Legal Information

Book Name: Software Vulnerability Research User Guide
Part Number: SVR-JUNE2023-UG00
Product Release Date: June 2023

Copyright Notice

Copyright © 2023 Flexera
This publication contains proprietary and confidential information and creative works owned by Flexera and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.
All copies of the technology and related information, if allowed by Flexera, must display this notice of copyright and ownership in full.

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see https://www.flexera.com/legal/intellectual-property.html. 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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Manager</td>
<td>71</td>
</tr>
<tr>
<td>Dashboard</td>
<td>63</td>
</tr>
<tr>
<td>Historic Advisories</td>
<td>82</td>
</tr>
<tr>
<td>Install the Daemon</td>
<td>46</td>
</tr>
<tr>
<td>Add a Digital Certificate to Windows Server Update Services (WSUS)</td>
<td>48</td>
</tr>
<tr>
<td>Create a Group Policy to Deploy Your Certificate</td>
<td>48</td>
</tr>
<tr>
<td>Smart Group Configuration</td>
<td>51</td>
</tr>
<tr>
<td>Daemon Deployment</td>
<td>46</td>
</tr>
<tr>
<td>Deploy a Linux Agent</td>
<td>34</td>
</tr>
<tr>
<td>Deploy the Windows Agent Application through Microsoft’s System Center Configuration Manager (SCCM)</td>
<td>36</td>
</tr>
<tr>
<td>Run Windows Agent through the Microsoft System Center as a Task Sequence</td>
<td>38</td>
</tr>
<tr>
<td>Package Deployment</td>
<td>60</td>
</tr>
<tr>
<td>Build Package</td>
<td>60</td>
</tr>
<tr>
<td>Patch Template</td>
<td>58</td>
</tr>
<tr>
<td>System Requirements for Patching</td>
<td>58</td>
</tr>
<tr>
<td>Packages</td>
<td>58</td>
</tr>
<tr>
<td>Patch Template</td>
<td>58</td>
</tr>
<tr>
<td>Build Package</td>
<td>60</td>
</tr>
<tr>
<td>Package Deployment</td>
<td>60</td>
</tr>
<tr>
<td>Additional Patching Information</td>
<td>61</td>
</tr>
<tr>
<td>Rule Triggers</td>
<td>54</td>
</tr>
<tr>
<td>Notification Actions</td>
<td>56</td>
</tr>
<tr>
<td>Default Workflow Rules</td>
<td>56</td>
</tr>
<tr>
<td>Custom Workflow Rules</td>
<td>57</td>
</tr>
<tr>
<td>Condition and Logic Operators</td>
<td>51</td>
</tr>
<tr>
<td>Smart Group Configuration</td>
<td>51</td>
</tr>
<tr>
<td>Advanced Smart Groups</td>
<td>52</td>
</tr>
<tr>
<td>Additional Smart Group Information</td>
<td>53</td>
</tr>
<tr>
<td>Workflow Management Rules</td>
<td>53</td>
</tr>
<tr>
<td>Create a Workflow Rule - Overview</td>
<td>54</td>
</tr>
<tr>
<td>Rule Triggers</td>
<td>54</td>
</tr>
<tr>
<td>Patch Rule Actions</td>
<td>55</td>
</tr>
<tr>
<td>Notification Actions</td>
<td>56</td>
</tr>
<tr>
<td>Default Workflow Rules</td>
<td>56</td>
</tr>
<tr>
<td>Custom Workflow Rules</td>
<td>57</td>
</tr>
<tr>
<td>Workflows</td>
<td>53</td>
</tr>
<tr>
<td>Workflows</td>
<td>53</td>
</tr>
<tr>
<td>Workflows</td>
<td>53</td>
</tr>
<tr>
<td>4 Dashboard</td>
<td>63</td>
</tr>
<tr>
<td>4 Dashboard</td>
<td>63</td>
</tr>
<tr>
<td>5 Notifications</td>
<td>69</td>
</tr>
<tr>
<td>6 Vulnerability Manager</td>
<td>71</td>
</tr>
<tr>
<td>Overview</td>
<td>71</td>
</tr>
<tr>
<td>Overview</td>
<td>71</td>
</tr>
<tr>
<td>Watch Lists &amp; Advisories</td>
<td>72</td>
</tr>
<tr>
<td>Watch Lists</td>
<td>72</td>
</tr>
<tr>
<td>View Watch Lists</td>
<td>73</td>
</tr>
<tr>
<td>Create Watch Lists</td>
<td>74</td>
</tr>
<tr>
<td>Edit Watch Lists</td>
<td>76</td>
</tr>
<tr>
<td>Import a New Watch List</td>
<td>78</td>
</tr>
<tr>
<td>Import an Updated Watch List</td>
<td>81</td>
</tr>
<tr>
<td>Historic Advisories</td>
<td>82</td>
</tr>
<tr>
<td>Install the Daemon</td>
<td>46</td>
</tr>
<tr>
<td>Add a Digital Certificate to Windows Server Update Services (WSUS)</td>
<td>48</td>
</tr>
<tr>
<td>Create a Group Policy to Deploy Your Certificate</td>
<td>48</td>
</tr>
<tr>
<td>4 Dashboard</td>
<td>63</td>
</tr>
<tr>
<td>Daemon Deployment</td>
<td>46</td>
</tr>
<tr>
<td>Deploy a Linux Agent</td>
<td>34</td>
</tr>
<tr>
<td>Deploy the Windows Agent Application through Microsoft’s System Center Configuration Manager (SCCM)</td>
<td>36</td>
</tr>
<tr>
<td>Run Windows Agent through the Microsoft System Center as a Task Sequence</td>
<td>38</td>
</tr>
<tr>
<td>Package Deployment</td>
<td>60</td>
</tr>
<tr>
<td>Build Package</td>
<td>60</td>
</tr>
<tr>
<td>Patch Template</td>
<td>58</td>
</tr>
<tr>
<td>System Requirements for Patching</td>
<td>58</td>
</tr>
<tr>
<td>Packages</td>
<td>58</td>
</tr>
<tr>
<td>Patch Template</td>
<td>58</td>
</tr>
<tr>
<td>Build Package</td>
<td>60</td>
</tr>
<tr>
<td>Package Deployment</td>
<td>60</td>
</tr>
<tr>
<td>Additional Patching Information</td>
<td>61</td>
</tr>
<tr>
<td>Rule Triggers</td>
<td>54</td>
</tr>
<tr>
<td>Notification Actions</td>
<td>56</td>
</tr>
<tr>
<td>Default Workflow Rules</td>
<td>56</td>
</tr>
<tr>
<td>Custom Workflow Rules</td>
<td>57</td>
</tr>
<tr>
<td>Workflows</td>
<td>53</td>
</tr>
<tr>
<td>Workflows</td>
<td>53</td>
</tr>
<tr>
<td>Workflows</td>
<td>53</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Group Selection Order</td>
<td>124</td>
</tr>
<tr>
<td>Create a Smart Group</td>
<td>125</td>
</tr>
<tr>
<td>Create a Smart Groups Report</td>
<td>127</td>
</tr>
<tr>
<td><strong>Devices</strong></td>
<td>127</td>
</tr>
<tr>
<td>Device Details</td>
<td>128</td>
</tr>
<tr>
<td><strong>Products</strong></td>
<td>130</td>
</tr>
<tr>
<td>Product Details</td>
<td>131</td>
</tr>
<tr>
<td><strong>Advisories</strong></td>
<td>132</td>
</tr>
<tr>
<td>Advisory Details</td>
<td>132</td>
</tr>
<tr>
<td>Create Advisory Tickets</td>
<td>134</td>
</tr>
<tr>
<td><strong>10 Patching</strong></td>
<td>135</td>
</tr>
<tr>
<td>Patch Library</td>
<td>135</td>
</tr>
<tr>
<td>Templates</td>
<td>136</td>
</tr>
<tr>
<td>Packages</td>
<td>137</td>
</tr>
<tr>
<td>Deployment</td>
<td>138</td>
</tr>
<tr>
<td>Information</td>
<td>138</td>
</tr>
<tr>
<td>Update Deployment</td>
<td>139</td>
</tr>
<tr>
<td>Patching Tickets</td>
<td>139</td>
</tr>
<tr>
<td>Delete Patching Tickets</td>
<td>140</td>
</tr>
<tr>
<td><strong>Manual Signatures</strong></td>
<td>140</td>
</tr>
<tr>
<td>Enable Manual Signatures</td>
<td>141</td>
</tr>
<tr>
<td>Share Unsigned and Signed .cab Files</td>
<td>141</td>
</tr>
<tr>
<td>Deploy the Agent for a Manual Signature</td>
<td>142</td>
</tr>
<tr>
<td>Deploy a Patch Package for a Manual Signature</td>
<td>143</td>
</tr>
<tr>
<td>Manual Signature Notifications</td>
<td>144</td>
</tr>
<tr>
<td><strong>11 Policy Manager</strong></td>
<td>147</td>
</tr>
<tr>
<td>Overview</td>
<td>147</td>
</tr>
<tr>
<td>Policies</td>
<td>147</td>
</tr>
<tr>
<td>Breaches</td>
<td>149</td>
</tr>
<tr>
<td><strong>12 Analytics</strong></td>
<td>151</td>
</tr>
<tr>
<td>Advisories</td>
<td>151</td>
</tr>
<tr>
<td>Advisories by Threat Score</td>
<td>153</td>
</tr>
<tr>
<td>Tickets</td>
<td>154</td>
</tr>
<tr>
<td>Devices</td>
<td>155</td>
</tr>
<tr>
<td>Products</td>
<td>156</td>
</tr>
<tr>
<td>Reports</td>
<td>157</td>
</tr>
<tr>
<td>LiveUpdate</td>
<td>163</td>
</tr>
<tr>
<td><strong>13 Ticket Manager</strong></td>
<td>165</td>
</tr>
<tr>
<td>View and Change Tickets Status and Priority</td>
<td>165</td>
</tr>
</tbody>
</table>
Create Tickets in Ticket Manager ................................................................. 166
Delete Tickets in Ticket Manager ............................................................... 167
Default Ticket Statuses in Ticket Manager .................................................. 167

14 Settings ......................................................................................... 169

Account .............................................................................................. 169
License Status .................................................................................. 170
Account Options ............................................................................... 170
Security Policy ................................................................................ 170

User Management .............................................................................. 170
Users ............................................................................................... 171
User Groups ..................................................................................... 172
Roles ............................................................................................... 173
SSO Settings .................................................................................... 173

Vulnerability Management ................................................................. 174
Watch List Groups .......................................................................... 175
Watch List Subscriptions ........................................................................ 175

Workflow Management .................................................................... 177
Rules ................................................................................................ 177
Default Workflow Rule Examples ..................................................... 181
Ticket Queues .................................................................................. 183
Ticket Status ................................................................................... 184
Ticket Priorities ............................................................................... 184

Assessment ...................................................................................... 185
Update Servers & Daemon .................................................................. 185
Daemon Resources ........................................................................... 185
Daemon and WSUS Troubleshooting ..................................................... 189
Certificate Configuration ................................................................. 192
Certification Authorities ...................................................................... 194
Scan Configuration .......................................................................... 195
Scan Configuration .......................................................................... 196
Microsoft Update Options ............................................................... 196
Add Custom Scan Paths ...................................................................... 197
Downloads ....................................................................................... 198

API .................................................................................................. 199

Logs .................................................................................................. 199
Logins .............................................................................................. 199
Tickets ............................................................................................. 200
Watch Lists ...................................................................................... 200
Email Logs ....................................................................................... 200
SMS Logs ......................................................................................... 200
Service Calls ................................................................................... 200

15 User Profile ................................................................................ 203
16 About Secunia Advisories ................................................................. 205
   CVSS (Common Vulnerability Scoring System) ........................................ 205
   CVSSv3 Score .................................................................................. 206
   CVE References .............................................................................. 208
   Where (Attack Vector) ................................................................... 209
   Criticality (Severity Rating) ............................................................... 210
   Impact (Consequence) ...................................................................... 210

A Appendix A - Threat Intelligence ..................................................... 213
   Evidence of Exploitation ................................................................. 214
   Criteria for the Threat Score Calculation ......................................... 214
   Threat Score Calculation - Examples .............................................. 216
   Threat Intelligence Data for Operations and Security ........................ 218
   Threat Intelligence for Research ..................................................... 218
Flexera’s Software Vulnerability Research is a one-stop solution for vulnerability management. The solution is available via a web-portal, giving you access to all the modules that you are entitled to use according to your subscription.

**Table 1-1 • Software Vulnerability Research Help Library**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong></td>
<td>Flexera’s Software Vulnerability Research combines Vulnerability Intelligence, Assessment, and Patch Creation with Patch Deployment Tool Integration to enable targeted, reliable, and cost-efficient Patch Management.</td>
</tr>
<tr>
<td><strong>Software Vulnerability Research Quick Start Guide</strong></td>
<td>This quick start guide walks you through setting up the key features of Software Vulnerability Research.</td>
</tr>
<tr>
<td><strong>Dashboard</strong></td>
<td>The Dashboard is the default home page that provides you with an overview of vulnerability management processes and gives you access to your latest vulnerability intelligence and advisories. The information is presented with the help of various widgets.</td>
</tr>
<tr>
<td><strong>Notifications</strong></td>
<td>Notifications provide detailed information about alerts you have received and any required actions. The number in the yellow bubble signifies the number of unread notifications.</td>
</tr>
<tr>
<td><strong>Vulnerability Manager</strong></td>
<td>Vulnerability Manager pages are used to manage the Vulnerability Intelligence associated with your account.</td>
</tr>
</tbody>
</table>

*Edition • The Vulnerability Manager module is not available for Software Vulnerability Research - Assessment Only.*
### Table 1-1 • Software Vulnerability Research Help Library (cont.)

<table>
<thead>
<tr>
<th>Topic</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Research</strong></td>
<td>Vulnerability Tracker (VulnTrack) represents our full Vulnerability Database, which has been updated and maintained since the inception of Secunia in 2002.</td>
</tr>
<tr>
<td></td>
<td><strong>Edition</strong> • The Research module is not available for Software Vulnerability Research - Assessment Only.</td>
</tr>
<tr>
<td><strong>Assessment Scenarios</strong></td>
<td>The Assessment Scenarios page provides descriptions of the available assessment scenarios.</td>
</tr>
<tr>
<td></td>
<td><strong>Edition</strong> • This module is not available for Software Vulnerability Research.</td>
</tr>
<tr>
<td><strong>Assessment Reports</strong></td>
<td>The Assessment Reports page displays a tree view of the Device Groups within your environment. The security status of each Device Group is assessed based on <strong>Average System Score</strong>, <strong>Device Details</strong> and <strong>Product Details</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Edition</strong> • This module is not available for Software Vulnerability Research.</td>
</tr>
<tr>
<td><strong>Patching</strong></td>
<td>The Patch Library and Grouped Patch Library pages list the patches available for your environment. Users can create a patch template for deploying patches and can track the patches deployed.</td>
</tr>
<tr>
<td></td>
<td><strong>Edition</strong> • This module is not available for Software Vulnerability Research.</td>
</tr>
<tr>
<td><strong>Policy Manager</strong></td>
<td>The Policy Manager pages are used to configure internal Compliance Policy Rules to associate with your account and view the details of breaches to your policies.</td>
</tr>
<tr>
<td></td>
<td><strong>Edition</strong> • The Policy Manager module is not available for Software Vulnerability Research - Assessment Only.</td>
</tr>
<tr>
<td><strong>Analytics</strong></td>
<td>The Analytics pages are used to filter data contained in the widgets and to create and save dynamic reports on Advisories.</td>
</tr>
<tr>
<td><strong>Ticket Manager</strong></td>
<td>The Ticket Manager page lists all issued tickets. Use this page to:</td>
</tr>
<tr>
<td></td>
<td>• View and Change Tickets Status and Priority</td>
</tr>
<tr>
<td></td>
<td>• Create Tickets in Ticket Manager</td>
</tr>
<tr>
<td></td>
<td>• Delete Tickets in Ticket Manager</td>
</tr>
<tr>
<td></td>
<td>• Default Ticket Statuses in Ticket Manager</td>
</tr>
</tbody>
</table>
Table 1-1 • Software Vulnerability Research Help Library (cont.)

<table>
<thead>
<tr>
<th>Topic</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings</strong></td>
<td>The Settings pages allow the main Administrator account holder to create and manage other accounts.</td>
</tr>
<tr>
<td></td>
<td>This section also tracks details of all activities taken by users related to your account, such as Logins and changes to Tickets, Watch Lists, Email Logs, SMS Logs and Service Calls.</td>
</tr>
<tr>
<td><strong>User Profile</strong></td>
<td>The User Profile page is used to view and edit your account information, including your password, personal details, preferences, and security settings.</td>
</tr>
<tr>
<td><strong>About Secunia Advisories</strong></td>
<td>Describes CVSS (Common Vulnerability Scoring System), CVE References, Where (Attack Vector), Criticality (Severity Rating), and Impact (Consequence).</td>
</tr>
<tr>
<td><strong>Appendix A - Threat Intelligence</strong></td>
<td>Threat Intelligence Module augments Software Vulnerability Research’s vulnerability intelligence with a Threat Score that provides the ultimate prioritization tool for your busy desktop operations teams. This module requires purchase by the user.</td>
</tr>
</tbody>
</table>

**Product Support Resources**

The following resources are available to assist you with using this product:

- Flexera Product Documentation
- Flexera Community
- Flexera Learning Center
- Flexera Support

**Flexera Product Documentation**

You can find documentation for all Flexera products on the Flexera Product Documentation site:

https://docs.flexera.com

**Flexera Community**

On the Flexera Community site, you can quickly find answers to your questions by searching content from other customers, product experts, and thought leaders. You can also post questions on discussion forums for experts to answer. For each of Flexera’s product solutions, you can access forums, blog posts, and knowledge base articles.

https://community.flexera.com

**Flexera Learning Center**

Flexera offers a variety of training courses—both instructor-led and online—to help you understand how to quickly get the most out of your Flexera products. The Flexera Learning Center offers free, self-guided, online training classes. You can also choose to participate in structured classroom training delivered as public classes. You can find a complete list of both online content and public instructor-led training in the Learning Center.

https://learn.flexera.com
Flexera Support

For customers who have purchased a maintenance contract for their product(s), you can submit a support case or check the status of an existing case by making selections on the Get Support menu of the Flexera Community.

https://community.flexera.com

Product Feedback

You can submit feedback about Software Vulnerability Manager in the Flexera Customer Community Forum. You can also submit feedback through the Software Vulnerability Manager user interface by clicking the feedback icon in the upper-right-hand corner of each module.

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:

http://www.flexera.com

You can also follow us on social media:

- Twitter
- Facebook
- LinkedIn
- YouTube
- Instagram
Flexera’s Software Vulnerability Research combines Vulnerability Intelligence, Assessment, and Patch Creation with Patch Deployment Tool Integration to enable targeted, reliable, and cost-efficient Patch Management.

- About Software Vulnerability Research
- Software Vulnerability Editions
- Optional Modules
- The Scan Process – How Does it Work?
- Software Vulnerability Research Life Cycle
- System Architecture Overview
- Vulnerability Assessment of Microsoft Products
- Getting Started with Software Vulnerability Research

About Software Vulnerability Research

Vulnerability Intelligence 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 Research, IT Operations and Security Teams are empowered to take control of the Vulnerability Threat from both Microsoft and non-Microsoft (third-party) product vulnerabilities.

The Software Vulnerability Research Assessment module scanning technology takes a different approach than other vulnerability scanning solutions by conducting non-intrusive scans to accurately identify all installed products and plugins on the system.

Software Vulnerability Research integrates seamlessly with Microsoft® WSUS and System Center Configuration Manager. The solution is available via a web-portal, giving you access to all the modules that you are entitled to use according to your subscription.

The sequence of the module descriptions in this document corresponds with the order in which they are presented in the graphical user interface of the solution.
Note • The available modules, menus and options will vary depending on the permissions granted to you by your Administrator.

Software Vulnerability Editions

Flexera offers the following editions for Software Vulnerability:

• Software Vulnerability Research (Includes all Modules)
• Software Vulnerability Research

The table below describes the differences between the Software Vulnerability editions.

Any module not available for a specific edition will be noted with an Edition Note. See the example below.

Edition • This module is not available for Software Vulnerability Research.

Table 2-1 • User Interface differences between Software Vulnerability Editions

<table>
<thead>
<tr>
<th>Software Vulnerability Research (includes all modules)</th>
<th>Software Vulnerability Research does not include Assessment or Patching</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>Dashboard</td>
</tr>
<tr>
<td>Notifications</td>
<td>Notifications</td>
</tr>
<tr>
<td>Vulnerability Manager</td>
<td>Vulnerability Manager</td>
</tr>
<tr>
<td>Research</td>
<td>Research</td>
</tr>
<tr>
<td>Assessment</td>
<td>Assessment</td>
</tr>
<tr>
<td>Patching</td>
<td>Patching</td>
</tr>
<tr>
<td>Policy Manager</td>
<td>Policy Manager</td>
</tr>
<tr>
<td>Analytics</td>
<td>Analytics</td>
</tr>
<tr>
<td>Ticket Manager</td>
<td>Ticket Manager</td>
</tr>
<tr>
<td>Settings</td>
<td>Settings</td>
</tr>
<tr>
<td>User Profile</td>
<td>User Profile</td>
</tr>
</tbody>
</table>

Main Menu
Optional Modules

Flexera offers the following optional modules:

- Software Vulnerability Research - Threat Intelligence Module

**Threat Intelligence Module**

When added to our Software Vulnerability Research solution, the Threat Intelligence Module helps operations to focus on the patches most critical to the security of the software deployed in your environment. When added to our Software Vulnerability Research (SVR) solution, the Threat Intelligence Module provides security professionals even more insight by exposing threat scores not only for security advisories, but for the specific CVEs associated with those advisories as well as what evidence was triggered to arrive at the provided threat score.

*Tip* • For more details about the Threat Intelligence Modules, see the following data sheet:


**The Scan Process – How Does it Work?**

The first step in scanning a system is to collect specific metadata from primarily .EXE, .DLL, and .OCX files on the system being scanned. Metadata is generic non-sensitive text strings embedded in the binary files from the vendors of the products. This data is collected and then sent to our Secure Data Processing Cloud where it is processed and parsed.

