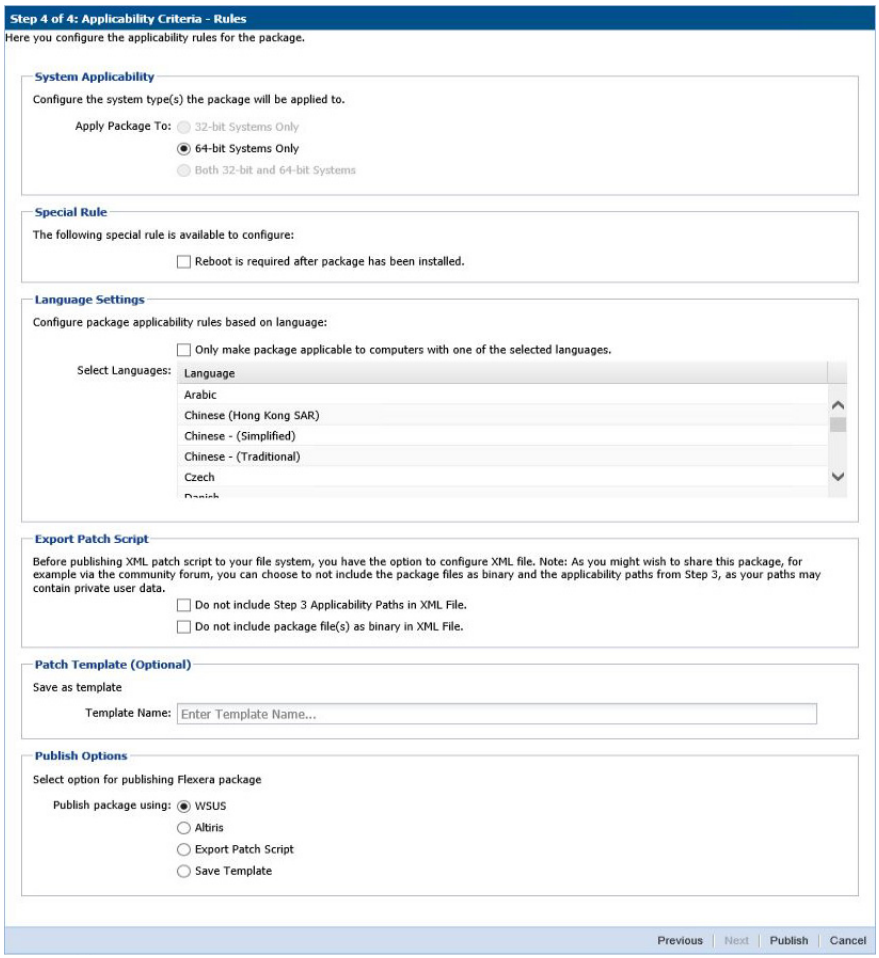
Note • *The version you enter must also be supported by the installer itself. You cannot enter arbitrary values here.*

Step 4 of 4: Applicability Criteria - Rules

In Step 4 you should specify if you want to limit the package to 32-bit or 64-bit systems or computers with specific operating system languages. The patch file to be deployed will be automatically downloaded in the background by the Software Vulnerability Manager 2018 console. Once this is completed, the Software Vulnerability Manager 2018 console will repackage and publish the update package into the WSUS/System Center.

The WSUS option will be unavailable if the WSUS Connection is not established.

To export the package select **File System (Export)** and click **Publish**.



If a reboot is required after the package has been installed, this option can also be configured in the second part of this step, as well as checking if Java is running.

To configure your package to only be applicable for certain languages of the operating system, select **Only make package applicable to computers with one of the selected languages** and select the relevant language.

In this step you are also able to export the package that you have already configured to be used for future reference. You have the option to include or exclude Step 3 applicability paths and the installer as binary.

The two options (**Do not include Step 3 Applicability Paths in XML File** and **Do not include the package file(s) as binary in XML File**) are taken into consideration only when exporting the package to the **File System (Export)**. Otherwise the selection will be disregarded.

Deploying the Update Package Using WSUS

To deploy the update package using WSUS, the update package must be approved. After publishing the package into the WSUS, and assuming that the update is visible under **Available**, right-click the package name and select **Approve**.

You will be prompted to select the computer target groups for which you would like to approve the update. These target groups are configured in the WSUS.

The same approach should be used if you wish to decline a previously approved update.

Deploying the Update Package Using System Center

The actions **Approve** and **Decline** are only applicable if the package is to be deployed through WSUS. If you are using the Microsoft System Center, the package created with Software Vulnerability Manager 2018 will be available in your System Center.

A

Appendix A - Certificates

This appendix describes the types of certificates to obtain to deploy patches and how to verify and validate the certificate.

- WSUS Self-Signed Certificate (Microsoft)
- Using Your Own Certification Authority (CA) Certificate
- CA Verification and Validation

WSUS Self-Signed Certificate (Microsoft)

A code-signing certificate is needed to publish third-party updates to the WSUS/System Center, so the updates can be deployed as patches. Therefore, the Microsoft WSUS creates its own certificate named WSUS Self-Signed Certificate.

The WSUS Self-Signed Certificate must be installed/provisioned in the following systems:

- WSUS Server: Trusted Root Certification Authorities, Trusted Publishers, WSUS certificate stores
- The system running Software Vulnerability Manager 2018 (note that the certificate must also be installed on the system running the Software Vulnerability Manager 2018 console): Trusted Root Certification Authorities, Trusted Publishers
- Clients receiving the Update: Trusted Root Certification Authorities, Trusted Publishers (both distributed by GPO)

Important • *To import your own certificate through Software Vulnerability Manager 2018, the WSUS connection must be configured to accept an SSL connection.*

Using Your Own Certification Authority (CA) Certificate

- If you would like to use a signing certificate to sign the updates created by Software Vulnerability Manager 2018, it must be a PKCS #12 format and have the private key included if not already present on your WSUS.
- Generally speaking, the certificate should match the requirements of Microsoft System Update Publisher (SCUP). Click here for more details.
- A Group Policy or a deployment package can be used to distribute certificates for locally created packages. In addition to the root certificate or the public signing certificate in Trusted Root Certification Authorities, the public code signing certificate has to be deployed to the Trusted Publishers folder.
- Furthermore, it is necessary to allow signed packages on target computers in Windows Update settings ("Computer Settings/Policies/Administrative Templates/Windows Components/Windows Updates").

CA Verification and Validation

Each publicly available program must be signed with a signing certificate that proves the identity and integrity of the application.

When enabled, the Check for Publisher Certificate Revocation security feature forces Internet Explorer to verify and validate the Certification Authority (CA) that issued the signing certificate used for signing Software Vulnerability Manager 2018. This feature also verifies whether Software Vulnerability Manager 2018's code-signing certificate was previously revoked or not. Internet Explorer will then attempt to connect to crl.verisign.net to verify the CA issuer or to crl.thawte.com to verify the Software Vulnerability Manager 2018's SSL certificate.

In corporate environments, where advanced Firewall setups or Proxy Servers are used to authenticate and strictly control all inbound/outbound connections, this security feature may cause a potential problem for Software Vulnerability Manager 2018 users.

If the addresses crl.verisign.net, crl.thawte.com and *.ws.symantec.com are not white-listed in the Firewall/Proxy server configuration, the CA validation check may not succeed. Additionally, Software Vulnerability Manager 2018, and its scanning Agent respectively, will be denied access to system and online resources causing them to fail to start.

White-listed in the Firewall/Proxy server configuration:

- crl.verisign.net
- crl.thawte.com
- *.ws.symantec.com