The data is then matched against our File Signatures, which are rules that match the raw metadata to an actual product installation.

Part of this matching process also results in an exact version being extracted from the metadata. This means that after the initial parsing Software Vulnerability Research knows exactly which products are on the system and their exact version – a precise inventory of software on the system.

The inventory of software is then compared against the unique Secunia Advisory and Vulnerability Database, which contains the most accurate and current Vulnerability Intelligence available.

The result is a precise inventory of products, their versions, the security state of each, along with a direct reference to any corresponding Secunia Advisory detailing the exact vulnerabilities and their Secunia assessed criticality and impact.

Since the scan process works by looking at the actual files on the system being scanned, the result is extremely reliable as a product cannot be installed on a system without the actual files required being present.
This in turn means that Software Vulnerability Research rarely identifies false-positives, and you can use the results from Software Vulnerability Research immediately without doing additional data mining.

For further information about the different Software Vulnerability Research scanning approaches, see Assessment Scenarios.

**Software Vulnerability Research Life Cycle**

Software vulnerability management is a critical component of any security infrastructure because it enables proactive detection and remediation of security vulnerabilities.

A process to identify vulnerable products, including products not authorized in an organization’s environment, paired with effective patch management is an absolute must to reduce the window of exposure and eliminate the root cause of a potential compromise.

Software Vulnerability Research automates all steps of the software vulnerability management life cycle, allowing you to strengthen the security of your networks.

![Software Vulnerability Research Lifecycle](image)

**Figure 2-1:** Software Vulnerability Research Lifecycle

**System Architecture Overview**

The following screenshot provides an overview of the Software Vulnerability Research system architecture.
Vulnerability Assessment of Microsoft Products

For Windows and other Microsoft products, Software Vulnerability Research obtains information about missing Microsoft security updates from the scanned device’s local Windows Update Agent.

If the Windows Update Agent is managed by the company’s IT department, the Microsoft security update has to be approved by the IT administrator before Software Vulnerability Research will report whether it is missing or not.

Getting Started with Software Vulnerability Research

See Software Vulnerability Research Quick Start Guide to help you set up the key features of Software Vulnerability Research.
Chapter 2  Introduction
Getting Started with Software Vulnerability Research
This Quick Start guide walks you through setting up the key features of Software Vulnerability Research:

- Account Activation
- Opening a Support Case
- System Requirements for Software Vulnerability Research
- Scan Configuration
- Agent Deployment
- Daemon Deployment
- Smart Group Configuration
- Workflow Management Rules
- Patching

**Account Activation**

This section takes you through the steps to securely create your Software Vulnerability Research account:

- Accept the Flexera Sales Token and Create Your Account
- Configure Two-Factor Authentication (2FA)
- Configuring Single Sign-On (SSO)

**Accept the Flexera Sales Token and Create Your Account**

To create your account, perform the following steps.
**Task**

To accept the Flexera Sales Token and Create your Software Vulnerability Research account:

1. After your sales order is complete, you will receive an activation email from Flexera Sales with a customized link to create your account. The link looks similar to the following token:

   https://app.flexerasoftware.com/trial/?token=xxxxxx

   Your activation email from Flexera includes the particular token number. Click the token link to begin the initial setup process for the main Administrator account. The following window will appear:

   ![Image of the initial setup process](image.png)

2. After completing the relevant details that are mandatory for the creation of your account, click Request Trial Account.

3. Go to your email’s inbox and find the verification link sent by Flexera. Click the verification link, and a new window will open for you to create your account’s user name and password.
Important • Before you enter any passwords, consider the default password rules required by Flexera:
- 8-200 characters
- At least one lowercase letter
- At least one uppercase letter
- At least one digit

Important • You should also consider the following recommendations for creating account passwords:
- No common passwords
- No personal details
- No old passwords
- Passwords created by a password generator

4. After entering your username and password, click Create Trial Account. You will then be taken to the Software Vulnerability Research Login page where you login with the previously configured credentials. When logging in to your account for the first time, you will be asked to Configure Two-Factor Authentication (2FA) to secure the account. You must configure 2FA before you are allowed to login, as two-factor authentication is mandatory.

Logging In to Software Vulnerability Research

If you already have a Software Vulnerability Research account and want to login, perform the following steps.
To login to Software Vulnerability Research:

1. Open the Software Vulnerability Research Login page and enter your username and password.
2. If you have forgotten your password, click Forgot your password? Enter your email address and click Send mail to receive instructions to reset your password.

Configure Two-Factor Authentication (2FA)

To secure your account in the event that the account password has been compromised, two-factor authentication (2FA) is mandatory.

Software Vulnerability Research allows the following 2FA configuration options:

- **Token-Based Two-Factor Authentication**
- **SMS-Based Two-Factor Authentication**

![Figure 3-1: Choosing a Two-Factor Authentication Method](image)

Token-based two-factor authentication is the default and recommended option.

In case your phone is lost or compromised, two-factor authentication can be reset. The reset method varies by account type. For details, see Two-Factor Authentication Recovery.

Token-Based Two-Factor Authentication

To use token-based two-factor authentication, you first need to install an application specific to your device. Flexera's Software Vulnerability Research uses the standard Time-Based On-Time Password Algorithm (TOTP) for token-based two-factor support, which is supported by applications like Google Authenticator or Duo by Cisco.

- **Android devices**—Download the Google Authenticator application from the Google Play Store:
  

- **iOS devices**—Download the Google Authenticator, available under iTunes in the App Store:
  

Logging Into Your Account Using Two-Factor Authentication

To login to your account using two-factor authentication, perform the following steps.
<table>
<thead>
<tr>
<th>Task</th>
<th>To log in to your account the first time with token-based two-factor authentication:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>After entering your username and password, you will be presented with a QR code and a field for the verification code.</td>
</tr>
<tr>
<td>2.</td>
<td>Open the Google Authenticator application and select the <strong>Scan a Barcode</strong> option.</td>
</tr>
<tr>
<td>3.</td>
<td>When the application loads the device camera, scan the QR barcode displayed on your computer screen.</td>
</tr>
<tr>
<td>4.</td>
<td>The mobile application will generate a unique code. Enter this code in the <strong>Verification Code</strong> field at the Software Vulnerability Research <strong>Login</strong> page.</td>
</tr>
<tr>
<td>5.</td>
<td>Click <strong>Save</strong> to proceed with logging in to your new account.</td>
</tr>
</tbody>
</table>

**SMS-Based Two-Factor Authentication**

SMS-based two-factor authentication is a less secure and a less reliable method that is available and can be used as a fallback in case your phone does not have an authenticator application.

- Logging in the First Time
- Logging in Subsequent Times
Logging in the First Time

Task To log in to your account the first time with SMS-based two-factor authentication:

1. At the Software Vulnerability Research two-factor authentication window, select SMS and click Next.

2. Enter your phone number in international format, starting with a +.

3. Click Send an SMS.

4. Once the SMS arrives, enter the code it contains on the Software Vulnerability Research Login page and click Verify Token.

Logging in Subsequent Times

Task To log in to your account with SMS-based two-factor authentication for all future logins:

1. After you are asked for the authentication Token, click Send SMS.

2. Once the SMS arrives, enter the code on the Software Vulnerability Research Login page and click Log in.

Two-Factor Authentication Recovery

In case your phone is lost or compromised, two-factor authentication can be reset. The reset method varies by account type.

- Recovering Two-Factor Authentication for Main Administrator Accounts
- Recovering Two-Factor Authentication for User Accounts

Recovering Two-Factor Authentication for Main Administrator Accounts

Two-factor authentication for the main Administrator account can be reset by our Support department after verifying the identity of the account holder.

Recovering Two-Factor Authentication for User Accounts

For User accounts, two-factor authentication can be reset by the main Administrator directly from Software Vulnerability Research. In the Settings module, go to User Management > Users. Expand the appropriate user row and click Reset two factor login. It is recommended to verify first the identity of the user requesting the reset.
Configuring Single Sign-On (SSO)

Note • The following information is unique to the single sign-on vendor Okta (SAML 2.0). Single sign-on procedures from other vendors may vary.

Task To set up Okta (SAML 2.0) to use as a single sign-on (SSO) with Software Vulnerability Research:

1. Sign in to Okta.
2. Create an admin account.
3. Click Create New App to create a new Okta SSO app.
4. Choose Web for the Platform and SAML 2.0 for the Sign on method. Then click Create.
5. Enter an **App name** (Example: SVM) and **App logo** (Example: see Software Vulnerability Research logo below). Then click **Next**.

6. Copy the following from the Software Vulnerability Research **Settings > User Management > Single Sign On** fields and paste in the **Okta SAML Settings >** fields:
   - Single Sign On URL (Same with Recipient URL and Destination URL) to Single sign on URL and Audience URL (SP Entity ID)
• Account Key to accountKey Value

Complete the remaining Okta SAML Settings > Attribute Statements (Optional) name and value fields using the field’s drop-down list:

• firstName
• lastName
• email
• username

7. Click (if not already selected) I’m an Okta customer adding an internal app for the Create SAML Integration - Step 3 Feedback screen. You can leave the rest of the fields blank.
8. At the Okta Sign On Settings screen, click the **Identity Provider metadata** link.
9. Copy the **Identity Provider metadata** URL from Okta into the Software Vulnerability Research **Settings > User Management > Single Sign On > IDP Metadata URL** field. Check **SSO Enabled**, check **Automatically create new users**, and assign a **Default group for new users**.

**Note** • For a secure connection, the **Assertions Signed (or similarly named)** setting should be enabled on your IDP.

10. If you want to disable standard login options for all of your users (except root), select the **Disable standard login option** under **Settings > User Management > SSO Settings > Service Provider Configuration**.

11. Click **Save** to on the **Settings > User Management** page.
Chapter 3  Software Vulnerability Research Quick Start Guide

Account Activation

**Important** • Before selecting this option, make sure that SSO is working correctly, to prevent user lockout.

12. Add Software Vulnerability Research users to the Okta SSO account.

13. Assign Software Vulnerability Research users to the Okta SSO app. A reset password link is sent to each user.

14. Users open the reset password link, reset their password, and click open the Okta SSO application.

15. Users are then logged into the Software Vulnerability Research Login page.

**Important** • For security purposes, Software Vulnerability Research has a session timeout that will log you off after 2 hours of inactivity.
Opening a Support Case

If you have any questions or concerns regarding your Software Vulnerability Research account, please open a support case via Flexera’s Customer Community. For more information, see:


System Requirements for Software Vulnerability Research

The Software Vulnerability Research User Interface will resize and adapt when being used on different devices. You can access the system from anywhere using any device, such as a smartphone or tablet.

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

Table 3-1 • System Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor resolution</td>
<td>The minimum resolution required is 1280 x 1024.</td>
</tr>
<tr>
<td>Browser</td>
<td>The following browsers are supported:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Edge</td>
</tr>
<tr>
<td></td>
<td>• Apple Safari</td>
</tr>
<tr>
<td></td>
<td>• Google Chrome</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Edge</td>
</tr>
<tr>
<td></td>
<td>• Mozilla Firefox</td>
</tr>
<tr>
<td></td>
<td>• Opera</td>
</tr>
<tr>
<td>Internet connection</td>
<td>Internet connection capable of connecting to <a href="https://app.flexerasoftware.com/">https://app.flexerasoftware.com/</a> is required.</td>
</tr>
<tr>
<td>Allow Listed sites</td>
<td>The following addresses should be Allow-listed in the Firewall/Proxy configuration:</td>
</tr>
<tr>
<td></td>
<td>• https://*.secunia.com/</td>
</tr>
<tr>
<td></td>
<td>• crl.verisign.net</td>
</tr>
<tr>
<td></td>
<td>• crl.thawte.com</td>
</tr>
<tr>
<td></td>
<td>• <a href="http://crl3.digicert.com">http://crl3.digicert.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="http://crl4.digicert.com">http://crl4.digicert.com</a></td>
</tr>
<tr>
<td></td>
<td>• http://*.ws.symantec.com</td>
</tr>
<tr>
<td>First-party cookie settings</td>
<td>First-party cookie settings should be set to at least Prompt (in Internet Explorer).</td>
</tr>
</tbody>
</table>
Chapter 3  Software Vulnerability Research Quick Start Guide

Scan Configuration

To control when and how Software Vulnerability Research agents, that are installed and running as a services, collect data, perform the following steps.

Task To control when and how Software Vulnerability Research agents collect data:

1. Log in to https://app.flexerasoftware.com/login/?next=/
2. Go to https://app.flexerasoftware.com/#/settings/env/scan/
3. The panel allows you to configure when and what you scan. By default, we scan daily at midnight (during the local agent host’s time zone). See Scan Configuration for further details.

Agent Deployment

This section details the following agent deployment methods:

- Deploy a Windows Agent
- Deploy a Mac Agent
- Deploy a Linux Agent
- Deploy the Windows Agent Application through Microsoft’s System Center Configuration Manager (SCCM)
- Run Windows Agent through the Microsoft System Center as a Task Sequence
- Deploy a Windows Agent through Microsoft’s Windows Server Update Services (WSUS)

Table 3-1 • System Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session cookie settings</td>
<td>The option to allow session cookies should be selected.</td>
</tr>
<tr>
<td>PDF reader</td>
<td>A PDF reader is required.</td>
</tr>
</tbody>
</table>

Important • The listed required URLs are absolutely mandatory as they relate to Certificate Validation of the non-repudiated SSL certificates, which guarantee that communication between your network and the Cloud is not intercepted, redirected, or modified in any way by a third-party.

Important • The Software Vulnerability Research IPs are subject to change without notice, and you should not lock access to Software Vulnerability Research based on the current IP, but should rely on the SSL and certificate validation instead.
Deploy a Windows Agent

These deployment instructions explain how to install the Software Vulnerability Research Agent on a single Windows machine, where the agent will run as a service and report back to the Software Vulnerability Research server on a daily basis.

Before deploying the Windows Agent, see the prerequisites in Agent-Based Scan – Requirements for Windows.

Task To deploy a Windows Agent:

1. Log in to https://app.flexerasoftware.com/login/?next=/
2. In the Settings module, go to Assessment > Downloads. For details see, Downloads.
3. Download the Vulnerable Software Discovery Tool Installer for Windows.
4. Run the SVMScanInstall.msi on a Windows machine you wish to scan. This step will set the Agent up to run as a service.
5. Follow the scan settings you have configured in the Scan Configuration (https://app.flexerasoftware.com/#/settings/env/scan/). There are no configuration options to set during installation. In about 30 minutes, you should see the first set of scan results in the Software Vulnerability Research website.

Deploy a Mac Agent

The Vulnerable Software Discovery Tool for Mac (svmscan_macos) is a small, simple, customizable and extremely powerful scan engine that offers a fully featured command line interface (CLI) for scanning functionality.

This CLI allows you to run scans directly from the command line, or to launch scans by using the Software Vulnerability Research console.

Important • Ensure that the Vulnerable Software Discovery Tool for Mac is always available in a local folder on the target host.

Before deploying the Mac Agent, see the prerequisites in Agent-Based Scan – Requirements for Mac OS X.

Task To deploy a Mac Agent:

1. Log in to https://app.flexerasoftware.com/login/?next=/
2. In the Settings module, go to Assessment > Downloads. For details see, Downloads.
3. Download the Vulnerable Software Discovery Tool for Mac.
4. Click svmscan_macos.dmg to download the Mac.
5. Double-click on downloaded dmg to view the contents. To save, drag and drop it to the preferred location.

6. Open a Terminal window and run the following commands:
   ```
cd Downloads/
To install:
sudo ./svmscan_macos -i
   ```

7. Enter your administrator password. Then you should get information like this.

![Terminal output](image)

In about 30 minutes, you should see the first set of scan results in the Software Vulnerability Research website.

**Note** • To un-install run the following command.

```
./svmscan_macos.dmg -r
```

### Deploy a Linux Agent

Red Hat Enterprise Linux (RHEL) 7 is the only operating system officially supported by Flexera for the Vulnerable Software Discovery Tool for Red Hat Linux 7 RPM. It may be possible to install the scan Agent on operating systems and configurations other than those described. However, these have not been tested and are not supported by Flexera.

The scan Agent for RHEL uses the inventory which is already present (RPM) and displays this in Software Vulnerability Research after being processed by Flexera Detection/Version Rules.

Before deploying the Linux Agent, see the prerequisites in Agent-Based Scan – Requirements for Red Hat Enterprise Linux (RHEL).
**Task**

**To deploy a Linux Agent:**

1. Log in to https://app.flexerasoftware.com/login/?next=/

2. In the Settings module, go to **Assessment > Downloads**. For details see, **Downloads**.

3. Based on your version of Red Hat Linux, download the appropriate **Vulnerable Software Discovery Tool for Red Hat Linux**.

4. Open a terminal session and run the following commands.

   **Note** • Your file name may be different depending on the agent version you downloaded.

   cd Downloads/
   sudo yum install svmscan_linux-8.0.345-1.el7.x86_64.rpm

5. Enter your administrator password.

6. If the following prompt appears, enter **y** if the installation is OK.

   **Note** • To un-install run the following command.
Deploy the Windows Agent Application through Microsoft’s System Center Configuration Manager (SCCM)

To deploy the Windows agent application (SVMScanInstall.msi) through System Center Configuration Manager, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To deploy the Windows Agent Application through SCCM:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Download the Windows Agent Application (SVMScanInstall.msi) from Software Vulnerability Research under Settings &gt; Assessment &gt; Downloads.</td>
</tr>
<tr>
<td>2.</td>
<td>Move the installer into a source package directory on the SCCM server.</td>
</tr>
<tr>
<td>3.</td>
<td>Open the Configuration Manager Administration Console and browse to Software Library.</td>
</tr>
<tr>
<td>4.</td>
<td>Click Applications and right-click the central window to Create Application.</td>
</tr>
<tr>
<td>5.</td>
<td>If you get any errors to browse and attach the SVMScanInstall.msi to the new application wizard while you’re browsing through shared directories on the local server, use instead the UNC path of the file.</td>
</tr>
<tr>
<td>6.</td>
<td>Open the General Information page to set up the primary configuration of your package, including the Installation parameters.</td>
</tr>
<tr>
<td>7.</td>
<td>Set the installation command: msiexec /i &quot;SVMScanInstall.msi&quot; /q</td>
</tr>
<tr>
<td></td>
<td>If you wish, append extra logging with: /L c:\agent.log</td>
</tr>
</tbody>
</table>
8. Finish the application wizard. Find your new application displayed under the Applications menu in the Software Library of the Configuration Manager Console.

9. Right-click the application name and select Distribute Content. Select your distribution point and then complete that wizard too.

10. Right-click your new application once again and select Deploy to enable your clients to install the application package containing the SVMScanInstall.msi installer file.

11. Target your Agent package to the necessary device collections you wish to deploy your package to.

12. Under Deployment Settings, select Required if you want your application to be deployed with maximum priority as soon as possible.

13. Select Available to allow users to interact with the application and install it through the Software Center. Click Next to finish the wizard and deploy the application.

14. On the receiving end, open the Control Panel and then the Configuration Manager Client. Run the Machine Policy Retrieval & Evaluation Cycle and the Application Deployment Evaluation Cycle to sync and install the Agent application on the local machine.
Check for More Detailed Steps

More detailed steps can be requested from Flexera’s Software Vulnerability Research Technical Support Team.

Run Windows Agent through the Microsoft System Center as a Task Sequence

To run the Software Vulnerability Research Agent from the Microsoft System Center as a scheduled task, see the steps below. No agents will be installed, and you will only need to maintain one agent binary. To stagger the scanning of multiple machines within a system, see Randomize the Agent Scan Schedule.

- Running the Vulnerable Software Discovery Tool Inside an SCCM Package
- Creating the Initial Scan and Weekly Reoccurring Scan

Running the Vulnerable Software Discovery Tool Inside an SCCM Package

To run the Vulnerable Software Discovery Tool inside an SCCM package, perform the following steps.

**Task**

**To run the Vulnerable Software Discovery Tool inside an SCCM package:**

1. Open the Software Vulnerability Research console. From **Settings > Assessment > Downloads**, download the latest SVRScan.exe file and place it into a deployment share.
Note • Make sure to right click on the .exe in the deployment share to “Unblock” it. Click Apply > OK.

2. Launch the ConfigMgr console. Select Software Library > Application Management > Packages.

3. From the ribbon, click Create Package.

4. Complete the package information and click Next.
5. On the **Program Type** page, ensure **Standard Program** is selected and click **Next**.

6. On the **Standard Program** page, configure the following settings and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter SVM Vulnerable Software Discovery Tool.</td>
</tr>
<tr>
<td><strong>Command Line</strong></td>
<td>Enter the following: SVMScan.exe -c - v -d c:\windows\temp\svmscan.log</td>
</tr>
<tr>
<td></td>
<td>This command line creates a scan log file up to 16 MB in size.</td>
</tr>
<tr>
<td><strong>Run</strong></td>
<td>Set to <strong>Hidden</strong>.</td>
</tr>
<tr>
<td><strong>Program can run</strong></td>
<td>Select <strong>Whether or not a user is logged on</strong>.</td>
</tr>
</tbody>
</table>
7. On the **Requirements** page, complete the requirements as shown below and click **Next**.
8. Finish the wizard.

9. Distribute the package to all Distribution Points or groups using the Distribute Content feature.

Creating the Initial Scan and Weekly Reoccurring Scan

To create the initial scan and the weekly reoccurring scan, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To create the initial scan and the weekly reoccurring scan:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select the Package and click Deploy on the ribbon.</td>
</tr>
<tr>
<td>2.</td>
<td>On the General page, select the target collection and click Next.</td>
</tr>
<tr>
<td>3.</td>
<td>On the Content page, verify that the content is distributed and click Next.</td>
</tr>
<tr>
<td>4.</td>
<td>On the Deployment Settings page, ensure the purpose is Required and click Next.</td>
</tr>
<tr>
<td>5.</td>
<td>On the Scheduling page, in the Assignment schedule click New. Schedule a scan for as soon as possible and create a weekly scanning schedule. Also configure the Rerun behavior deployment to Always rerun program.</td>
</tr>
</tbody>
</table>
**Tip** • For larger environments, it is recommended to spread out the execution schedule of the scan package to avoid spikes of network traffic.

6. On the user **Experience** page, click **Next**.

7. On the user **Distribution Points** page, select **Download content**, and click **Next**.
8. Finish the wizard.

You can now monitor the scanning results from the Software Vulnerability Research console. To stagger the scanning of multiple machines within a system, see Randomize the Agent Scan Schedule.

Randomize the Agent Scan Schedule

To set up a random scan schedule to stagger the scanning of multiple machines within a system, the following command line applies to all platforms:

```
SVMScan.exe -c -si <scan interval upper limit>
```

“si” represents the scan interval, and the scan interval’s upper limit can be set up by the number of minutes.

For example, `SVMScan.exe -c -si 50` would mean that the scanning agent will start scanning after a delay of random minutes, which could be from 1 to 50 minutes.

Deploy a Windows Agent through Microsoft’s Windows Server Update Services (WSUS)

When you deploy the Software Vulnerability Research Windows Agent through Microsoft’s WSUS, the Windows Agent is installed on machines that report into WSUS, is scheduled to run as a service, and reports results back daily.
Task To deploy a Windows Agent through WSUS:

1. If not already done, install and configure the Software Distribution Daemon for Windows. See Daemon Deployment and Install the Daemon.

2. To view the Daemon’s status page, go to Settings > Assessment > Update Servers & Daemon. After you click a Daemon, select one of the following options: More Info, Schedule Refresh, View Servers & Groups, Deploy Daemon, Delete Daemon, and Disable Daemon.

   • Select the More Info option to see Daemon information like the screen capture below. The Last Connected time stamp confirms whether the Daemon has reported recently, which is usually an indicator for good health. To sign packages externally, click Sign Packages manually. By default, it is set to Automatic.

   • Select View Servers & Groups to display the Software Vulnerability Research instance your Daemon has been integrated with.

3. To publish an Agent Deployment package to WSUS and to select the server and corresponding computer groups it maintains, select Deploy Agent.

   In theory and practice, you can have multiple Daemons set up in multiple networks connected to multiple deployment servers. You can also select your package to be published to multiple deployment servers simultaneously in a centralized fashion.
Daemon Deployment

The Software Distribution Daemon has to be installed and configured to publish patches (see Patching) as software updates to WSUS. It runs as a background service with no user interaction. It doesn’t have to be installed on the WSUS server, but the host must be the exact same operating system version and patch level. For details, see the Daemon Software Requirements.

The account that runs the Daemon must have:

- Run-as Service privileges
- Windows Server Update Services Administrator privileges

This section details the following daemon deployment activities:

- Install the Daemon
- Add a Digital Certificate to Windows Server Update Services (WSUS)
- Create a Group Policy to Deploy Your Certificate

For additional Windows Server Update Services (WSUS) and daemon information, see Update Servers & Daemon.

Install the Daemon

To install the daemon, perform the following steps.

1. Log in to https://app.flexerasoftware.com/login/?next=/
2. In the Settings module, go to Assessment > Downloads. For details see, Downloads.
3. Download the Software Distribution Daemon for Windows.
4. Identify the machine to host the SVM Daemon. This machine must have access to your company’s Windows Server Update Services (WSUS) server and must have the Windows Remote Server Administration Tools installed. The daemon runs in the background of this machine and acts as the host to receive patch data from the Software Vulnerability Research web server and to deploy the patches to your company’s WSUS server.
5. Run the Installer.
6. Enter the server name, scheme, port, and credentials to your WSUS server.
7. Click Install.

8. After the daemon is installed (wait about 10 minutes), you should see the daemon appear in the Software Vulnerability Research web server.

9. The best way to test to ensure the daemon is communicating correctly is to click View Servers & Groups. You should see a list of computers your WSUS server can talk to.

At this point, the daemon is configured. Before you can deploy patches, you must Add a Digital Certificate to Windows Server Update Services (WSUS), and then ensure that certificate is trusted by all machines you wish to deploy patches to.
Add a Digital Certificate to Windows Server Update Services (WSUS)

Before you can deploy third-party patches in WSUS, you must prepare the WSUS server.

Task To add a Digital Certificate to WSUS:

1. Create the following Registry Key:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Update Services\Server\Setup]
"EnableSelfSignedCertificates"=dword:00000001
```

2. Add a Code Signing Digital Certificate to WSUS.

You have two options:

- Add a Code Signing Digital Certificate you already have to WSUS
- Have the Daemon generate a new code signing certificate

Add a Code Signing Digital Certificate you already have to WSUS

Open a command prompt and enter (replace `<pfxFile>` with a path to your pfx file and replace `[password]` with the pfx file password):

```
cd "c:\Program Files\Flexera Software\SVM Daemon"
svmpd.exe UseCert <pfxFile> [password]
```

Have the Daemon generate a new code signing certificate

Open a command prompt and enter:

```
cd "c:\Program Files\Flexera Software\SVM Daemon"
svmpd.exe NewCert
```

Once you have added a certificate, you need to deploy the certificate to machines that will receive the patches (they need to trust the patches from WSUS). See the next topic for this.

Create a Group Policy to Deploy Your Certificate

This section describes how to create a Group Policy Object (GPO) for WSUS by using the Group Policy Management console. Once the GPO is created and linked to the correct Organizational Unit (OU), the computers in that OU will download the WSUS publisher self-signed certificate and Windows settings so that third-party updates can be downloaded correctly.
Task | To create a Group Policy Object (GPO):
--- | ---
1. | Connect to the WSUS server and click **Next**.
2. | When the “Export Signing Certificate” pop-up appears, click **OK** to save certificates to your documents folder.
3. | Launch the Group Policy Management Console on your Domain Controller.
4. | Navigate to **Group Policy Management > Forest > Domains > Organizational Unit**.
5. | Right-click the **Organizational Unit > Create a GPO** in this domain, and Link it here > **Name the GPO** such as “SVM-WSUS” or as per your policy.
6. | Right-click the GPO and click **Edit**.
8. | Import the previously exported “wsuskey.cer” Certificate in the ”Trusted Root Certification Authorities” and ”Trusted Publishers” Folders.
10. | Double-click the Windows Update Folder.
11. | Double-click **Specify Intranet Microsoft update service location** and change the Settings to **Enabled**. Specify your WSUS server address on **Set the intranet update service for detecting updates** and click **Apply**.
Note • This setting should only be changed if you are using WSUS. Don’t configure this setting if you are using SCCM.

If you have another GPO which points your machines to the correct WSUS server, then re-specifying WSUS is not required.

12. Double-click **Allow signed updates from an intranet Microsoft update service location** and change the **Settings** to **Enabled**.

13. Click **Apply > OK** and close the GPO editor.

Computers will download the Policy after the next policy refresh interval or reboot. You can force the policy to apply by running the command:
gpupdate /force

Sometimes it may take several hours for the policy to actually propagate. You can verify that the GPO is being applied to the machine by checking to see if the certificates have been added to the appropriate certificate stores on any given machine.

If the GPO has not been applied yet, or it is not being applied to the machine in question, then you will receive an error (0x800b0109) when deploying third-party updates.

**Smart Group Configuration**

Smart Groups are powerful reporting tools that can be customized to deliver a valuable overview of the software vulnerability exposure of your clients, networks, and products. You can create a Smart Group in the Assessment module of Software Vulnerability Research.

This section includes the following Smart Group topics:

- Conditions and Logic Operators
- Simple Smart Groups
- Advanced Smart Groups
- Additional Smart Group Information

### Conditions and Logic Operators

Smart Groups can be saved when there is one or more conditions configured with their corresponding logic operators and values. You can create as many Smart Groups as you need, as long as you don’t repeat the same condition and logic combination twice within a single smart group.

Smart Group configuration consists of 21 conditions, which are sorted into three primary categories: Device, Product, and Advisory. Many of the conditions include one or more logic operators, which allow you to further customize your use cases.
Simple Smart Groups

Before creating a Simple Smart Group, you should consider the scenario you want to report on and know the particular conditions of your use case. For example, insecure status, product name, network location, and attack vector are all conditions that can be used on its own to report a great deal of valuable information.

Smart Groups that contain a single condition are simple by design, but they can deliver great insight on devices and network, products and vulnerabilities.

The following are Simple Smart Group examples that contain one condition:

**Table 3-2 • Simple Smart Group Examples**

<table>
<thead>
<tr>
<th>Smart Group</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show all Insecure Products or EOL</td>
<td>Product Secure Status = Insecure / EOL</td>
</tr>
<tr>
<td>Show Windows devices managed by me</td>
<td>Device Platform = Windows</td>
</tr>
<tr>
<td>Monitor a specific program version</td>
<td>Product Version Name = Flash 31.x</td>
</tr>
<tr>
<td>See sum of devices and programs under a specific organizational unit (OU)</td>
<td>Device Active Directory = DC=Clients, DC=domain, DC=com</td>
</tr>
<tr>
<td>See all vulnerable software from a Remote attack vector</td>
<td>Advisory Where = From Remote</td>
</tr>
</tbody>
</table>

Advanced Smart Groups

Advanced Smart Groups usually represent a use case scenario with multiple logic conditions being true.

If you take the five Simple Smart Groups illustrated above and configure all of them under one single Smart Group, you will achieve an Advanced Smart Group.

For example, the Advanced Smart Group shown in the screen shot below will report on Insecure Flash 31.x with attack vector From Remote on PCs in the Workstations OU of my domain.
The more specific you are in the search you perform, the more specific the results will be that you get back from the vulnerability database of your account, which manages your Smart Group queries.

Additional Smart Group Information

For additional Smart Group information, see:

- Smart Group Selection Order
- Create a Smart Group
- Create a Smart Groups Report

Workflow Management Rules

In Software Vulnerability Research under Settings > Workflow Management > Rules, you can create rules that partially or fully automate workflow.

Rules can only be created by an Administrator and must contain at a minimum one trigger and one action. For a list of triggers and actions, see Rule Channels, Triggers, and Actions. If needed, you can configure many different options into one rule.

This section includes the following Workflow Management Rule topics:

- Create a Workflow Rule - Overview
- Rule Triggers
- Patch Rule Actions
- Notification Actions
Create a Workflow Rule - Overview

To create a workflow rule, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To create a Workflow Rule:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click + to create a new Workflow Rule.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter the Rule name and click Choose Rule Trigger. For details, see Rule Triggers.</td>
</tr>
<tr>
<td>3.</td>
<td>Select the channel and trigger from the drop-down lists and click Save. An Add Action icon will appear. For an example, see Patch Rule Actions.</td>
</tr>
<tr>
<td>4.</td>
<td>Select the action to be taken from the drop-down list when the rule is triggered and click Save. Add any additional actions required and save the rule.</td>
</tr>
<tr>
<td>5.</td>
<td>Select the appropriate rule Notification. If you choose to send an email or SMS, you can select multiple users or broadcast groups for the email or SMS notification by clicking the appropriate user names or broadcast groups. A check mark will appear next to the selected users or broadcast groups. The selected user names will appear in the Users field; the selected broadcast groups will appear in the Broadcast to Groups field. For details, see Notification Actions.</td>
</tr>
<tr>
<td>6.</td>
<td>Click Edit to change and to Enable or Disable a rule.</td>
</tr>
</tbody>
</table>

Rule Triggers

Within a given rule, select one of the following Rule Triggers: Advisory, Analytics, Patch, Policy, Release, Ticketing, and User management.
For example, if you select Patch as the subject of your desired workflow, you must choose one patch rule trigger:

**Table 3-3 • Patch Rule Trigger Options**

<table>
<thead>
<tr>
<th>Option 1: Patch ready for manual signing</th>
<th>Option 2: Patch available with template, affecting my environment = Yes, Not Critical or Above</th>
<th>Option 3: Patch available without template, affecting my environment = Yes, Not Critical or Above</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option 1: Patch ready for manual signing</td>
<td>Option 2: Patch available with template, affecting my environment = Yes, Not Critical or Above</td>
<td>Option 3: Patch available without template, affecting my environment = Yes, Not Critical or Above</td>
</tr>
<tr>
<td>Patch ready for manual signing</td>
<td>Patch available with template, affecting my environment = Yes, Not Critical or Above</td>
<td>Patch available without template, affecting my environment = Yes, Not Critical or Above</td>
</tr>
<tr>
<td>Package ready for manual signing</td>
<td>Package available with template</td>
<td>Package available without template</td>
</tr>
<tr>
<td>Package ready for manual signing</td>
<td>Package available with template</td>
<td>Package available without template</td>
</tr>
<tr>
<td>Patch ready for manual signing</td>
<td>Patch available with template, affecting my environment = Yes, Not Critical or Above</td>
<td>Patch available without template, affecting my environment = Yes, Not Critical or Above</td>
</tr>
<tr>
<td>Patch ready for manual signing</td>
<td>Patch available with template, affecting my environment = Yes, Not Critical or Above</td>
<td>Patch available without template, affecting my environment = Yes, Not Critical or Above</td>
</tr>
<tr>
<td>Package ready for manual signing</td>
<td>Package available with template</td>
<td>Package available without template</td>
</tr>
<tr>
<td>Patch ready for manual signing</td>
<td>Patch available with template, affecting my environment = Yes, Not Critical or Above</td>
<td>Patch available without template, affecting my environment = Yes, Not Critical or Above</td>
</tr>
<tr>
<td>Patch ready for manual signing</td>
<td>Patch available with template, affecting my environment = Yes, Not Critical or Above</td>
<td>Patch available without template, affecting my environment = Yes, Not Critical or Above</td>
</tr>
<tr>
<td>Package ready for manual signing</td>
<td>Package available with template</td>
<td>Package available without template</td>
</tr>
<tr>
<td>Patch ready for manual signing</td>
<td>Patch available with template, affecting my environment = Yes, Not Critical or Above</td>
<td>Patch available without template, affecting my environment = Yes, Not Critical or Above</td>
</tr>
<tr>
<td>Package ready for manual signing</td>
<td>Package available with template</td>
<td>Package available without template</td>
</tr>
<tr>
<td>Patch ready for manual signing</td>
<td>Patch available with template, affecting my environment = Yes, Not Critical or Above</td>
<td>Patch available without template, affecting my environment = Yes, Not Critical or Above</td>
</tr>
<tr>
<td>Package ready for manual signing</td>
<td>Package available with template</td>
<td>Package available without template</td>
</tr>
<tr>
<td>Patch ready for manual signing</td>
<td>Patch available with template, affecting my environment = Yes, Not Critical or Above</td>
<td>Patch available without template, affecting my environment = Yes, Not Critical or Above</td>
</tr>
<tr>
<td>Package ready for manual signing</td>
<td>Package available with template</td>
<td>Package available without template</td>
</tr>
<tr>
<td>Patch ready for manual signing</td>
<td>Patch available with template, affecting my environment = Yes, Not Critical or Above</td>
<td>Patch available without template, affecting my environment = Yes, Not Critical or Above</td>
</tr>
<tr>
<td>Package ready for manual signing</td>
<td>Package available with template</td>
<td>Package available without template</td>
</tr>
</tbody>
</table>

**Patch Rule Actions**

After selecting the appropriate Patch Rule trigger option, you can create Patch Rule actions such as Patch - Create Packages and Patch - Publish to deployment servers.

**Table 3-4 • Patch Rule Action Options**

<table>
<thead>
<tr>
<th>Patch - Create Packages</th>
<th>Patch - Publish to deployment servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patch - Create packages</td>
<td>Patch - Create packages</td>
</tr>
<tr>
<td>Call service provider</td>
<td>Call service provider</td>
</tr>
<tr>
<td>Charge ticket assignment</td>
<td>Charge ticket assignment</td>
</tr>
<tr>
<td>Charge ticket status</td>
<td>Charge ticket status</td>
</tr>
<tr>
<td>Patch - Create packages</td>
<td>Patch - Create packages</td>
</tr>
<tr>
<td>SMS</td>
<td>SMS</td>
</tr>
</tbody>
</table>
Notification Actions

You can create several Notification Actions to communicate your rules using Email, SMS, Notify, Create ticket, and Call service provider.

Table 3-5 • Notification Actions

<table>
<thead>
<tr>
<th>Email the user with custom message and broadcast the email to members of a particular group</th>
<th>SMS the user with custom message and broadcast the text to members of a particular group</th>
<th>Notify the user with custom message and broadcast the email to members of a particular group</th>
<th>Create ticket with status Waiting for handling</th>
<th>Call Service Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Choose Action</strong></td>
<td><strong>Choose Action</strong></td>
<td><strong>Choose Action</strong></td>
<td><strong>Choose Action</strong></td>
<td><strong>Choose Action</strong></td>
</tr>
<tr>
<td>Email</td>
<td>SMS</td>
<td>Notify</td>
<td>Create ticket</td>
<td>Call Service Provider</td>
</tr>
<tr>
<td>Templates Available/Patches</td>
<td>Published Package Successfully</td>
<td>Notify</td>
<td>Status Waiting for handling</td>
<td></td>
</tr>
<tr>
<td>Patches</td>
<td>New Package/Package</td>
<td>Patches</td>
<td>Waiting</td>
<td></td>
</tr>
<tr>
<td>Available</td>
<td>Installed</td>
<td>Open</td>
<td>Handling</td>
<td></td>
</tr>
<tr>
<td>Patch Management Admin</td>
<td>Patch Management Admin</td>
<td>Not Found</td>
<td>Check</td>
<td></td>
</tr>
<tr>
<td>Save</td>
<td>Save</td>
<td>Delete</td>
<td>Delete</td>
<td></td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancel</td>
<td>Cancel</td>
<td>Cancel</td>
<td></td>
</tr>
</tbody>
</table>

**Note** • This option requires prior integration configuration with the service provider.

Default Workflow Rules

Software Vulnerability Research includes default workflow rules, which relate to ticketing, advisories, patching, and more. When selecting workflow rules, you should use either default workflow rules or custom workflow rules. Custom rules cancel out default rules, and two custom rules with identical triggers and actions cancel each other out.

The screen shot below provides two default patch rules:

- The first rule detects Patches without a template, and it sends an internal notification and an Email.
- The second rule detects Patches with a configured template, creates the package, and sends an internal notification and an Email.
The default workflow rules should be used as a template. It's good practice to disable the default workflow rules to make custom workflow rules with the same settings. Custom rules cancel out default rules, which might cause unforeseen issues. For additional information, see Default Workflow Rule Examples.

Custom Workflow Rules

A Custom Workflow Rule is any workflow rule that was built from scratch by the user. It might be a simple workflow rule or a more complex one.

The custom workflow rule screen shot below includes:

1. A patch with a template
2. Creating an internal notification in Software Vulnerability Research
3. Creating a patch package
4. Single user email notification
5. Publishing the patch package
6. Creating a notification to the single user and to the Patch Management Admins user group
7. Creating a ticket and marking it **Handled** because this workflow rule automatically handled the package from its release phase to its publishing to the WSUS/System Center Configuration Manager.

**Note** • This custom workflow rule will cancel out all default workflows labeled *Patch available with Template*.

Patching

Patching through the Software Vulnerability Research can be performed as a manual, semi-automated, or fully automated process.

This section describes the following patching topics:

- System Requirements for Patching
- Packages
- Patch Template
- Build Package
- Package Deployment
System Requirements for Patching


Important • If your organization allows specific URL access to the Internet, and you are having problems downloading or verifying a patch, ensure the CRLs are allowed; examine the logs to identify the download’s source, and examine the certificate at that address for its CRL distribution points.

Packages

You can create packages without scanning your network because Flexera has provided several default package templates that are ready to be built into physical update packages on the fly.

It’s a best practice to scan your hosts before creating any packages. After clicking the Patching module’s blue filter icon, the left-most filter allows you to filter only patches Affecting Your Environment. There are other patching filters under the blue filter button.

Task

To successfully create and deploy third-party packages:

1. Install and configure the Software Distribution Daemon for Windows. See Deploy the Windows Agent Application through Microsoft’s System Center Configuration Manager (SCCM).

2. Configure Workflow Rules for Patching and automate the patching process as much as you want or as much as the process requires.

   • For automatic patching workflow rule examples, see Rule Triggers, Patch Rule Actions, and Notification Actions.

   • For a manual patching workflow rule, create the following steps: Create Template > Build Package > Create Deployment > Confirm Daemon Publishing.

For further information regarding package deployment filters, package deployment details, and package updates see Patch Library, Packages, and Deployment.

Patch Template

To create a patch template, perform the following steps.
Task  To create a patch template:

1. After applying the filter to view only the patches required in your environment as described in Packages, select the most important application to patch. Then select Create template.

A blank Patch Template window appears with fields to enter the features and configuration settings of an update package.

2. Enter the **Template name** and (optional) **Description**.

3. Select the **Package configuration** options from the drop-down lists and click **Save**. A sample patch template is shown below.

   ![Sample patch template](image)

   **Note** • The Package configuration options will vary depending on the Product you are creating a Patch template for.

4. The **Path information** option allows users to create custom patch templates, which may be specified to account for multiple or non-standard installation paths to aid in detection of such applications. To create a custom patch template, click **Add Path**. When the **Add Path Applicability Rule for Package** window appears, manually enter the
custom installation path and click Add Path. To delete this path, click the red minus button. After entering the applicable Path information, click Save.

5. After creating a Patch Template, deploy the patch using a Build Package.

**Build Package**

*Important* • To build and deploy a package, you must first download and install the Software Vulnerability Research Daemon on your Windows Software Update Server. For further information, see Daemon Deployment and Install the Daemon.

**Task**

To build a package:

1. Click a package in the Patch Library grid and select Build packages.

2. When the Build packages window appears, select all templates to build packages for from the drop-down list and click Build. Patch Templates include the user who created the Patch Template and a time stamp for when the Patch Template was created.

3. Publish the package to your environment using Package Deployment.

**Package Deployment**

To publish the package to your environment, navigate to Patching > Packages in Software Vulnerability Research. To view package options other than deployment, see Packages.
To create deployment:

1. Select Create Deployment. The Choose where to publish the patch(es) dialog box will open.

2. Select the servers or groups to publish the patch(es).

3. Click OK.

After you create your deployments, it is up to your Daemon to come and collect the deployed packages. The Daemon connects to the Flexera Cloud about once every 10 minutes. However, the Daemon connection time might be extended if the Daemon experiences network issues.

Additional Patching Information

For additional Patching information, see:

- Patching Tickets
- Manual Signatures
The Dashboard is the default home page that provides you with an overview of vulnerability management processes and gives you access to your latest vulnerability intelligence and Advisories. The information is presented with the help of various widgets.

- Dashboard with Threat Intelligence Module
- Dashboard without Threat Intelligence Module

Dashboard with Threat Intelligence Module

The below figure shows the Dashboard with the Threat Intelligence Module, the additional widget **Highest threat scores affecting your watch lists** get included in the main page.

**Note** • Please note the following:

- This add-on requires purchase of the Software Vulnerability Research Threat intelligence Module
- To purchase this module, contact your sales representative or contact us online at: [https://www.flexera.com/about-us/contact-us.html](https://www.flexera.com/about-us/contact-us.html)
Click the icon to add the **Highest threat scores affecting your watch lists** widget and Save to save the changes you made.

---

**Note** • Click the icon to see more information about the widget.

**Dashboard Widget**

In additional to the features explained in the **Dashboard > Dashboard without Threat Intelligence > Dashboard Widgets**, the following widget is added:

- **Highest threat scores affecting your watch lists** - displays those advisories with the highest threat scores affecting the watch lists.

**Dashboard without Threat Intelligence Module**

The below figure shows the Dashboard without the Threat Intelligence module.
Click + to add widgets (when available) and Save to save the changes you made.

---

**Note** • Click the † icon to see more information about the widget.

### Dashboard Widgets

The Dashboard widgets on the main page includes the following:

**Table 4-1 • Dashboard Widgets**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices Overview</td>
<td>Displays an overview of the average security score (current verses last week) for the Devices, Products and Operating Systems within your environment.</td>
</tr>
<tr>
<td>Devices status - Time since last scan</td>
<td>Displays the number of devices that have been scanned within a given time frame.</td>
</tr>
<tr>
<td>Devices status - System Score</td>
<td>Displays how your devices rank based on the computed system score.</td>
</tr>
</tbody>
</table>
### Table 4-1 • Dashboard Widgets

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most critical advisories affecting your security</td>
<td>Displays the most critical Advisories based on all software detected within your environment.</td>
</tr>
<tr>
<td>Latest advisories affecting your security</td>
<td>Displays a complete list of the latest Advisories released by Secunia. Click a Secunia Advisory ID (SAID) to view the complete advisory details, including (where applicable) the Creation Date, Criticality (Severity Rating), Impact (Consequence), Where (Attack Vector), Solution Status, Secunia CVSS (Common Vulnerability Scoring System), CVE References, Affected software and Advisory Description, Solution, References and Changelog.</td>
</tr>
<tr>
<td>Latest advisories affecting your security</td>
<td>Displays the most recent Advisories affecting software from your Devices.</td>
</tr>
<tr>
<td>Latest advisories per watch list</td>
<td>Displays the most recent Advisories released by Secunia based on your configured Watch Lists. Click a Secunia Advisory ID (SAID) to view the complete advisory details, including (where applicable) the Creation Date, Criticality, Impact, Where, Solution Status, Secunia CVSS Scores, CVE references, Affected software and Advisory Description, Solution, References and Changelog.</td>
</tr>
<tr>
<td>Advisories released last year</td>
<td>Displays a month-by-month graph of the total number of advisories released by Secunia over the previous 12 months.</td>
</tr>
<tr>
<td>Your latest assigned tickets</td>
<td>Displays the latest tickets that have been assigned to you. Click a Secunia Advisory ID (SAID) to view the complete advisory details, including (where applicable) the Creation Date, Criticality, Impact, Where, Solution Status, Secunia CVSS Scores, CVE references, Affected software and Advisory Description, Solution, References and Changelog.</td>
</tr>
<tr>
<td>Open tickets split by advisory criticality</td>
<td>Displays a color coded pie chart of the criticality of all open tickets assigned to you. Hover over the criticality legend (Low, Medium, High and Urgent) to display a tooltip with the total percentage of tickets applicable to the ticket criticality.</td>
</tr>
<tr>
<td>Tickets split by status</td>
<td>Displays a color coded pie chart of the statistics of all tickets assigned to you. Hover over the ticket type legend (Open, Waiting, Handled and Irrelevant) to display a tooltip with the total percentage of tickets applicable to the ticket type.</td>
</tr>
<tr>
<td>Open tickets pattern</td>
<td>Displays a trend line of the number of tickets that have been created based on your configured Watch Lists. The trend line applies to the status of all ticket types (Open, Waiting, Handled and Irrelevant).</td>
</tr>
<tr>
<td>Most prevalent EOL software installations</td>
<td>Displays the list of End-of-Life (EOL) software installations that no longer provide security fixes, which can lead to insufficient firewall and anti-virus protection. Please note that Flexera’s definition of EOL software may differ from a software vendor’s.</td>
</tr>
<tr>
<td>Most prevalent insecure software installations</td>
<td>Displays the most insecure software based on the number of Devices within your environment.</td>
</tr>
</tbody>
</table>
### Table 4-1 • Dashboard Widgets

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latest available patches</td>
<td>Displays the latest available patches based on your scan results.</td>
</tr>
</tbody>
</table>
Notifications provide detailed information about alerts you have received and any required actions. The number in the yellow bubble signifies the number of unread notifications.

**Important** • You shall not, unless expressly authorized in writing by Flexera, reproduce, distribute, display, sell, publish, broadcast, or circulate any information or other material provided by Flexera and/or any information or other material provided as a result of the Product(s) (such as advisories and security updates) to any third-party, including Customer’s affiliates, or any unauthorized Recipient, nor make such information or material available for any such use. The Product(s) may only be used by the legal entity that has purchased a license, and no shared use with any other legal entity (including Customer’s affiliates) is allowed.

**Task**

**To view notifications:**

1. Open the **Notifications** page.

2. Click the filter icon to filter the notifications by **Search by keyword, Criticality, Status, From** and **To** dates, and **Type**.

3. Click the **Apply** or **Reset** buttons to apply or reset the filters.
4. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

5. Click a Secunia Advisory ID (SAID), ticket number and so on to view detailed information related to the item.

6. Click the Notification check boxes to select from the available options in the Actions drop-down list.

7. Click to export the results to a CSV file.

## Setting Rules for Notifications

Your Administrator should set Rules to enable you to receive notifications, as shown in the following graphic. Please refer to [Workflow Management > Rules](#) for further information.
Edition • The Vulnerability Manager module is not available for Software Vulnerability Research - Assessment Only.

You can use the Vulnerability Manager pages to manage watch lists, advisories, and ticketing and approve advisories.

- Overview
- Watch Lists & Advisories
- Ticketing in Vulnerability Manager
- Approve Advisories

Overview

Use the Vulnerability Manager pages to manage the Vulnerability Intelligence associated with your account. You can:

- Create, import and view Watch Lists.
- Create and view Shared Watch Lists
- View and create tickets for Historic Advisories for all Watch Lists
- View and create tickets for Product Advisories for all products
- View, edit and Create Tickets in Vulnerability Manager
- View and approve Advisories associated with each Watch List
- Send Notifications to alert users via Email/SMS
- Edit, share or delete Watch Lists

Click an item in the grid to select from the available options.
Watch Lists & Advisories

Select Watch Lists from the Watch Lists & Advisories drop-down menu to view, create and configure multiple Watch Lists, each with their own unique set of Vendors (all products from the vendor), Products (all versions) and specific Product Versions that you want to receive vulnerability alerts and track Advisories for.

Select Historic Advisories from the Watch Lists & Advisories drop-down menu to view a comprehensive and thorough collection of reports and statistics about all Advisories affecting a specific Watch List.

After adding a Watch List, it is recommended that you view the Historic Advisories page to confirm that the vendor has addressed all the relevant issues in the software.

Watch Lists

You can define which vendors, products, and product versions you want to receive vulnerability alerts and track Advisories for.

The monitored Vendors (all products from the vendor), Products (all versions) and specific Product Versions are organized into Watch Lists. Each Watch List can have different notification levels, can be grouped into Watch List Groups and can be shared with all Users and User Groups associated with your account. There is no limit to the number of Watch List Groups that can be created.

For details, see:
- View Watch Lists
- Create Watch Lists
- Edit Watch Lists
- Import a New Watch List
- Import an Updated Watch List

The Watch List Enforced by admin column with a Yes or No response relates to the sharing of Watch Lists. For details, see Shared Watch Lists. By default, the notifications (such as an email or SMS) generated by a Watch List are sent only to the Watch List creator when a new advisory is released that matches a Watch List. If Watch List creators wish to share their asset list with other users from their organization, the Watch List is then shared based on the following options:

- If an administrator shares a Watch List, he or she has the option to enforce the targeted users to receive the notification, with the selected subscription levels. All targeted users will then receive the notification, as it is mandatory. The targeted users can’t unsubscribe from that Watch List. This will result in a Yes response in the Enforced by admin column.

- If a non-administrator shares a Watch List or an administrator does not select the Watch List’s “enforce” subscription option, the targeted users (Users with roles - Watch list manger and Watch list Manager Local) can decide whether or not to subscribe to the shared Watch List. The targeted users can manually subscribe to the Watch List, and notifications will not be sent to them before they manually subscribe to the Watch List page with their preferred subscription levels. This will result in a No response in the Enforced by admin column.
View Watch Lists

**Task**  
**View Watch Lists**

1. Open the **Vulnerability Manager > Watch Lists & Advisories > Watch Lists** page.

2. Click **+** to create a new Watch List or **Import** to import a Watch List from a text or CSV file that you have previously created and saved.

3. Click the Watch List check boxes in the grid to select from the available options from the CSV export button **Import** drop-down menu.

4. Click **Filter** to filter the watch lists and advisories by **Name**, **Group**, **Enabled** (yes or no), **Approval Needed** (yes or no), and **Created by**.

5. Click the **Apply** or **Reset** buttons to apply or reset the filters.

6. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

7. Click a Watch List in the grid to select **Historic Advisories, View, Edit, Change notification, Unsubscribe, Un-Share/Share, or Delete**.

8. To enable all of your users to collaborate, you can click a Watch List, select **Share**, and select the **With all users, Group (or Groups)** from the drop-down list and Enforce subscriptions options as required and click **Save**.

9. Click **Shared Watch Lists** to **View, Subscribe, or Clone** the Watch List. Select **Clone** to copy it to your Watch Lists, where you can then use the **Historic Advisories, View, Edit, Change notification, Share, Un-Share or Delete** options for the cloned Watch List.

**Note**  
Any changes you make to a shared Watch List are shared by all users. If you want to change only your Watch List, you should first clone it.

**Important**  
When creating, editing or sharing Watch Lists, the Deny auto-approval role will determine if the normal user can create Watch Lists with auto approval. The role must be manually added to a user group and that user group assigned to the restricted users by the administrators. For users with Deny auto-approval:

- **Create new Watch List**—The field Advisories need approval will be checked and cannot be disabled.
- **Edit existing Watch List**—The field Advisories need approval cannot be edited (either enabled or disabled).
Shared Watch Lists for the user will have the normal behavior. It is the responsibility of the creator to ensure the Watch List has Advisories need approval selected if it is shared with restricted users.

Create Watch Lists

To create a watch list, perform the following steps.

Task

**To create a Watch List**

1. Open the **Vulnerability Manager > Watch Lists & Advisories > Watch Lists** page.
2. To create a new Watch List, click . The **Create Watch List (Step 1 of 2)** page opens. On this page, you can select **Product Versions**, **Products**, **Vendors**, or **Assessment**.

3. Use the search field to find the products, vendors, product versions, and device groups to select and add to your Watch List.
4. Click in the Database suggestions column heading to add the current page or click next to the individual items to add them to the **Selected** items list.

Note • You can select the Receive all advisories check box to receive Secunia Advisories for all Product Versions, Products, and Vendors.
5. Click \( \times \) in the Selected items column heading to remove the current page or DELETE \( \times \) next to an individual item to remove it from the list.

6. Click Next. The Create Watch List (Step 2 of 2) page opens.

7. Enter the Name of the Watch List.

8. Select the Watch List Groups, if available, from the drop-down list to associate with this Watch List. You can also click + to create a new Watch List group.

9. Notifications and/or tickets are not sent for disabled Watch Lists. If you wish to preserve a Watch List for historical reasons, you can disable it by clearing the selection of the Enabled check box.

10. If you select the Advisories need approval option, you will receive a notification and an email for advisories that match your Watch List. You can approve that advisory, in which case a ticket is created or you can dismiss the advisories.

    \[ \text{Note} \ • \ If \ the \ users \ have \ the \ rejected \ advisories \ option \ enabled, \ the \ threshold \ filters \ may \ not \ apply \ since \ the \ advisory \ may \ not \ have \ the \ criticality \ set. \]

11. Select the Ticket threshold, Email and SMS notification levels from the drop-down lists.

    The Ticket threshold level is used to determine whether or not tickets will be created for advisories matching your Watch List.

12. You can optionally select the impact that a vulnerability in any item in the Watch List will have to your environment (Low, Medium or High) by Confidentiality Requirement (CR), Integrity Requirement (IR), and Availability Requirement (AR) from the drop-down lists (optional).
The table below defines the Low, Medium, and High impact for CR, IR and AR. For the tickets created on the Watch List with values in the CR, IR, and AR fields, the system will use those values to calculate the custom Common Vulnerability Scoring System (CVSS) for the ticket.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Low Definition</th>
<th>Medium Definition</th>
<th>High Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR</td>
<td>There is a low impact on the confidentiality of the system.</td>
<td>There is considerable disclosure of information, but the scope of the loss is constrained such that not all of the data is available.</td>
<td>There is total information disclosure, providing access to any or all data on the system.</td>
</tr>
<tr>
<td>IR</td>
<td>There is a low impact on the integrity of the system.</td>
<td>Modification of some data or system files is possible, but the scope of the modification is limited.</td>
<td>There is total loss of integrity; the attacker can modify any files or information on the target system.</td>
</tr>
<tr>
<td>AR</td>
<td>There is a low impact on the availability of the system.</td>
<td>There is reduced performance or loss of some functionality.</td>
<td>There is total loss of availability of the attacked resource.</td>
</tr>
</tbody>
</table>

Note • For further definition details, see: https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System#Impact_metrics

Note • After creating an Assessment Watch List from the Create a Watch List steps above:

- When a new scan is done, the new data is available in the Create Watch List pop-up window.
- When any scan result is deleted from the Assessment module, a refresh needs to be done to see the changes in the Assessment module and also in the Create Watch List pop-up window.
- When a Smart Group is deleted from the Assessment module, it may take at least 15 minutes to see the deleted Smart Group removed from the Assessment tab of the Create Watch List pop-up window.

13. Click Save to save the Watch List. Once saved, you will begin to receive alerts and advisories based on your configuration.

Edit Watch Lists

To edit a watch list, perform the following steps.
Task: To edit a Watch List:

1. Click an item in the grid and select Edit.

2. Select Receive all advisories and Filter by FNMS data as appropriate. When you have finished making your selections, click Next. The Edit Watch List (Step 2 of 2) page opens.

3. Enter the Name of the edited Watch List.

4. Select the Watch List Groups, if available, from the drop-down list to associate with this Watch List. You can also click + to create a new Watch List group.

5. Notifications and/or tickets are not sent for disabled Watch Lists. If you wish to preserve a Watch List for historical reasons, you can disable it by clearing the selection of the Enabled check box.

6. If you select the Advisories need approval option, you will receive a notification and an email for advisories that match your Watch List. You can approve that advisory, in which case a ticket is created or you can dismiss the advisories.

   Note • If the users have the rejected advisories option enabled, the threshold filters may not apply since the advisory may not have the criticality set.

7. Select the Ticket threshold, Email and SMS notification levels from the drop-down lists.
The **Ticket threshold level** is used to determine whether or not tickets will be created for advisories matching your Watch List.

8. You can optionally select the impact that a vulnerability in any item in the Watch List will have to your environment (Low, Medium or High) by **Confidentiality Requirement (CR)**, **Integrity Requirement (IR)** and **Availability Requirement (AR)** from the drop-down lists (optional).

9. Click **Save** to save the edited Watch List. Once saved, you will begin to receive alerts and advisories based on your configuration.

## Import a New Watch List

To import a new Watch List, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To import a new Watch List:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open the <strong>Vulnerability Manager &gt; Watch Lists &amp; Advisories &gt; Watch Lists</strong> page.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <img src="image.png" alt="button" />.</td>
</tr>
<tr>
<td>3.</td>
<td>Choose <strong>Create Watch List</strong> and <strong>Submit</strong>.</td>
</tr>
</tbody>
</table>

The **Create Watch List (Step 1 of 4)** dialog box opens.

4. Define the **Columns separator** (""," is the default) for the file you are importing.

5. Select **First row has column names**, if applicable.

6. Click **Upload file**. The **Create Watch List (Step 2 of 4)** dialog box opens.
7. Select the **Filter by quality** field to match your Watch List against the criteria you select from the drop-down list or use the **Search in your products** field to find a specific product.

8. Click + in the Database suggestions column heading to add the current page or click + next to the individual items to add them to the **Selected** items list.

9. Click X in the Selected items column heading to remove the current page or DELETE X next to an individual item to remove it from the list.

10. When you have finished making your selections, click **Continue**. The **Create Watch List (Step 3 of 4)** dialog box opens.
11. Choose other watch lists to add or delete and click **Next**. The **Create Watch List (Step 4 of 4)** dialog box opens.

12. Enter the **Name** of the Watch List.

13. Select the **Watch List Groups**, if available, from the drop-down list to associate with this Watch List. You can also click **+** to create a new Watch List group.

14. Select the **Enabled** and **Advisories need approval** check boxes as required.

15. Select the Ticket threshold, **Email** and **SMS criticality notification** levels from the drop-down lists.

16. You can optionally select the impact that a vulnerability in any item in the Watch List will have to your environment (Low, Medium or High) by **Confidentiality Requirement (CR)**, **Integrity Requirement (IR)** and **Availability Requirement (AR)** from the drop-down lists (optional).
17. Click **Save** to save the Watch List. Once saved, you will begin to receive alerts and advisories based on your configuration.

**Import an Updated Watch List**

To import an updated Watch List, perform the following steps.

**Task**

**To import an updated Watch List:**

1. Open the **Vulnerability Manager > Watch Lists & Advisories > Watch Lists** page.

2. Click ✅.

3. Choose **Edit Watch List**, enter the Watch List to update in the search field, and click **Submit**.

   The **Edit Watch List (Step 1 of 4)** dialog box opens.

4. Choose **File** to import and click **Upload file**. The **Edit Watch List (Step 2 of 4)** dialog box opens.
5. Make the necessary edits and click **Continue**. The **Edit Watch List (Step 3 of 4)** dialog box opens.

6. Make the necessary edits and click **Next**. The **Edit Watch List (Step 4 of 4)** dialog box opens.

7. Make any necessary edits and click **Save**.

**Historic Advisories**

The **Historic Advisories** page provides access to a comprehensive and thorough collection of reports and statistics about all Secunia Advisories.
Task  To view historic advisory data:

1. Open the Vulnerability Manager > Watch Lists & Advisories > Historic Advisories page.

2. Click \( \text{T} \) to filter the advisories by All Watch Lists, Impact, CVE(s), SAID, From and To dates, Criticality, Solution status, Where, CVSS Score Minimum and Maximum values, Has Ticket, and Advisory Type.

3. Click the Apply or Reset buttons to apply or reset the filters.

4. Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

5. Click a Secunia Advisory ID (SAID) to view detailed information related to the advisory.

6. Click an Advisory check box in a row or rows in the grid or click the Advisory and select View Advisory or Create ticket.

\[ \text{Note} \] • If you select multiple advisories, one ticket will be created for each of the advisories selected.

\[ \text{Note} \] • Once you have selected an Advisory check box, you can click \( \text{+} \) to create a ticket.

Product Advisories

The Product Advisories page provides access to a comprehensive and thorough collection of reports and statistics about all Secunia Advisories affecting all products.
Chapter 6  Vulnerability Manager
Watch Lists & Advisories

**Task**

*To review product advisories*

1. Open the Vulnerability Manager > Watch Lists & Advisories > Product Advisories page.

2. Click to filter the Advisories by Zero Day, Impact, SAID, CVE(s), From and To dates, Criticality, Solution status, Where, CVSS Score Minimum and Maximum values, and Advisory type.

3. Click the Apply or Reset buttons to apply or reset the filters.

4. Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

5. Click a Secunia Advisory ID (SAID) to view detailed information related to the Advisory.

6. Click an Advisory check box in a row or rows in the grid or click the Advisory and select View Advisory or Create ticket.

   **Note** • If you select multiple advisories, one ticket will be created for each of the advisories selected.

   **Note** • Once you have selected an Advisory check box, you can click to create a ticket.

### Shared Watch Lists

To enable all of your users to collaborate, you can click any of your Watch Lists, select Share, and select the With all users, Group (or Groups) from the drop-down list and Enforce subscriptions options as required and click Save.

If an account administrator wants to share a Watch List with all Users or User Groups on a mandatory basis, they can select Enforce subscriptions. All users that match from the selected groups (or from the entire account) will automatically receive notifications for the released advisories that match the Watch List. If Enforce subscriptions is not selected, the users have the option to voluntarily subscribe to advisories from that Watch List and can choose their own notifications levels.

**Note** • Subscribers to the Watch List can edit the Watch List, resulting in changes for all users.

Click a Shared List in the grid to View or Clone the Watch List. Select Clone to copy it to your Watch Lists, where you can then use the Historic Advisories, View, Edit, Change notification, Share, Un-Share or Delete options for the cloned Watch List.

**Note** • Any changes you make to a Shared List are shared by all users. If you want to change only your Watch List, you should first clone it.

**Note** • A watch list can only be shared once. If you need to share the watch list with multiple groups or with multiple levels, you will need different watch lists.
FlexNet Manager Suite (FNMS) Import

Go to Vulnerability Manager > Inventory > FNMS Import to display a list of products imported from FlexNet Manager Suite.

You can Search by keyword for a specific product or click to filter the list by Name, Version, Publisher, Matched by Flexera (select Unknown by Flexera or Matched by Flexera from the drop-down list), Matched by Intelligence (select Unmatched by Intelligence or Matched by Intelligence from the drop-down list) or Import status (select New, Same or Removed from the drop-down list).

For further information, please refer to the FlexNet Manager Suite Inventory Exporter documentation.

You can also select Filter by FNMS data when creating or editing Watch Lists.

Note • It may take up to 5 minutes for the submitted products to be processed and displayed.

Important • The minimum version of FlexNet Manager Suite supported by the Software Vulnerability Research import tool is 2015 R2 SP2.

Ticketing in Vulnerability Manager

A ticket enables you to track and manage vulnerabilities based on the current state of all your Products, Vendors, and Watch Lists.

You can manually create a ticket from all Advisories, in case you would like to further process an Advisory for a vulnerability not affecting any of your Watch Lists, giving you the possibility to track any vulnerability which might affect the organization, not only vulnerabilities in software included in any of your Watch Lists.

Use the Ticketing page to view and change the Ticket Status and Ticket Priority of each Ticket.

Task

To view and change ticket status and ticket priority

1. Open the Vulnerability Manager > Ticketing page.
2. To filter the results by ticket status, select one of the bold ticket statuses in the upper-left-hand corner followed by a ticket count. The default ticket statuses are Open, Waiting, Handled, and Irrelevant. See Default Ticket Statuses in Vulnerability Manager for more information.
3. Click to filter the results by ID, From and To dates, Queue, Priority, Watch List, SAID, Criticality, Solution status and CVSS Score Minimum and Maximum values, and Assigned User.

4. Click the Apply or Reset buttons to apply or reset the filters.

5. Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

6. Click a Secunia Advisory ID (SAID) to view detailed information related to the Advisory.

7. To view one ticket, click the appropriate ticket check box in the grid to View, Edit, or Delete the ticket. To view multiple tickets, click the appropriate ticket check boxes in the grid and select an option from the Actions drop-down menu such as Delete multiple tickets (see Delete Tickets in Vulnerability Manager) or Edit multiple tickets.

8. Click to export tickets to a CSV file.

9. Click to Create Tickets in Vulnerability Manager.

Create Tickets in Vulnerability Manager

To create tickets in Vulnerability Manager, perform the following steps.

Task

To create a ticket in Vulnerability Manager:

1. Open the Vulnerability Manager > Ticketing page.

2. Click an Advisory or to create a ticket for the Advisory.

3. From the Status drop-down list, select the appropriate status. The default ticket statuses are Open, Handled, Closed, or Irrelevant. See Default Ticket Statuses in Vulnerability Manager for more information.
4. From the **Priority** drop-down list, select the appropriate priority. The default ticket priorities are **Low**, **Medium**, **High** or **Urgent**.

5. From the **Queue** drop-down list, select a queue to assign the ticket to.

6. From the **Assigned to** drop-down list, select an individual to assign the ticket to.

7. In the **Add comment** field, add an appropriate comment to the ticket (mandatory).

8. Click **Save**.

### Delete Tickets in Vulnerability Manager

To delete tickets in Vulnerability Manager, perform the following steps.

**Task**

**To delete tickets in Vulnerability Manager:**

1. Open the **Vulnerability Manager > Ticketing** page.

2. Insert a check mark in front of the ticket or tickets to delete.

3. To delete one ticket, select **Delete** under the listed ticket in the grid.

4. To delete multiple tickets, select **Delete multiple tickets** from the **Actions** drop-down menu.

5. When the “Are you sure you want to delete these tickets” pop-up window appears, click **Yes**.
Default Ticket Statuses in Vulnerability Manager

The default ticket statuses are used by the Advisories and Policy Manager to run and display reports. While you are free to configure the ticket statuses, priorities and queues as you see fit, Flexera needs to know your equivalent “open” statuses to be able to correctly report the statistics.

The following are the default ticket statuses:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Tickets</td>
<td>An Open Ticket is one for which no action has yet been triggered.</td>
</tr>
<tr>
<td>Waiting Tickets</td>
<td>A ticket is marked as Waiting when it has been decided that an action needs to be taken at a later stage.</td>
</tr>
<tr>
<td>Handled Tickets</td>
<td>A ticket is considered Handled when the appropriate action has been taken.</td>
</tr>
<tr>
<td>Irrelevant Tickets</td>
<td>A ticket is considered Irrelevant when it has been handled and is no longer considered of importance to you.</td>
</tr>
</tbody>
</table>

Click a Secunia Advisory ID (SAID) to view detailed information related to the Advisory or click a ticket to View or Edit the details.

Approve Advisories

The Approve Advisories page displays a list of all Advisories pending your approval.

Note • To approve Advisories, you should select the Advisories need approval check box when you Create Watch Lists.

Task Approve advisories

1. Open the Vulnerability Manager > Approve Advisories page.

2. Click to filter the Advisories by In queue, Watch List, SAID, From and To dates, Title, Criticality, and Solution status.

3. Click the Apply or Reset buttons to apply or reset the filters.
4. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

5. To approve one advisory, click the appropriate advisory check box in the grid to **Approve** the advisory. The **Approve advisory** pop-up window appears. Continue to step 7.

6. To approve multiple advisories, click the appropriate advisory check boxes in the grid and select **Approve multiple advisories** from the Actions drop-down menu. The **Approve multiple advisories** pop-up window appears.
7. Select the Status (Open, Waiting, Handled or Irrelevant) from the drop-down list.

8. Select the Priority (Low, Medium, High or Urgent) from the drop-down list.

9. Select the Queue (Default or Approval) from the drop-down list.

10. Select who the ticket should be Assigned to from the drop-down list.

11. Enter a comment.

12. Click **Save** to approve the Advisory or Advisories.

**Note** • Once an Advisory has been approved, the corresponding ticket will be marked as **Open**.
Vulnerability Intelligence represents our full Vulnerability Database, which has been updated and maintained since the inception of Secunia in 2002.

Use the Research pages to:

- View Advisories
- Create Tickets in Vulnerability Manager
- View Vendors, Product Versions, Products, Suggest Software, and Download Software Suggestion Tool

**Advisory Database**

When a potential software vulnerability is publicly disclosed, our Research Team verifies that it is in fact a vulnerability. Once confirmed, we analyze the severity and what software might be affected.

Then, a standardized and 100% vendor independent Secunia Advisory is written for the vulnerability, detailing attack vector, criticality rating, impact and solution.

The Secunia Advisory is uploaded to Software Vulnerability Research, and adapted intelligence feeds are delivered to you, based on customized pre-configured filters, to ensure the right groups of people are alerted whenever a new vulnerability that could affect your IT infrastructure is discovered.

You can customize filters according to, for example, software responsibility, compliance criteria or geography for each of the recipients in your organization.

Personalized security alerts – via email or SMS - are then issued in real-time to the correct individual in your organization.

Select Advisories or Rejection Advisories from the drop-down list to display details that are applicable to your Watch Lists.

**Advisories**

The Advisories page displays details of all the advisories released.

The Advisories page can be,
Advisories with Threat Score

The Advisories page with the Threat Score module is shown below.

Note • Please note the following:
This add on requires purchase of the Software Vulnerability Research Threat intelligence Module.

To purchase this module, contact your sales representative or contact us online at:
https://www.flexera.com/about-us/contact-us.html

In addition to the features explained in the Advisories Page > Advisories without Threat Score, the following features are added:

- **To filter the Advisories by Threat Score minimum and maximum values**, click.
- **To see the threat score and threat reason**, click a Secunia Advisory ID (SAID) > CVE References. Additional information of the selected Secunia Advisory ID is shown below:

  **Microsoft Windows PDF Library Two Code Execution Vulnerabilities**

<table>
<thead>
<tr>
<th>Secunia Advisory ID</th>
<th>SAB6099</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation Date</td>
<td>2010-03-08</td>
</tr>
<tr>
<td>Criticality</td>
<td>Highly critical</td>
</tr>
<tr>
<td>Zero Day</td>
<td>No</td>
</tr>
<tr>
<td>Impact</td>
<td>System access</td>
</tr>
<tr>
<td>Where</td>
<td>From remote</td>
</tr>
<tr>
<td>Solution Status</td>
<td>Vendor Patched</td>
</tr>
</tbody>
</table>

**Secunia CVSS Scores**
- Base: 10, Overall: 8.3
- AV:N/AC:L/Au:N/C/I/A:U/E/F/R/L/O/R/C

**CVE references**
- CVE-2016-9118
- CVE-2016-9117

**Threat Score**
- 54 (Last Updated 2019-02-21)

**Affected operating system and software**

**Operating systems**
- **Microsoft Windows 10**
- **Microsoft Windows 8.1**

- **To see the threat Score, threat Reason and their associated exploits**, click on the CVE references, as shown below:
Advisories without Threat Score

The Advisories page without the Threat Score is shown below:

Task

1. Open the Research > Advisory Database > Advisories page.
2. Use Search by keyword to filter the Advisories by the text you enter.
3. Click \( \text{Filter} \) to filter the Advisories by **Zero Day**, Impact, **CVE(s)**, **SAID**, From and To dates, **Criticality**, **Solution status**, Where, **Score Minimum** and **Maximum** values, and **Advisory Type**.

**Note** • To search for multiple advisories at the same time to determine which advisories apply to more than a single CVE for which you have interest, enter the CVEs in the **CVE(s)** filter and leave one space between entries (Example: CVE-2014-0224 CVE-2014-0160 CVE-2013-0169 CVE-2009-3555 CVE-2015-7575).

4. Click the **Apply** or **Reset** buttons to apply or reset the filters.

5. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

If you select **Hide rejected advisories** under **Settings > Account > Account Options**:  
- The **Advisory Type** filter will not appear under **Research > Advisory Database > Advisories**.
- The search result “No advisories found” appears under **Research > Advisory Database > Rejection Advisories**.

**Note** • The CVSS Score column in the grid contains either a CVSS 2.0 score or a CVSS 3.1 score. A CVSS 3.1 score will be noted with “v3” listed after the score.

6. Click a Secunia Advisory ID (SAID) to view detailed information related to the Advisory.
Chapter 7  Research

Advisory Database

Google Chrome Adobe Flash Player Multiple Vulnerabilities

<table>
<thead>
<tr>
<th>Security Advisory ID</th>
<th>SA57056</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation Date</td>
<td>2015-10-23</td>
</tr>
<tr>
<td>Criticality</td>
<td>- Highly Critical</td>
</tr>
<tr>
<td>Impact</td>
<td>System access</td>
</tr>
<tr>
<td>Where</td>
<td>From remote</td>
</tr>
<tr>
<td>Solution Status</td>
<td>Vendor Patched</td>
</tr>
<tr>
<td>Security CVSS Scores</td>
<td>Base: 9.0, Overall: 7.4</td>
</tr>
<tr>
<td></td>
<td>(AV:N/A/C/U:NC/CL/C/E/RL/OF/RC/C)</td>
</tr>
</tbody>
</table>

Affected operating system and software

Software

| Google Chrome 64.0       | CPE: N/A |

Advisory Details:

Description:
Multiple vulnerabilities have been reported in Google Chrome, which can be exploited by malicious people to compromise a user's system.

The vulnerabilities are caused due to the application bundling a vulnerable version of Adobe Flash Player.

For more Information:
SA56915

The vulnerabilities are reported in versions prior to 46.0.2490.80.

Solution:
Update to version 46.0.2490.80.

Original advisory:

References:
SA56915
https://security.google.com/supdate/66915/

Changeelog:
2015-10-23: Initial release

7. Click an Advisory check box in a row or rows in the grid or click the Advisory and select View Advisory or Create ticket.

Note • If you select multiple advisories, one ticket is created for each of the Advisories selected.

Note • Once you have selected an Advisory check box, you can click + to create a ticket. For more information, see Create Tickets in Vulnerability Manager.
Rejection Advisories

For compliance reasons, for example NERC (North American Electric Reliability Corporation), you may be required to report not only the vulnerabilities covered by the normal Advisories but also vulnerabilities, which our Research Team has rejected as not being a valid threat to security.

The Rejection Advisories page displays the advisories affecting your Watch Lists that did not pass our validation and filtering process rules and provides you with information about rejected vulnerabilities to make it possible for you to fulfill your compliance requirements. The Rejection Advisories page can be shown or hidden, depending on the Account Options set by your Administrator.

An advisory can be rejected for one of many reasons. The most common are:

- **No reachability**—The vulnerability cannot be exploited because the affected systems cannot be reached by an attacker.
- **No gain**—The vulnerability may be reached, but without any gain for the attacker.
- **No exploitability**—The vulnerability cannot be exploited because, for example, policy forbids installation of the affected software.
- **Dependent on other**—The vulnerability cannot be exploited by itself but is depending on another vulnerability being present.


**Note** • The rules outlined below are rules of thumb and not strictly pass/fail rules.

**Task**

To view rejection advisories

1. Open the Research > Advisory Database > Rejection Advisories page.

2. Click to filter the Advisories by Zero Day, Impact, CVE(s), SAID, From and To dates, Criticality, Solution status, Where, and Score Minimum and Maximum values.
Note • Rejection advisories may not have all the details of the normal advisories: CVSS Vector and score, criticality, and so on.

3. Click the Apply or Reset buttons to apply or reset the filters.

4. Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

5. Click a Secunia Advisory ID (SAID) to view detailed information related to the Advisory.

6. Click an Advisory check box in a row or rows in the grid or click the Advisory and select View Advisory or Create ticket.

Note • If you select multiple advisories, one ticket will be created for each of the advisories selected.

Once you have selected an Advisory check box, you can click + to create a ticket. For more information, see Create Tickets in Vulnerability Manager.

Products Database

The Products Database represents the full list of products tracked by our database, which has been updated and maintained since the inception of Secunia in 2002. You can browse Vendors, Products, and search for specific Product Versions applicable to your Watch Lists. You can also Suggest Software that you would like us to add to our database. You can also Download Software Suggestion Tool to suggest a software that is not detected by SVR.

- Vendors
- Product Versions
- Products
- Suggest Software
- Download Software Suggestion Tool

Vendors

The Vendors page displays a list of all available vendors. Click View Products to display the products associated with the vendor or click a vendor in the grid to view past advisories related to the vendor.
**Task**  
**To view vendors**

1. Open the Research > Products Database > Vendors page.

2. To search for a specific vendor, pick a name from the Vendor column, enter it in the Search by keyword field and press Enter.

3. Click to download a CSV file containing details of all vendors.

**Product Versions**

The Product Versions page displays a list of all available products, specified by product version number.

**Task**  
**To view product versions:**

1. Open the Product Versions page.

2. Click a product version in the grid to view past advisories related to the product version.

3. To search for a specific product version, pick a number from the Version column, enter it in the Search by keyword field and press Enter.

4. Click to filter the results by Name, Vendor, Version, Software type, (Software/Operating system), and Is end of life (No/Yes).

5. Click the Apply or Reset buttons to apply or reset the filters.

6. Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

7. Click to download a CSV file containing details of all product versions.

**Products**

The Products page displays a list of all available products.
Chapter 7  Research
Products Database

To view products

1. Open the **Products** page.

2. Click a product in the grid to view past advisories related to the product.

3. To search for a specific product, pick a name from the Name column, enter it in the **Search by keyword** field and press Enter.

4. Click 📊 to filter the results by **Name**, **Vendor**, and **Software type** (Software/Operating system).

5. Click the **Apply** or **Reset** buttons to apply or reset the filters.

6. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

7. Click **View versions** under the **View Releases** column to display the **Vendor**, **Product**, **Version**, **Type** and **End-of-Life details**.

8. Click 📃 to download a CSV file containing details of all products.

Suggest Software

Use the **Suggest Software** page to suggest new software to our Research Team. After clicking the **Suggest Software** button, the **Suggest a software** window appears. You must provide a Software name, Software version, a valid URL to the software Internet page, valid email addresses, and an optional comment.

*Note* • Multiple email addresses can be added in the **Email** field. Use a semi-colon or comma to separate multiple e-mail addresses.
You can also upload a CSV file or a TXT file with multiple product suggestions. Each row from the file must contain all details needed for a single product suggestion (Name, Version, and a valid URL).

**Note** • Multiple email addresses can be added in the Email field. Use a semi-colon or comma to separate multiple e-mail addresses.

Upon successful import, all entries present in the CSV file will be displayed in the Suggest Software page. Under Status column you can view the status as given below:

**Table 7-1** • Suggest Software Status Column Details

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Sent</td>
<td>Indicates the suggested software request as been sent to SVR.</td>
</tr>
</tbody>
</table>
You can view the average resolution time for addressing suggested software.

### Download Software Suggestion Tool

Use this page to suggest a software that is not detected by SVR. After clicking the Suggest Software button.

**Task**

To specify Suggest Software:

1. Open the **Research > Products Database > Suggest Software** page.
2. Click **Download Software Suggestion Tool** button to download the Software Suggestion Tool.
3. Open the Software Suggestion Tool.

4. The Software Suggestion Tool window includes the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Token</td>
<td>Click Get Account Token and select the desired token number.</td>
</tr>
<tr>
<td>Program Name</td>
<td>Program name auto-populates with respect to the selected program file. Modify the name (If required).</td>
</tr>
<tr>
<td>Program File</td>
<td>Click browse and select file from the preferred location.</td>
</tr>
<tr>
<td>Program URL</td>
<td>Specify the program URL.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Specify valid email addresses.</td>
</tr>
<tr>
<td>Note</td>
<td>Multiple email addresses can be added. Use a semi-colon or comma to separate multiple e-mail addresses.</td>
</tr>
<tr>
<td>Additional Information</td>
<td>Add additional information (if required).</td>
</tr>
</tbody>
</table>

5. After entering the above details, click Send to Flexera button.
6. Upon successful action, the details of the suggested software will be added in Suggest Software page.

7. By clicking on the View My Software Suggestions button, it navigates to the Research > Products Database > Suggest Software page where the details of the software suggestion will be displayed.
Assessment Scenarios

Edition • This Assessment module is not available for Software Vulnerability Research.

With Flexera’s Software Vulnerability Research, you can scan target hosts using a variety of approaches:

- Agent-Based Scan – Requirements for Windows
- Agent-Based Scan – Requirements for Mac OS X
- Agent-Based Scan – Requirements for Red Hat Enterprise Linux (RHEL)
- Vulnerable Software Discovery Tool Command Line Options
- Scanning Via Local Agents

Note • If the WSUS Self-Signed Certificate will be used to sign the update packages created by Software Vulnerability Research, you can use a different certificate as an alternative.

Important • Administrators must ensure that Software Vulnerability Research and its Vulnerable Software Discovery Tool have access to all necessary system and online resources which allow the application to run as intended. The following addresses should be white-listed in the Firewall/Proxy configuration to ensure that the client system is allowed access to these online resources:

- crl.verisign.net
- crl.thawte.com
- http://crl3.digicert.com
- http://crl4.digicert.com
- http://*.ws.symantec.com
- https://app.flexerasoftware.com/
Note • If a machine has not checked in with Software Vulnerability Research in 90 days, the machine will be removed from your view. If the machine checks in again, it will reappear.

Agent-Based Scan – Requirements for Windows

The flexibility offered by Software Vulnerability Research ensures that it can be easily adapted to your environment. To deploy the Windows agent, see Deploy a Windows Agent.

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

Table 8-1 • Agent-Based Scan / Windows System Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permissions</td>
<td>Administrative privileges to download and install Software Vulnerability Research’s Vulnerable Software Discovery Tool files SVMScanInstall.msi and SVMScan.exe from: <a href="https://app.flexerasoftware.com/">https://app.flexerasoftware.com/</a></td>
</tr>
<tr>
<td>Access</td>
<td>Access to: <a href="https://agent.app.flexerasoftware.com">https://agent.app.flexerasoftware.com</a></td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Operating System 7 Service Pack 1, 8.1, 10</td>
</tr>
<tr>
<td>Internet Connection</td>
<td>SSL 443/TCP to <a href="https://app.flexerasoftware.com/">https://app.flexerasoftware.com/</a></td>
</tr>
<tr>
<td>Update agent</td>
<td>Windows Update Agent 2.0 or later</td>
</tr>
<tr>
<td>Port</td>
<td>Port 443 (standard HTTPS) to access the cloud</td>
</tr>
</tbody>
</table>
Agent-Based Scan – Requirements for Mac OS X

The following requirements should be met before installing the Software Vulnerability Research’s Vulnerable Software Discovery Tool for Mac (see Deploy a Mac Agent) on an Intel-based Mac OS X machine:

**Table 8-2 •**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating System</strong></td>
<td>Supported operating systems:</td>
</tr>
<tr>
<td></td>
<td>• 10.8 Mountain Lion</td>
</tr>
<tr>
<td></td>
<td>• 10.9 Mavericks</td>
</tr>
<tr>
<td></td>
<td>• 10.10 Yosemite</td>
</tr>
<tr>
<td></td>
<td>• 10.11 El Capitan</td>
</tr>
<tr>
<td></td>
<td>• 10.12 Sierra</td>
</tr>
<tr>
<td></td>
<td>• 10.13 High Sierra</td>
</tr>
<tr>
<td></td>
<td>• 10.14 Mojave</td>
</tr>
<tr>
<td><strong>Permissions</strong></td>
<td>• Administrator at minimum (“root” privileges required for the installation)</td>
</tr>
<tr>
<td></td>
<td>• The user installing the Agent must have ‘execute’ permissions on the file (chmod +x)</td>
</tr>
<tr>
<td><strong>Internet Connection</strong></td>
<td>SSL 443/TCP to <a href="https://app.flexerasoftware.com/">https://app.flexerasoftware.com/</a>.</td>
</tr>
</tbody>
</table>

To scan Apple Mac OS X machines, you need to deploy the Vulnerable Software Discovery Tool for Mac locally on the target system. This Vulnerable Software Discovery Tool for Mac pulls information from text and binary coded plist files.

The installation can only be done under the Mac Terminal, as the Vulnerable Software Discovery Tool for Mac will be installed as a daemon (service) under the LocalSystem account.

Installation of Local Services on Mac OS X systems requires root privileges. The “root” account is disabled by default on Mac systems. Therefore you need to enable it to proceed.

To view and edit the assessment configurations for Mac OS X, see:

• Prepare Your Mac

• Install the Vulnerable Software Discovery Tool for Mac

**Prepare Your Mac**

Installation of daemons (services) on Mac OS X systems requires root account privileges. This means that the root account should always be used when installing the Vulnerable Software Discovery Tool for Mac.

You can switch to your local root account by using the command ‘su root’ in your Mac Terminal. You will be prompted to provide the password for the root account.
Provide the password for “root” if you know it. If you are not certain about the password, you may want to try entering “toor”, which is the default password for the root account, or you may also try with the current password of your Administrator account. Both ways may work, but if the account is disabled on the system, none of the passwords would work.

---

**Important** • The Terminal window will not display the password you typed in. Once you have entered the password correctly, press ENTER and wait for confirmation.

If you do not know the password for the root account, or the latter is currently disabled, you can perform the following actions to enable the account and set a new password:

- Open Terminal
- Type sudo passwd root
- Provide a new password

For more details on how to enable root account on Mac OS X systems, refer to:

http://support.apple.com/kb/ht1528

---

**Important** • If you cannot enable the “root” account on the Mac, or you prefer to not use it directly, you can alternatively use the “sudo” switch before each command associated with Vulnerable Software Discovery Tool for Mac activities. For example:

```
sudo ./svmscan_macos -c -v -v -v
```

can be used to install the Vulnerable Software Discovery Tool for Mac on the system.

Once you are ready with setting/logging the root account, you are one step away from installing the Vulnerable Software Discovery Tool for Mac.

When you download the Vulnerable Software Discovery Tool for Mac on your system, normally the file is being set with limited file permissions on the system. You must check whether the file is allowed execution on the system by using the `ls -l` command, which will list the file and will show its file permissions.

```
sh-3.2$ ls -l
```

```
total 3848
-rwxr-xr-x@ 1 administrator staff 1558928 Oct 25 12:25 svmscan_macos
```

In case the permissions do not include execute rights (the “x” character) for any user, you should set them for the root account by using the `chmod +x` command.

```
sh-3.2$ chmod +x svmscan_macos
```

```
sh-3.2$ ls -l
```

```
total 3840
-rwxr-xr-x@ 1 administrator staff 1558928 Oct 25 12:25 svmscan_macos
```

(If you are not using the root account, add sudo before chmod.)
Install the Vulnerable Software Discovery Tool for Mac

The traditional way of installing the Vulnerable Software Discovery Tool for Mac is as a daemon (similar to local service in Windows) as it will operate under the Mac OS X LocalSystem account. Install the binary by using the Mac Terminal services as follows:

```
# Prepare Your Mac (if not already done).
# Browse to the directory where you have placed the svmscan_macos binary file.
# Type the following command to install the Vulnerable Software Discovery Tool for Mac:

./svmscan_macos -i
```

The Vulnerable Software Discovery Tool for Mac shows in the Software Vulnerability Research console approximately 15 minutes after the installation.

4. To launch a new scan manually under the Mac Terminal, issue the command “./svmscan_macos -c”

5. Use the “-h” switch to see a full list of parameters supported by the Vulnerable Software Discovery Tool for Mac.

Agent-Based Scan – Requirements for Red Hat Enterprise Linux (RHEL)

To deploy the Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM and Vulnerable Software Discovery Tool for Red Hat Linux 7 RPM, see Deploy a Linux Agent.

**Note** • The svmscan_linux agent for RHEL is architecture independent (that is, it works for 32- and 64-bit).

To install the Single Host Agent on a Red Hat Enterprise Linux (RHEL) machine, the user:

- Must be a member of the sudoer group.
- Must have write access to the /etc/smvscan folder to save configuration data.
- Must have a RHEL machine that supports the following operating systems:
  - **RHEL 6**: requires bash, gzip, sed, gawk, procps, coreutils, glibc(x86-32), libcurl(x86-32), libconfig(x86-32), libuuid(x86-32), yum, yum-security
  - **RHEL 7**: requires: bash, sed, gawk, procps, coreutils, glibc(x86-32), libcurl(x86-32), libconfig(x86-32), libuuid(x86-32), yum

To install the RHEL agent, see Install the Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM and 7 RPM.
Chapter 8  Assessment Scenarios
Agent-Based Scan – Requirements for Red Hat Enterprise Linux (RHEL)

Note • It may be possible to install the scan Agent on RHEL operating systems and configurations other than those described above. However, these have not been tested and are not supported by Flexera.

Install the Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM and 7 RPM

Note • This is a sample reference implementation that you can use to help guide your setup.

For information on installing the Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM and 7 RPM, see:

- Installing the Vulnerable Software Discovery Tool
- Specifying Proxy Settings for the Scanner (Recommended Method)
- Specifying the LAN Group of the Machine
- Immediately Update the RHEL Agent Configuration
- Uninstalling the Scanner RPM Package

Installing the Vulnerable Software Discovery Tool

To install the Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM and 7 RPM, perform the following steps.

Task To Install the Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM and 7 RPM:

1. The 6 RPM tool requires: bash, gzip, sed, gawk, procps, coreutils, glibc(x86-64), libcurl(x86-64), libconfig(x86-64), libuuid(x86-64), yum, yum-security
   
   The 7 RPM tool requires: bash, sed, gawk, procps, coreutils, glibc(x86-64), libcurl(x86-64), libconfig(x86-64), libuuid(x86-64), yum

2. Login as root at the RHEL machine and install/update the package (the same command line option works for both cases):
   
   su root
   yum localinstall --nogpgcheck:
   Red Hat 7 RPM: yum install <path>/svmscan_linux-8.x.xxx-x.el7.x86_64.rpm
   Red Hat 6 RPM: yum install <path>/svmscan_linux-8.x.xxx-x.el6.x86_64.rpm

Specifying Proxy Settings for the Scanner (Recommended Method)

You can update the proxy setting to override the environment variables.
Chapter 8  Assessment Scenarios
Agent-Based Scan – Requirements for Red Hat Enterprise Linux (RHEL)

Task  To specify proxy settings for the scanner:
1. Update the proxy setting in the configuration file /etc/csia/svmscan_conf
2. Login as root and restart the scanner service:
   su root
   service com.flexera.svmscan restart (RHEL 6)
   OR
   systemctl restart com.flexera.svmscan (RHEL 7)

Specifying the LAN Group of the Machine
This setting will be overridden if the DNS domain name of the machine is publicly available (check with the "dnsmasq" command).

Task  To specify the LAN group of the machine:
1. Update the LanGroup setting in the configuration file /etc/csia/svmscan_conf
2. Login as root and restart the scanner service:
   su root
   service com.flexera.svmscan restart (RHEL 6)
   OR
   systemctl restart com.flexera.svmscan (RHEL 7)

Immediately Update the RHEL Agent Configuration
If you have set the Agent check-in time to, for example, 1 day, it will be 1 day until the RHEL Agent picks up any configuration changes. If you want the RHEL Agent to immediately adapt to configuration changes, you can use the commands below to accomplish this by simply restarting the Agent service.

Task  To immediately update the RHEL agent configuration:
1. Login as root and restart the scanner service:
   su root
   service com.flexera.svmscan restart (RHEL 6)
   OR
   systemctl restart com.flexera.svmscan (RHEL 7)

Uninstalling the Scanner RPM Package
To uninstall the scanner RPM package, perform the following steps.
Chapter 8  Assessment Scenarios
Vulnerable Software Discovery Tool Command Line Options

Task

To uninstall the scanner RPM package;

1. Login as root and uninstall the scanner RPM package:

   su root
   yum erase svmscan_linux.x86_64

Vulnerable Software Discovery Tool Command Line Options

You can use the following command line options for the Vulnerable Software Discovery Tool.

- Help
- Version
- Install
- Uninstall
- Modify Settings
- Controlling the Service
- Scanning from the Command Line
- Agent Configuration Options

Help

Run the Vulnerable Software Discovery Tool to get instructions and a list of command line options (ignores all other command line options, prints instructions and exits immediately). Also prints version as with -V. Exclusive:

SVMScan.exe  -h

Version

Print the version number of the Vulnerable Software Discovery Tool on the command line (exclusive):

SVMScan.exe  -V

Install

The following explain how to install the Vulnerable Software Discovery Tool from the command line:

- Install as Current User
- Install to Run as LocalSystem
- Install to Run as <user>
Install the Vulnerable Software Discovery Tool from the command line, with configuration options. Installs as current user, prompts for password, settings saved to HKCU:

```
SVMScan.exe -i <config options>
```

**Install to Run as LocalSystem**

Install the Vulnerable Software Discovery Tool from the command line to run as LocalSystem, with configuration options. Saves settings to HKLM:

```
SVMScan.exe -i -L <config options>
```

**Install to Run as <user>**

Install the Vulnerable Software Discovery Tool from the command line to run as <user>, with configuration options. Prompts for password and saves settings to HKEY_<user>:

```
SVMScan.exe -i -R <user> <config options>
```

**Install to Run as <user> with <password>**

Install the Vulnerable Software Discovery Tool from the command line to run as <user>, with <password> with configuration options. Saves settings to HKEY_<user>:

```
SVMScan.exe -i -R <user>:<password> <config options>
```

**Install But Without Writing Anything to the Registry**

Install the Vulnerable Software Discovery Tool from the command line but not write anything to the registry (also works with -R and -L):

```
SVMScan.exe -i -N
```

**Uninstall**

Uninstall the Vulnerable Software Discovery Tool service, remove all settings and delete the key from the registry where the service reads them from:

```
SVMScan.exe -r
```

---

**Note** • The -L and -R options are irrelevant when uninstalling.

If the service is installed but cannot be removed, then the registry settings aren’t removed.

If the service is not installed, does nothing.

If the registry settings cannot be removed, a warning is given, and the service is removed regardless.

To uninstall the Vulnerable Software Discovery Tool service, while leaving the registry settings intact:
SVMScan.exe -r -N

To remove the service, if installed, and delete the Vulnerable Software Discovery Tool registry key from everywhere in the registry (exclusive):
SVMScan.exe --delete-all-settings

Modify Settings

Save the command line setting to the registry, so the service will use it. The settings are saved to the location based on where installed the Vulnerable Software Discovery Tool reads the settings from. If the Vulnerable Software Discovery Tool is not installed, or the settings cannot be saved to the correct location, nothing is saved, an error is printed and the command aborts:
SVMScan.exe -S <config option>

Controlling the Service

Starts the service if it is not running (exclusive):
SVMScan.exe --start
SVMScan.exe --restart

Stops the service if it is running (exclusive):
SVMScan.exe --stop

Scanning from the Command Line

Run the Vulnerable Software Discovery Tool with immediate command line scan, with options. Ignores registry settings and server settings:
SVMScan.exe -c <config options>

Run the Vulnerable Software Discovery Tool with immediate command line scan for Proof of Concept environments that will process scans fast, typically less than 1 minute:
SVMScan.exe -c --urgent-scan

Run the Vulnerable Software Discovery Tool locally in service mode as current user, reading options from command line, registry and server, with command line options taking precedence, then server options, then registry options. To stop the service once it is running, press CTRL+C:
SVMScan.exe -fg <config options>

If possible, run the Vulnerable Software Discovery Tool locally in service mode as a different user with -L and -R. This will read options in exactly the same way as a service, with the exception of <config options> on the command line override which, unlike a service, has no command line:
SVMScan.exe -fg -L <config options>
SVMScan.exe -fg -R <user> <config options>

Order of precedence:

- Settings given on command line take precedence but, when running as a service, there is no command line.
Settings from server take precedence over settings read from registry.

Agent Configuration Options

The following table lists the Agent configuration options.

Table 8-3 • Agent Configuration Options

<table>
<thead>
<tr>
<th>Category</th>
<th>Configuration Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Options</td>
<td>-A/--network-appliance</td>
<td>Run in Network Appliance mode.</td>
</tr>
<tr>
<td></td>
<td>-c/--cli</td>
<td>Run software inspection from the command line using command-line settings and server-supplied settings. Exit codes returned: 0 - SUCCESS 1 - SERVER BUSY 2 - OPERATION FAILED 3 - SERVICE FAILED</td>
</tr>
<tr>
<td></td>
<td>-d &lt;path&gt; --debug &lt;path&gt;</td>
<td>Write diagnostic information to the specified file.</td>
</tr>
<tr>
<td></td>
<td>--getfileinfo &lt;path&gt;</td>
<td>Directory for output file</td>
</tr>
<tr>
<td></td>
<td>-h/--help</td>
<td>Display this message and exit.</td>
</tr>
<tr>
<td></td>
<td>-n/--checkin-interval &lt;interval&gt;</td>
<td>Set the check-in interval for the service. This setting is in the format INTEGER followed by M/H/D representing minutes, hours, or days. Example: 10M for a 10-minute interval or 2H for a two-hour interval</td>
</tr>
<tr>
<td></td>
<td>-o/--outdir &lt;path&gt;</td>
<td>Directory for output file</td>
</tr>
<tr>
<td></td>
<td>-oc/--output-csv &lt;file&gt;</td>
<td>Output inspection results to a CSV file.</td>
</tr>
<tr>
<td></td>
<td>-ox/--output-xml &lt;file&gt;</td>
<td>Output inspection results to an XML file.</td>
</tr>
<tr>
<td></td>
<td>-si/--scantime_interval &lt;minutes&gt;</td>
<td>Set a random range to delay running software inspection. 0 means no random range, or 1-60 minutes.</td>
</tr>
<tr>
<td></td>
<td>--skip-wait/--skipwait</td>
<td>Skip the initial 10 minute wait before the first check in.</td>
</tr>
<tr>
<td></td>
<td>-v  --verbose</td>
<td>Display or log additional diagnostic information.</td>
</tr>
<tr>
<td></td>
<td>-V/--version</td>
<td>Display program version information and exit. Use this option when you want to check the version of the agent.</td>
</tr>
</tbody>
</table>
Table 8-3 • Agent Configuration Options (cont.)

<table>
<thead>
<tr>
<th>Category</th>
<th>Configuration Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Area Option</td>
<td><code>-g/-group &lt;group&gt;</code></td>
<td>Create host as a member of <code>&lt;group&gt;</code> in your Software Vulnerability Research Account (defaults to domain or langroup if unspecified).</td>
</tr>
<tr>
<td>Mac Agent Option</td>
<td><code>--delete-all-settings</code></td>
<td>Deletes all information, including Globally Unique Identifiers (GUID), from the system to ensure it is clean to accommodate a new installation.</td>
</tr>
</tbody>
</table>
### Table 8-3 • Agent Configuration Options (cont.)

<table>
<thead>
<tr>
<th>Category</th>
<th>Configuration Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Settings</strong></td>
<td>-D --direct-connection</td>
<td>Bypass proxy, use direct connection.</td>
</tr>
<tr>
<td></td>
<td>--forcehttps</td>
<td>Force HTTPS, regardless of port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When this option is not specified, we default HTTPS on port 443 and HTTP on other ports. This option is for debugging purposes.</td>
</tr>
<tr>
<td></td>
<td>--ignore-ca</td>
<td>Ignore unknown certificate authority.</td>
</tr>
<tr>
<td></td>
<td>--ignore-cn</td>
<td>Ignore invalid Common Name in cert.</td>
</tr>
<tr>
<td></td>
<td>--ignore-crl</td>
<td>Ignore Certificate Revocation list.</td>
</tr>
<tr>
<td></td>
<td>--pac-url &lt;url&gt;</td>
<td>Proxy Autoconfig url</td>
</tr>
<tr>
<td></td>
<td>--request-timeout &lt;minutes&gt;</td>
<td>Sets a timeout on network connections. Set for 1-10 minutes or use 0 for no timeout.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use this option to increase the timeout period of HTTP requests to prevent the timeout error when the server does not respond in 2 minutes.</td>
</tr>
<tr>
<td></td>
<td>-U <a href="">user:pass</a> --proxy-user <a href="">user:pass</a></td>
<td>Set proxy credentials (saved in encrypted form).</td>
</tr>
<tr>
<td></td>
<td>--use-network-winhttp</td>
<td>Enable WinHttp network stack.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use WinHTTP when you want the agent to control the behaviors of the HTTP Internet protocol. We default WinHTTP to force using TLS 1.2. Also, the command line options for proxy such as -x, -U, and -D are designed to work in conjunction with WinHTTP. This option is for debugging purposes.</td>
</tr>
<tr>
<td></td>
<td>--use-network-wininet</td>
<td>Enable WinInet network stack (default).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use WinInet when you want to control the behaviors of HTTP Internet protocol using the Internet Options. Since WinInet does not have services support, the agent running as a service ignores this option. This option is for debugging purposes.</td>
</tr>
<tr>
<td></td>
<td>-x <a href="">proxy:port</a> --proxy <a href="">proxy:port</a></td>
<td>Set proxy.</td>
</tr>
</tbody>
</table>
### Proxy Options

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-D/--direct-connection</td>
<td>Force direct connection, overriding default internet proxy settings.</td>
</tr>
<tr>
<td>--pac-url &lt;URL&gt;</td>
<td>Specify the URL of the Proxy Auto Configuration file (.pac/.dat).</td>
</tr>
<tr>
<td>-U/--proxy-user &lt;user[:pass]&gt;</td>
<td>Specify Proxy authentication.</td>
</tr>
<tr>
<td>-x/--proxy &lt;host[:port]&gt;</td>
<td>Use HTTP proxy on given port.</td>
</tr>
</tbody>
</table>

### Scan Options

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--check-wmi</td>
<td>Use WMI to get Windows updates.</td>
</tr>
<tr>
<td></td>
<td>Use this option to query Windows updates on SCCM using WMI in addition to a query using Windows Update Agent.</td>
</tr>
<tr>
<td></td>
<td>This option could be used to see if the SCCM client on the device/host can be used for reporting missing KBs.</td>
</tr>
<tr>
<td>-t/--type</td>
<td>Software scan type:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Minimal Scan</strong>—Scan Type 1: Inspect applications in default locations only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Optimal Scan</strong>—Scan Type 2: Inspect applications in non-default locations.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Full Scan</strong>—Scan Type 3: Inspect all .dll, .exe, and .ocx files.</td>
</tr>
<tr>
<td></td>
<td>For details, see <a href="#">Scan Types</a>.</td>
</tr>
<tr>
<td>-w/--no-os-update/--no-win-update</td>
<td>Do not connect to Windows Update.</td>
</tr>
<tr>
<td>--wua-proxy &lt;0,1 or host[:port]&gt;</td>
<td>Configure proxy settings for Windows Update.</td>
</tr>
<tr>
<td></td>
<td>• 0: Use the default setting.</td>
</tr>
<tr>
<td></td>
<td>• 1: Use the proxy configured with -x/--proxy.</td>
</tr>
<tr>
<td></td>
<td>• &lt;host[:port]&gt; Manually set the proxy host and port.</td>
</tr>
</tbody>
</table>
### Table 8-3 • Agent Configuration Options (cont.)

<table>
<thead>
<tr>
<th>Category</th>
<th>Configuration Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Settings that Server Can Override</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-g <code>&lt;group&gt;</code> --group <code>&lt;group&gt;</code></td>
<td></td>
<td>Group name for association</td>
</tr>
<tr>
<td>-n <code>&lt;minutes&gt;M</code> --checkin-interval <code>&lt;minutes&gt;M</code></td>
<td></td>
<td>Set Check-in interval.</td>
</tr>
<tr>
<td>-n <code>&lt;hours&gt;H</code> --checkin-interval <code>&lt;hours&gt;H</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security Options</strong></td>
<td>--ignore-ca</td>
<td>Ignore Unknown SSL Certificate Authority (CA).</td>
</tr>
<tr>
<td></td>
<td>--ignore-crl</td>
<td>Ignore SSL Certificate Revocation Check.</td>
</tr>
<tr>
<td></td>
<td>--ignore-cn</td>
<td>Ignore Invalid SSL Certificate Common Name (CN).</td>
</tr>
<tr>
<td><strong>Server Options</strong></td>
<td>--userid <code>&lt;userid&gt;</code></td>
<td>Set the Software Vulnerability Research access user ID.</td>
</tr>
<tr>
<td></td>
<td>--token <code>&lt;token&gt;</code></td>
<td>Set the Software Vulnerability Research access token.</td>
</tr>
<tr>
<td></td>
<td>--host <code>&lt;hostname&gt;</code></td>
<td>Set the Server hostname.</td>
</tr>
<tr>
<td></td>
<td>--port <code>&lt;port&gt;</code></td>
<td>Set the Server port.</td>
</tr>
</tbody>
</table>
### Table 8-3 • Agent Configuration Options (cont.)

<table>
<thead>
<tr>
<th>Category</th>
<th>Configuration Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Options</strong></td>
<td>--delete-all-settings</td>
<td>Delete all settings related to this program from the registry.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deletes these settings from all registry keys.</td>
</tr>
<tr>
<td></td>
<td>--dry-run/--dryrun</td>
<td>Run up to the point of scanning without writing any changes and then exit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(useful to log the configuration).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use this option to examine if the agent is able to run and communicate with</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the server. It will exit before scanning and won't make any changes to the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>system. You can use this option along with -c.</td>
</tr>
<tr>
<td></td>
<td>-i/--install</td>
<td>Install service.</td>
</tr>
<tr>
<td></td>
<td>-L/--localsystem</td>
<td>Run the service as the LocalSystem user.</td>
</tr>
<tr>
<td></td>
<td>--manual</td>
<td>When installing, set service to only be started manually, rather than</td>
</tr>
<tr>
<td></td>
<td></td>
<td>automatically.</td>
</tr>
<tr>
<td></td>
<td>-N/--no-registry-write</td>
<td>When installing, do not write any settings to registry.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When removing, do not delete settings from registry.</td>
</tr>
<tr>
<td></td>
<td>-p/--copy &lt;dest&gt;</td>
<td>Before installing, copy executable file to &lt;dest&gt; and install the service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to run from &lt;dest&gt;.</td>
</tr>
<tr>
<td></td>
<td>-r/--remove</td>
<td>Remove service.</td>
</tr>
<tr>
<td></td>
<td>-R/--runas &lt;user[:pass]&gt;</td>
<td>Specify the user the service should run as.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For a domain user type &quot;user@domain&quot; or &quot;domain\user&quot;</td>
</tr>
<tr>
<td></td>
<td>-S/--only-save-settings</td>
<td>Only save settings from the command line to registry, as the relevant user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not run, install or remove.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use this option when you want to modify the agent registry settings after</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the agent is installed. You need to restart the agent service to make the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>changes effective.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This option could be used to edit the server options like user/id/token/host/</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port stored in the registry.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This setting is the opposite of &quot;-N&quot; options. If -N is used, no registry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>setting will be edited.</td>
</tr>
</tbody>
</table>
Chapter 8  Assessment Scenarios
Scanning Via Local Agents

Software Vulnerability Research provides different Scan Types, 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 Vulnerable Software Discovery Tool will run silently in the background.

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Configuration Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Recovery</td>
<td>--service-failure-actions</td>
<td>Failure actions and their delay time (in milliseconds), separated by / (forward slash) – e.g., run/5000/reboot/800. Valid actions are &lt;run</td>
</tr>
<tr>
<td></td>
<td>--service-failure-command</td>
<td>Command line to be run on failure.</td>
</tr>
<tr>
<td></td>
<td>--service-failure-flag</td>
<td>Changes the failure actions flag setting of a service. If this setting is not specified, the Service Control Manager (SCM) enables configured failure actions on the service only if the service process terminates with the service in a state other than SERVICE_STOPPED. If this setting is specified, the SCM enables configured failure actions on the service if the service enters the SERVICE_STOPPED state with a Win32 exit code other than 0 in addition to the service process termination as above. This setting is ignored if the service does not have any failure actions configured.</td>
</tr>
<tr>
<td></td>
<td>--service-failure-reboot</td>
<td>Message broadcast before rebooting on failure.</td>
</tr>
<tr>
<td></td>
<td>--service-failure-reset</td>
<td>Length of period of no failures (in seconds) after which to reset the failure count to 0 (may be INFINITE). (Must be used in conjunction with --service-failure-actions)</td>
</tr>
</tbody>
</table>
## Scan Types

Under **Scan Configuration** settings, you will be asked to select a scan type, which are compared below.

**Table 8-4 • Scan Types**

<table>
<thead>
<tr>
<th>Scan Type</th>
<th>Folders Searched</th>
<th>File Name Match</th>
<th>Applications Detected</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimal Scan - Scan Type 1</strong></td>
<td>Default folders only</td>
<td>File names are matched first; then metadata is matched.</td>
<td>Known applications in predefined locations on a device</td>
</tr>
<tr>
<td></td>
<td>Example: Program Files</td>
<td></td>
<td>Example: c:\Program Files\Mozilla Firefox\Firefox.exe</td>
</tr>
<tr>
<td><strong>Optimal Scan - Scan Type 2</strong></td>
<td>All files and folders</td>
<td>File names are matched first; then metadata is matched.</td>
<td>Known applications in any location (“portable applications”) on a device</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Example: c:\Custom Mozilla Firefox Folder\Firefox.exe</td>
</tr>
<tr>
<td><strong>Full Scan - Scan Type 3</strong></td>
<td>All files and folders</td>
<td>Metadata only</td>
<td>Renamed applications that match a pattern detected in the first two scan types such as .exe, .dll, and .ocx in any location on a device</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Example: c:\Custom Mozilla Firefox Folder\myFirefox.exe</td>
</tr>
</tbody>
</table>
Assessment Reports

Edition • This Assessment module is not available for Software Vulnerability Research.

The Assessment pages display where software vulnerabilities are installed across your organization by device and product. A list of advisories is also provided to address software vulnerabilities.

- Overview
- Devices
- Products
- Advisories

Overview

The Overview page displays a tree view of the Device Groups within your environment. Click an item under the My Environment listing to view the Average System Score, Device Details, Last Scan Details, and Product Details of the security status of the Device Group.

You can customize your Device Groups using Smart Groups.

Click the Devices, Products and Advisories tabs to view detailed information regarding the selected Device Group.

Important • You must first download and deploy Software Vulnerability Research’s Scan Agent to scan your devices. Refer to Downloads for further information.
Smart Groups

Smart Groups organize your environment by defining specific groups of devices, products, or advisories to identify and meet regulatory needs that are situation specific. These Smart Groups filter assessment results and reports to prioritize remediation efforts.

This section includes the following Smart Group topics:

- Smart Group Selection Order
- Create a Smart Group
- Create a Smart Groups Report

Smart Group Selection Order

To create a Smart Group, you can use any combination of device, products and advisories conditions. However, the order in which conditions are evaluated is this: device conditions filter out the devices on which the following conditions are applied; products conditions filter out devices without those products installed; advisory conditions filter out products and devices without those conditions. Following are some sample Smart Group selections.

- **Only device conditions**—Select those devices and show all products and advisories detected on those devices
- **Only product conditions**—Select the devices that have the products installed and show devices and advisories for those products
- **Only advisory conditions**—Select the devices and the products that have those advisories associated
- **All types of conditions**—Select the devices; then select devices with the product conditions and eliminate devices or products that do not have the advisory conditions. This selection order ensures that a group with the conditions “Windows platform, Python product installed, Highly and extremely critical advisories” show devices that have a Python product with highly critical advisories. This selection order also ensures you do not include devices with critical advisories on products that are not Python.
Create a Smart Group

To create a Smart Group, perform the following steps.

**Task**

To create a Smart Group:

1. **Click the green + sign next to My Smart Groups.**

2. **When the Create Smart Group pop-up window appears, enter the Smart Group Name in the Name field.**

3. **Select the Priority.**

**Note** • *The priority determines how often a smart group recalculates to show the latest results. The more critical the priority, the more often the results are calculated to reflect the latest data, with the following mention: if all groups are critical, none are critical. The exact frequency with which results are being recalculated can't be determined or...*
guaranteed as it depends on the number of groups in your environment (both Active Directory groups and Smart Groups) and the priorities set on all Smart Groups.

4. Select the desired combination of Device, Product Version, and Advisory Conditions. Click the green + sign to add multiple conditions under the corresponding category.

**Note** • *Device Platform is limited to Windows, macOS, and RedHat Enterprise Linux. If you want to select a particular operating system (Example: Windows 8), Select Windows as the Device Platform, add Device Condition “Operating System In”, click “Select Operating System(s)”; enter Windows 8 in the search tab, and click Save.*

**Note** • *To make sure date filters like Last Scan Date or Advisory Released conditions reflect the User Interface selection, ensure that your User Profile includes your time zone preference (Default time zone is set to Europe/Copenhagen). To change your time zone, go to User Profile and click Edit. Under Preferences, select the appropriate Timezone, and click Save.*

**Note** • *For the Advisory CVSS Score condition, Flexera applies the condition to the CVSS3 value if the advisory has CVSS3 data. Otherwise, the condition is applied to the CVSS2 score.*

5. Click Save. The newly created Smart Group folder will now appear under My Smart Groups.

6. You can now click Refresh to view the associated Overview, Devices, Products, and Advisories information. The data is calculated asynchronously, so you will need to change the group selection (or potentially refresh the page) to see the latest data.

**Note** • *In the Smart Groups Overview tab is a field titled “Latest data available” with the options “Yes” or “No”. For Active Directory (AD) groups, a “Yes” response means that no device in the folder tree underneath the AD sent new data. For Smart Groups, a “Yes” response means no device in a customer’s environment has sent new data. When a new device for either an AD group or Smart Group sends data, the “No” option appears until the group is reprocessed by the system. Once the group’s results are recalculated, the “Yes” option will reappear.*

**Note** • *The products counts on the device tab represent the total number of products installed on the device, regardless of the product conditions. The products and advisories counts on the products and advisories tabs are cross conditions. For example, for conditions “Adobe Flash products, Highly critical advisories”, the counts will represent: **Device product counts**: total number of products installed, not just Adobe Flash products; **Product advisory counts**: number of Highly...*
critical advisories affecting the product; **Advisory product counts**: number of Adobe Flash products affected by the advisory.

**Ensuring an Accurate Advisory Count**

To ensure an accurate advisory count between the Assessment module’s User Interface (which considers the user’s timezone and the Assessment module’s filters for the whole day) and the user-generated Assessment Report, use the following date filters to create a list of advisories released on a specific date (Example: March 31, 2018):

- For the **Advisory Initial Release Date** and **Advisory Current Release Date** conditions, enter 2018-03-01.
- In the Assessment > Advisories > Advisory List From (date) To (date) filters, enter 2018-03-01 in the From (date) filter and 2018-03-02 in the To (date) filter.

**Create a Smart Groups Report**

To create a Smart Groups Report, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To create a Smart Groups report under Analytics &gt; Reports:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click the green + button and select Add Assessment Report.</td>
</tr>
<tr>
<td>2.</td>
<td>When the Configure New Assessment Report pop-up window appears, under Device Groups select the appropriate Smart Group under the My Smart Groups listing.</td>
</tr>
<tr>
<td>3.</td>
<td>Select any other appropriate report conditions and click Save. The new report will be listed under Analytics &gt; Reports.</td>
</tr>
<tr>
<td>4.</td>
<td>To save the report as a CSV file or PDF file:</td>
</tr>
<tr>
<td></td>
<td>a. Select the appropriate Smart Group listing in the grid.</td>
</tr>
<tr>
<td></td>
<td>b. Click View Files.</td>
</tr>
<tr>
<td></td>
<td>c. Click Generate PDF.</td>
</tr>
<tr>
<td></td>
<td>d. Click Download once the file is generated.</td>
</tr>
</tbody>
</table>

**Note** • For recurring reports based on a Smart Group, the Smart Group contents are recalculated, based on the conditions before the report is sent out, to reflect the latest data for your selection.

**Devices**

The **Devices** page displays the details of the scan configuration status of all Devices or machines within your environment.

The Last Scanned column refers to the last time the Vulnerable Software Discovery Tool (Daemon) submitted scan data to the user interface. The time stamp in the **Last Scanned** column refers to the local time zone of the scanned server.
Task

To view devices:

1. Open the Assessment > Devices > Device List page.

2. Click and select from the drop-down lists to filter the Devices by Device Name, Platform (Windows, macOS, or RedHat Enterprise Linux), System score (100, 80-89, 50-79, <50, Unknown, or Not Calculated), Is secure (Yes or No), and Days since last Scan.

3. Click the Apply or Reset buttons to apply or reset the filters.

4. Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

5. Click an item in the grid to select Device details, Installed products, Advisories, Queue scan or Delete.

6. Click to export the results to a CSV file.

Device Details

The Device Details page displays Overview, Installations and Advisories details for the selected Device.
Task

To view device details:

1. In the Overview tab, click an Installed or Missing KB Details link to view detailed KB information. The selected KB Details will be highlighted.

2. Click in the Installations and Advisories tabs to export the results to a CSV file.
3. In the **Installations** tab, click a Device in the grid to find further information regarding the device’s **Missing KB(s)** for insecure Microsoft products, **Product details**, and **Available Patches**.

4. In the **Advisories** tab, click an SAID in the grid to view detailed information regarding the Advisory.

---

**Products**

The Products page displays the details of all Products within your environment.

---

**Task**

**To view products:**

1. Open the **Assessment > Products > Product List** page.

2. Click ⌁ and select from the drop-down lists to filter the Products by **Product Status** (Secure, Insecure, or EOL), Product name, and Vendor Name.

3. Click the **Apply** or **Reset** buttons to apply or reset the filters.

4. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

5. Click an item in the grid to select Product details, Installations or Advisories.

6. Click ⌘ to export the results to a CSV file.
Product Details

The Product Details page displays Overview, Installations and Advisories details for the selected Product.

**Task**

**To view product details:**

1. In the Advisories tab, click an SAID in the grid to view detailed information regarding the Advisory.
2. Click in the Installations and Advisories tabs to export the results to a CSV file.
Advisories

The Advisories page displays the details of all Advisories applicable to your environment.

On this page you can:

- View Advisory Details
- Create Advisory Tickets

Task

To view advisories:

1. Open the Assessment > Advisories > Advisory List page.

2. Click ☑ to filter the Advisories by Zero Day (yes/no), Impact (select from the drop-down list), CVE(s), SAID, From and To dates, Criticality (select from the drop-down list), Solution status (select from the drop-down list), Where (select from the drop-down list), CVSS Minimum Score, and CVSS Maximum Score.

   Note • To search for multiple advisories at the same time to determine which advisories apply to more than a single CVE for which you have interest, enter the CVEs in the CVE(s) filter and leave one space between entries (Example: CVE-2014-0224 CVE-2014-0160 CVE-2013-0169 CVE-2009-3555 CVE-2015-7575).

3. Click the Apply or Reset buttons to apply or reset the filters.

4. Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

5. Click a SAID in the grid to view the Advisory or click an item in the list and select Advisory details, Devices, Products or Installations that the Advisory relates to.

6. Click ☐ to export the results to a CSV file.

Advisory Details

The Advisory Details page displays Overview, Devices, Products and Installations details for the selected Advisory.

Click ☐ in the Devices, Products and Installations tabs to export the results to a CSV file.

Under Advisory Details > Overview is a Zero Day field. Zero Day refers to a vulnerability that is actively exploited prior to its disclosure. A zero day is one criteria to increase criticality. For example, a typical "Highly Critical" vulnerability becomes an “Extremely Critical” vulnerability.
### Google Chrome Multiple Vulnerabilities

<table>
<thead>
<tr>
<th>Advisory ID</th>
<th>SA7042</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation Date</td>
<td>2017-09-22</td>
</tr>
<tr>
<td>Criticality</td>
<td>- Highly critical</td>
</tr>
<tr>
<td><strong>Zero Day</strong></td>
<td>No</td>
</tr>
</tbody>
</table>

**Software**
- **Google Chrome 51.x**

**CPE**: NIL

**Affected operating system and software**

<table>
<thead>
<tr>
<th>Device Details</th>
<th>Installed products</th>
<th>Advisories</th>
<th>Queue scans</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPE: NIL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CWE Reference**
- CWE-2017-0122 (CWE-2017-0121)

**CVE References**
- CVE-2017-0122
Create Advisory Tickets

From the Assessment > Advisories > Advisory List page, you can create advisory tickets to remediate vulnerabilities affecting your devices.

**Task**

To create Advisory Tickets:

1. Select the appropriate advisory in the grid and click Create Ticket. When the Create Ticket pop-up window appears, the Secunia Advisory ID will be populated in the Advisory field.

2. From the Status drop-down list, select the appropriate status. The default ticket statuses are Open, Handled, Closed, or Irrelevant. See Default Ticket Statuses in Ticket Manager for more information.

3. From the Priority drop-down list, select the appropriate priority. The default ticket priorities are Low, Medium, High or Urgent.

4. From the Queue drop-down list, select a queue to assign the ticket to.

5. From the Assigned to drop-down list, list, select an individual to assign the ticket to.

6. In the Add comment field, add an appropriate comment to the ticket (mandatory).

7. Click Save.
The Patching module is not available for Software Vulnerability Research.

The patching feature in Software Vulnerability Research remediates software vulnerabilities in third-party applications. Software Vulnerability Research provides Patch and Grouped Patch Libraries that list all patches available for your environment, provides patch templates and build packages to deploy patches, and tracks deployed patches.

- Patch Library
- Templates
- Packages
- Deployment
- Patching Tickets
- Manual Signatures

Important - Before you can patch, the following Daemon for Windows activities must be completed first.

- Install the Daemon
- WSUS Configuration and Certificate Troubleshooting
- Saving Successful WSUS Self-Signed Certificates
- Create a Group Policy to Deploy Your Certificate

Patch Library

The Patch Library page displays details of all patches available for your environment.
Task  
To view patches:

1. Open the **Patching > Patch Library** page.
2. Click **1** to filter the patches by **Affecting my environment** (yes/no), **CVE**, **Product name**, **Vendor name**, **Secure version**, **SAID**, and **Has template** (yes/no). In the Patch Library grid, the default sorting view includes sorting first by the **Vendor** column (A-Z) and then by the **Product** column (A-Z).
3. Click the **Apply** or **Reset** buttons to apply or reset the page layout.
4. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
5. Click an item in the grid to select **View templates** (if a template already exists), **Create patch template** or **Build packages**.
6. Click **4** to export the results to a CSV file.

To select and deploy patches in your environment, see **Patch Template and Build Package**.

Templates

The **Templates** page displays a list of Patch templates that you have created and saved. Each template is linked to the specific product version the template was created for.
5. Click an item in the grid to select **Edit, View Packages, or Delete**.

6. To delete multiple templates, select the appropriate templates in the grid and click the **Actions** button.

7. Click **A** to export the results to a CSV file.

---

### Packages

The **Packages** page displays details of all packages available for your environment.

---

**Task**

**To view packages:**

1. Open the **Patching > Packages** page.

2. Click **1** to filter the packages by Language (select the required installation language or languages from the drop-down list), Package name, Vendor name, Package status (select Not ready, Building, Ready or Error building from the drop-down list), Platform (select All, Windows, Mac, Red Hat, Android or IOS from the drop-down list), and Architecture (select 32-bit, 64-bit or 32-bit/64-bit from the drop-down list).

3. Click the **Apply** or **Reset** buttons to apply or reset the filters.

4. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

5. Click an item in the grid and select Details, Download, **Create deployment**, **View deployments**, or **Delete** to view the package deployment details for the selected item. Select the check boxes next to the grid items to select from the Actions drop-down menu.

  - **Details** provides information regarding the package’s unique metadata and origin.
  - **Download** allows you to store the physical file for initial testing purposes before deploying it.
  - **Create deployment** provides options for where you want to publish the patches.
  - **View deployments** takes you to the Deployment menu. You can filter this view to show similarly deployed packages.
  - **Delete** packages.

6. To publish or delete multiple packages, select the appropriate packages in the grid and click the appropriate option under the **Actions** button.

   **Note** - *If you choose to publish the selected packages, you must select the server(s) to publish the package to in Package Deployment.*
7. Click to export the results to a CSV file.

### Deployment

The Deployment page displays details of all patches published in your environment.

#### Task

**To view deployments:**

1. Open the Patching > Deployment page.

2. Click to filter the deployments by Package, Vendor, Server, From and To dates, and the **Status Options**:
   - Pending
   - Loaded
   - Completed
   - Failed
   - Pending Delete
   - Deleted
   - Waiting for signature

3. Click the Apply or Reset buttons to apply or reset the filters.

4. Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

5. Click an item in the grid, and you should see the options **Information**, Refresh status (of the Daemon), **Update Deployment**, or Delete Deployment.

6. To delete multiple deployments, select the appropriate deployments in the grid and click the Actions button.

7. Click to export the results to a CSV file.

### Information

After clicking Information, you can view the package deployment details for the selected item.
If you need to see where a package has been published or you need to change the publishing options for one or more patches, click Update Deployment and the **Choose where to publish the patch(es)** dialog box will open. Make the needed changes and click OK.

### Patching Tickets

After you **Create a Workflow Rule to Create a Patching Ticket**, you can view and export patching ticket information and delete patching tickets.

#### Task To view and export patching tickets:

1. Open the **Patching > Tickets** page.
2. To filter the results by ticket status, select one of the bold ticket statuses in the upper-left-hand corner followed by a ticket count. The default ticket statuses are **Open**, **Waiting**, **Handled**, and **Irrelevant**. See Default Ticket Statuses in **Ticket Manager** for more information.
3. Click ☐️ to filter the results by ID, **From** and **To** dates, **Queue**, **Priority**, **product**, **vendor**, **SAID**, and **Assigned User**.
4. Click the **Apply** or **Reset** buttons to apply or reset the filters.
5. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

6. Click a Secunia Advisory ID (SAID) to view detailed information related to the Advisory.

7. To view one ticket, click the appropriate ticket check box in the grid and select the **Affected Devices** (lists all devices affected by the ticket) or **View**, **Edit**, or **Delete** the ticket. To view multiple tickets, click the appropriate ticket check boxes in the grid and select an option from the Actions drop-down menu such as **Delete multiple tickets** (see Delete Patching Tickets) or **Edit multiple tickets**.

8. Click **Export** to export tickets to a CSV file.

### Delete Patching Tickets

To delete Patching Tickets, perform the following steps.

| Task | To delete patching tickets:
|------|---------------------------
| 1.   | Open the **Patching > Tickets** page.
| 2.   | Insert a check mark in front of the ticket or tickets to delete.
| 3.   | To delete one ticket, select **Delete** under the listed ticket in the grid.
| 4.   | To delete multiple tickets, select **Delete multiple tickets** from the **Actions** drop-down menu.
| 5.   | When the “Are you sure you want to delete these tickets” pop-up window appears, click **Yes**.

![Are you sure you want to delete these tickets?](image)

Yes  No

### Manual Signatures

Using Manual Signatures (also known as External Signatures) allows separating the privilege of Windows Server Update Services (WSUS) administration from the privilege to mark a package as trusted for deployment. With automatic signatures (typically, but not always, using a self-signed certificate), the WSUS administrator has full access to a digital certificate and private key that is trusted by all the machines within the organization. With Manual signatures, WSUS, and thus the WSUS administrator, does not require access to the private key.

The following sections describe how to process a manual signature:

- Enable Manual Signatures
- Deploy the Agent for a Manual Signature
- Deploy a Patch Package for a Manual Signature
- Manual Signature Notifications
Enable Manual Signatures

This section describes how to enable manual signatures and how to **Share Unsigned and Signed .cab Files**.

<table>
<thead>
<tr>
<th>Task</th>
<th>To enable manual signatures:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Connect a daemon to your Software Vulnerability Research account by going to <strong>Settings &gt; Assessment &gt; Update Servers &amp; Daemon</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Select a daemon.</td>
</tr>
<tr>
<td>3.</td>
<td>Click the <strong>More Info</strong> action. In the pop-up, you will see a summary of the current state: the label <strong>Digital signatures: Automatic</strong> and the button <strong>Sign packages manually</strong>.</td>
</tr>
<tr>
<td>4.</td>
<td>Toggle the <strong>Sign packages manually</strong> button to create the desired state: the label <strong>Digital signatures: Manual</strong> and the button <strong>Sign packages automatically</strong>.</td>
</tr>
</tbody>
</table>

**Daemon #73 Info**

- **Version**: Daemon/6.0.3.305
- **Daemon ID**: 3b1109f-22fa-4b4e-ab89-22526c7829f
- **Machine ID**: [redacted]
- **Digital signatures**: Manual
- **Created**: 2018-02-12 06:49:40
- **Last connected**: 2018-02-12 09:29:41

**Note** • The daemon will continue to process requests from the Software Vulnerability Research server while waiting for the signed .cab file, regardless how long it takes. However, if a new agent is released during this window, the process will deploy the older version of the agent.

**Note** • Enabling manual digital signatures changes the behavior of two Software Vulnerability Research patching processes: **Deploy the Agent for a Manual Signature** and **Deploy a Patch Package for a Manual Signature**. Both processes now require a manual step to sign a .cab file before it can be deployed to WSUS. Reverting to automatic digital signatures results in future packages being signed with the certificate that WSUS is configured to use, just like occurred before the introduction of manual signature support. In all cases, the signature that is applied to a .cab file must be trusted by downstream machines, or updates will not be applied.

Share Unsigned and Signed .cab Files

To access unsigned and signed .cab files from other machines, create and share the following folders:

- **Unsigned files** (read only is fine): `C:\ProgramData\Flexera Software\SVMPD IO\Unsigned`
- **Signed files** (only useful if writable): `C:\ProgramData\Flexera Software\SVMPD IO\Signed`
Chapter 10  Patching
Manual Signatures

**Note** • Altering or removing these shared folder names while a file is being signed will result in stale paths being shown in the Software Vulnerability Research user interface. Wait until no files are waiting for signatures before changing shared folder names.

**Deploy the Agent for a Manual Signature**

To deploy the Agent for a manual signature, perform the following steps.

**Task**

To deploy the agent for a manual signature:

1. Click **Deploy Agent**.

2. Select any target groups.

3. Click **Deploy Agent**.

4. Once initiated, the daemon will download the current agent binary and build a `.cab` file containing it. Then a **Sign Agent Package** pop-up displays the location of the unsigned `.cab` file to deploy the agent and a location to place the signed copy of this `.cab` file.
Chapter 10  Patching
Manual Signatures

Note • These two locations have one or two buttons each. Copy Path will always be shown. This button copies the content of the box above it and enables you to open File Explorer and paste the path. You may also manually copy the path by selecting it and hitting Ctrl+C or equivalent. If, as shown here, the machine running the daemon has been configured with the appropriate file shares, the paths will leverage this and Open Folder will be shown. In some browsers (notably Internet Explorer and Edge), Open Folder will open File Explorer to the path; in others, Open Folder may do nothing.

5. Copy the unsigned .cab file from the location mentioned under Unsigned file and invoke your organization’s process for getting it signed. Once the .cab has been signed, copy the file into the folder mentioned under Signed file. The daemon will find the signed file, and, if the signature and chain of trust are verified, deployment to WSUS will continue.

Deploy a Patch Package for a Manual Signature

To deploy a Patch Package for a manual signature, perform the following steps.

Task  To deploy a patch package for a manual signature:

1. Navigate to Patching > Packages.
2. Select a package.
3. Click Create Deployment.
4. Select any target groups.
5. Click OK.
6. If there are no packages, select a product in Patching > Patch Library.
7. Create a template if necessary, and click **Build Packages**. Once deployment is initiated, the daemon will download the patch package and build a .cab file containing it.

8. When the status **Waiting for signature** appears in the **Status** column under **Patching > Deployment**, click **Sign Package** (first screen shot below). Then a **Manual Digital Signatures** pop-up appears with the location of the unsigned .cab file and a location where a signed copy of this .cab file should be placed (second screen shot below).

   ![Manual Digital Signatures](image)

   **Manual Digital Signatures**
   **Install/Update 7-zip 15.x to 16.x**

   **Unsigned file**
   Get the unsigned file from this location:
   `C:\Program Files\Flexera Software\VMSVMPD 10\Unsinged\66fb56fd-4963-4e19-b277-49b8834ed73`
   
   ![Copy Path](image)

   **Signed file**
   Place signed file in this location:
   `C:\Program Files\Flexera Software\VMSVMPD 10\Signed\66fb56fd-4963-4e19-b277-49b8834ed73`
   
   ![Copy Path](image)

   ![Close](image)

   **Note** • These two file locations have one or two buttons each. **Copy Path** will always be shown. This button copies the content of the box above it and enables you to open File Explorer and paste the path. You may also manually copy the path by selecting it and hitting Ctrl+C or equivalent. If, as shown here, the machine running the daemon has not been configured with the appropriate file shares, the paths will be local to the machine running the daemon, and **Open Folder** will not be shown.

9. Access the daemon machine to copy the unsigned .cab file from the location mentioned under **Unsigned file** and invoke your organization's process for getting it signed. Once the .cab has been signed, copy the file into the folder mentioned under **Signed file**. The daemon will find the signed file, and, if the signature and chain of trust are verified, deployment to WSUS will continue.

   **Note** • If multiple patch packages are all waiting for signature, it is safe to place signed .cab files in their respective signed paths in any order. The daemon will deploy the packages as they arrive.

### Manual Signature Notifications

Typically, there is a pause between requesting to deploy an agent and the unsigned .cab file becoming available. To address this issue, you can notify the proper users that a .cab file is ready to be signed, where to get the .cab file and place it. To receive a notification, set up a rule in **Settings > Workflow Management > Rules**.
Task **To create a rule to send a notification when a .cab file is ready to be signed:**

1. Add a new rule by clicking the green plus sign in the upper-right hand corner.
2. Specify a rule name, such as Manual Signing, and optionally a description.
3. Select the Rule Trigger channel *Patch* and the trigger *Package ready for manual signing*.
4. Add and configure any desired actions, such as Email.
5. Enable the rule.
6. Save the rule.

Once the package is ready for your signing process, the configured notifications are sent. These notifications include links to the relevant part of the Software Vulnerability Research user interface (either to the Deployment or the Daemon). These notifications also include the unsigned and signed paths, if the medium permits, as there is no further need to visit the Software Vulnerability Research user interface to complete the manual signing process.
Policy Manager

Edition • The Policy Manager module is not available for Software Vulnerability Research - Assessment Only.

You can use the Policy Manager pages to configure internal Compliance Policy Rules to associate with your account and view the details of breaches to your policies.

• Overview
• Policies
• Breaches

Overview

Click a Policy name or Ticket number to view detailed information about the Policy or Ticket.

Click an item in the grid to view policy breaches, view, edit or delete a policy, or click to create a new policy and specify:

• Rule Name—Define a unique name for the Compliance Policy Rule.
• Apply Scope—Define if the rule should apply globally to all users or to a specific user and Watch List.
• Set Policy Rule Criteria (optional)—Define your tolerances for handling advisories based on the Ticket Priorities, Ticket Status, Criticality (Severity Rating), CVSS (Common Vulnerability Scoring System) Base Score and Threat Score. The interval starts from the date when the Advisory was added to the ticketing system.

Note • Set Policy Rule Criteria based on Threat Score (optional) requires purchase of Threat Intelligence Module

Policies

You can use this page to create a new policy and specify the policy rules.
To create a new policy, perform the following steps:

**Task**

**To create a new policy:**

1. To create a new policy, click ✚.

2. **Add new Policy** dialog box appears. Enter a unique name for the Compliance Policy Rule in the **Rule Name** field.

3. Click on the **Apply scope** drop-down and select the following from the list:
   - Apply to all Watch Lists and users
   - Apply only to one user
   - Apply only to one Watch List
   - Apply only to one User Group

   To apply a scope for the specific User, Watch List, or User Group then select **Apply only to one user,** **Apply to one Watch List,** or **Apply only to one User Group** respectively.

4. The **Set Policy Rule Criteria** fields are optional and you can follow the dialog box instructions to create criteria to specifically fit your requirements.

5. Select **Enable / Disable Policy Breach Warning Email** option and then select the number of days in the **Send Policy Breach Warning Email Before** field.

   If you select this option, then you will be able to send a policy breach warning emails for applicable open or waiting tickets. This warning can be configured for priority based rule of the policy and will enable the ticket assignees to prioritize their tickets. You will be able to configure the number of days before the policy breach, to send such a warning.
6. Click the **Save** button to begin receiving alerts regarding breaches to the policies you have created.

7. Click on any policy in the grid and select **Breaches, View, Edit, Disable** or **Delete**.

**Note** • The email notifications will include SLA days as defined in policy rule criteria for priority. If more than one policy is associated with a newly released advisory, the lowest defined SLA days, will be shown in the email.

**Note** • The email notifications will include CVSS overall score.

---

**Breaches**

The **Breaches** page displays details of active and inactive breaches to the policies you created. Click an item in the grid to view or edit the breach details. Click **Export** to export the results to a CSV file.
Use the **Analytics** pages to filter data contained in the widgets and to create dynamic reports on Advisories, Tickets, Devices and Products.

The Analytics widgets are dynamic, and you can segment information by clicking the individual chart legends or segments in any widget to alter the data displayed accordingly.

- **Advisories**
- **Tickets**
- **Devices**
- **Products**
- **Reports**
- **LiveUpdate**

**Advisories**

The **Advisories** page displays widgets that contain information regarding:

- **Secunia Advisories**—Displays a month-by-month bar chart of the number of advisories based on your configured Watch Lists.
- **Advisories by year**—Displays a bar chart of the number of advisories based on your configured Watch Lists.
- **Advisories by level of criticality**—Displays a color coded pie chart of the criticality levels (Extremely critical, Highly critical, Less critical, Moderately critical, None (Rejected) and Not critical) of advisories based on your configured Watch Lists.
- **Advisories by solution status**—Displays a color coded pie chart of the solution status (None (Rejected), Partial Fix, Unpatched, Vendor Patched and Vendor Workaround) levels of advisories based on your configured Watch Lists.
- **Advisories by attack vector**—Displays a color coded pie chart of the attack vector (From local network, From remote, Local system, and None (Rejected)) of advisories based on your configured Watch Lists.
• **Advisories by CVSS score**—Displays a bar chart of the CVSS score intervals for the Advisories. The intervals follow standard mathematical notation, for example, \((3, 4]\) means strictly greater than 3 and less than or equal to 4. The interval starts from the date when the advisory was added to the ticketing system.

The Analytics widgets are dynamic, and you can segment information by clicking the individual chart legends or segments in any widget - with the exception of Secunia Advisories and Advisories by year - to alter the data displayed in all widgets and the Advisory details grid accordingly.

**Note** • Click the icon to see more information about the widget.

---

**Task**  
To view analytics for advisories:

1. Open the [Analytics > Advisories](#) page.
2. Click to filter the results by Watch List, From and To dates, and Criticality (select from drop-down menu).
3. Click the Apply or Reset buttons to apply or reset the filters.
4. Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
5. Click Save Layout to save the page layout. Adjusting the size of the widgets activates this function.
6. In the example above, clicking the **Extremely critical** legend in the Advisories by level of criticality widget, and then clicking Refresh grid, displays the relevant data.

7. Click the legends or segments again to return to the original, unfiltered, information displayed.

8. Click a Secunia Advisory ID (SAID) to view the complete Advisory details, including (where applicable) the Creation Date, Criticality (Severity Rating), Zero Day (yes or no), Impact (Consequence), Where (Attack Vector), Solution Status, Secunia CVSS (Common Vulnerability Scoring System), CVE References, Affected operating system and software, Affected watch lists, Related tickets, Advisory Description, Reason for rating, Original advisory references and Changelog. Click **Download PDF** to save a copy of the advisory.

**Advisories by Threat Score**

This page displays a bar chart of the number of advisories by threat scores.
Note • Please note the following:

- **Advisory by threat score** chart and **Threat Score** column in the grid requires purchase of the Software Vulnerability Research Threat Intelligence module.
- To purchase this module, contact your sales representative or contact us online at: [https://www.flexera.com/about-us/contact-us.html](https://www.flexera.com/about-us/contact-us.html)
- For more details about the Threat Intelligence Modules, see our datasheet: [https://www.flexera.com/media/pdfs/datasheet-svm-threat-intelligence-module.pdf](https://www.flexera.com/media/pdfs/datasheet-svm-threat-intelligence-module.pdf)

## Tickets

The Tickets page displays widgets that contain information regarding:

- **Ticket performance**—Displays a month-by-month bar chart of the performance of ticket handling based on ticket priority.
- **Ticket priority**—Displays a color coded pie chart of the priority (High, Low, Medium, and Urgent) of all tickets.
- **Ticket status**—Displays a color coded pie chart of the status (Open, Waiting, Handled and Irrelevant) of all tickets.
- **Tickets queue**—Displays a color coded pie chart of the number of tickets assigned to each queue you created.

The Tickets widgets are dynamic and you can segment information by clicking the individual chart legends or segments in any widget - with the exception of Ticket performance - to alter the data displayed in all widgets and the Ticket details grid accordingly.

**Note** • **Click the icon to see more information about the widget.**
Task

To view analytics for tickets:

1. Open the Analytics > Tickets page.
2. Click ☰ to filter the results by From and To dates, Ticket Queues, Status, Watch Lists, and SAID.
3. Click the Apply or Reset buttons to apply or reset the filters.
4. Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
5. Click Save Layout to save the page layout. Adjusting the size of the widgets activates this function.

Devices

The Devices page displays widgets that contain information regarding:

- **Devices by System Score**—Displays a color-coded pie chart for devices grouped by system score.
- **Devices by Criticality**—Displays a color-coded pie chart for devices grouped by criticality levels.
- **Devices by Attack Vector**—Displays a color-coded pie chart for devices grouped by attack vector.
- **Devices by Solution Status**—Displays a color-coded pie chart for devices grouped by solution status.
The Devices widgets are dynamic, and you can segment information by clicking the individual chart legends or segments in any widget to alter the data displayed.

Note • Click the icon to see more information about the widget.

Products

The Products page displays widgets that contain information regarding:

- **Products by Criticality**—Displays a color-coded pie chart for products grouped by criticality levels.
- **Products by Attack Vector**—Displays a color-coded pie chart for products grouped by attack vector.
- **Products by Solution Status**—Displays a color-coded pie chart for products grouped by solution status.

The Products widgets are dynamic, and you can segment information by clicking the individual chart legends or segments in any widget to alter the data displayed.

Note • Click the icon to see more information about the widget.
Reports

You can generate reports based on the current state of all Device Groups, Devices, Products, Watch Lists, Advisories and Tickets. This convenient and powerful feature allows you to schedule reports to run at any time of the day, with any recurrence, and with no user interaction necessary.

The Reports page displays a list of reports that have been configured and scheduled for generation.

Click ☑ and select either Add Research Report or Add Assessment Report to create a new report, or click an existing report in the grid to Edit, View Files or Delete the report. The reports are provided in PDF format and are sent to the assigned recipients based on your configuration.

Task To create a new Research report:

1. Click ☑ and select Research Report.
2. Specify the Time Frame and Generation Schedule for the report. From the drop-down list, select:
   - **One-Time Report**—Generate only one report for a specific time frame.

   *Note* • When searching for advisories within a specific date period for a One-Time Report, use the year, month, and date format. Example: To view only the July 2018 advisories, use the query **Start Date:** 2018.07.01 and **End Date:** 2018.07.31.

   - **Recurring Report**—Generated based on the configured time frame and recurrence schedule.
3. Configure the Start Date and End Date for the report.

4. Select the Watch List(s) or Watch List Group(s) from which data will be used for the report from the drop-down list:

5. Select the Relevant Advisories to be included in the report. The time frame configured above will be used for selecting the relevant advisories. You can optionally select an additional time frame to include for comparative purposes. You can select:
6. Specify the type of Tickets statistics to be included in the report:

- **Type of Tickets Statistics** (choose from the drop-down list)
- **Include Action History**

You can choose to include the Action History view in the report. Select the option here if desired, as well as the additional optional configuration parameters:

- **Include Ticket Comments**
- **Only Include Tickets**:
  - with a Criticality Rating of (choose from the drop-down list) or Above
  - with the following Attack Vectors (choose from the drop-down list)
  - with the following Solution Status (choose from the drop-down list)
  - with the following Impact Types (choose from the drop-down list)
7. Select the **User Groups** to receive the generated report form the drop-down list.

8. Specify the **General Configuration Options** (PDF File name, Report Title, and Generate CSV advisory data) for the generated report:

9. Click **Save**. Once saved, you and the specified recipients will begin to receive notifications and reports based on your configuration.

---

**Creating a New Assessment Report**

To create a new Assessment Report, perform the following steps.

---

**Task**  
**To create a new Assessment Report:**

1. Click ➕ and select Assessment Report.

2. Specify the **Time Frame** and **Generation Schedule** for the report. From the drop-down list, select:
• **One-Time Report** - Generate only one report for a specific time frame.
• **Recurring Report** - Generated based on the configured time frame and recurrence schedule.

3. Configure the **Start Date** and **End Date** for the report.

4. Select the **Device Groups** from which data will be used for the report from:

5. Select the **Device** statistics from the drop-down list to be included in the report. You can select multiple statistics:

6. Select the **Product** statistics from the drop-down list to be included in the report. You can select multiple statistics:
7. Select the **Relevant Advisories** to be included in the report. The time frame configured above will be used for selecting the relevant advisories. You can optionally select an additional time frame to include for comparative purposes. You can select:

- **Type of Advisory Statistics** (choose from the drop-down list)
- **Select Additional Time Frame for Comparison** (choose from the drop-down list)

You can choose to include a detailed list of advisories in the report. You can further filter this by a minimum criticality to refine the output:

- **Include Detailed Advisory List**
- **Only Include Advisories**:
  - with a Criticality Rating of: (choose from the drop-down list) or Above
  - with the following Attack Vectors (choose from the drop-down list)
  - with the following Solution Status (choose from the drop-down list)
  - with the following Impact Types (choose from the drop-down list)
- **Sort Advisories List by**: (choose from the drop-down list)
8. Specify the type of Tickets statistics to be included in the report:
   - **Type of Tickets Statistics** (choose from the drop-down list)
   - **Include Action History**
     
     You can choose to include the Action History view in the report. Select the option here if desired, as well as the additional optional configuration parameters:
   - **Include Ticket Comments**
   - **Only Include Tickets**:
     - with a Criticality Rating of (choose from the drop-down list) or Above
     - with the following Attack Vectors (choose from the drop-down list)
     - with the following Solution Status (choose from the drop-down list)
     - with the following Impact Types (choose from the drop-down list)

9. Select the **User Groups** to receive the generated report form the drop-down list.

10. Specify the **General Configuration Options** (PDF File name, Report Title, and Generate CSV device, advisory and product data) for the generated report:
11. Click Save. Once saved, you and the specified recipients will begin to receive notifications and reports based on your configuration.

**LiveUpdate**

As in our previous LiveUpdate capability, Software Vulnerability Research natively accounts for new vulnerability data based on existing scan data. After you have scanned your system, the scanned data is stored in Software Vulnerability Research’s database. LiveUpdate automatically runs in the background to identify any new advisories that have come in since you last scanned your system. As soon as new vulnerabilities are added to the Secunia Vulnerability Research Database, LiveUpdate will reference your latest scan results against it. As a result, you’ll find out immediately if you’re affected without having to run another scan.

**Important** • LiveUpdate is limited to your current scanning filters for devices and products.
The Ticket Manager page lists all issued tickets. Use this page to:

- View and Change Tickets Status and Priority
- Create Tickets in Ticket Manager
- Delete Tickets in Ticket Manager
- Default Ticket Statuses in Ticket Manager

View and Change Tickets Status and Priority

The following is a view of Change Tickets status and priority.

To view and change ticket status and ticket priority, perform the following steps.

**Task**  
*To view and change ticket status and ticket priority:*

1. Open the Ticket Manager page.

2. To filter the results by ticket status, select one of the bold ticket statuses in the upper-left-hand corner followed by a ticket count. The default ticket statuses are *Open*, *Waiting*, *Handled*, and *Irrelevant*.

3. Click 📊 to filter the results by ID, *From* and *To* dates, *Queue*, *Priority*, and *Assigned User*. 
Create Tickets in Ticket Manager

To create tickets in Ticket Manager, perform the following steps.

**Task**

**To create tickets in Ticket Manager:**

1. Open the Ticket Manager page.
2. Click to create a ticket.
3. From the Status drop-down list, select the appropriate status. The default ticket statuses are Open, Handled, Closed, or Irrelevant. See Default Ticket Statuses in Ticket Manager for more information.
4. From the Priority drop-down list, select the appropriate priority. The default ticket priorities are Low, Medium, High or Urgent.
5. From the Queue drop-down list, select a queue to assign the ticket to.
6. From the Assigned to drop-down list, list, select an individual to assign the ticket to.

4. Click the Apply or Reset buttons to apply or reset the filters.
5. Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
6. To view one ticket, click the appropriate ticket check box in the grid to View, Edit, or Delete the ticket. To view multiple tickets, click the appropriate ticket check boxes in the grid and select an option from the Actions drop-down menu such as Delete multiple tickets (see Delete Tickets in Ticket Manager) or Edit multiple tickets.
7. Click to export tickets to a CSV file.
8. Click to Create Tickets in Ticket Manager.
7. In the **Add comment** field, add an appropriate comment to the ticket (mandatory).

8. Click **Save**.

---

### Default Ticket Statuses in Ticket Manager

The default ticket statuses are used to run and display reports. While you are free to configure the ticket statuses, priorities and queues as you see fit, Flexera needs to know your equivalent “open” statuses to be able to correctly report the statistics.
The following are the default ticket statuses:

**Table 13-1 • Default Ticket Statuses**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Tickets</td>
<td>An Open Ticket is one for which no action has yet been triggered.</td>
</tr>
<tr>
<td>Waiting Tickets</td>
<td>A ticket is marked as Waiting when it has been decided that an action needs to be taken at a later stage.</td>
</tr>
<tr>
<td>Handled Tickets</td>
<td>A ticket is considered Handled when the appropriate action has been taken.</td>
</tr>
<tr>
<td>Irrelevant Tickets</td>
<td>A ticket is considered Irrelevant when it has been closed and is no longer considered of importance to you.</td>
</tr>
</tbody>
</table>
The **Settings** pages allow the main Administrator account holder to create and manage other accounts.

**Note** • Administrators can access the **Settings** pages, and any changes made will effect all users. Depending on the rights given to a User Group, some users may also have access to some of the **Settings** pages.

Use the **Settings** pages to:

- View details of your **Account License Status**, **Account Options** and **Security Policy**
- Perform **User Management** tasks
- Configure **SSO Settings**.
- View, create and add **Vulnerability Management** for Watch List Groups and subscriptions, Ticket queues, statuses and priorities
- Create and edit **Workflow Management Rules**, **Ticket Queues**, **Ticket Status** and **Ticket Priorities**.
- View and edit **Assessment** configurations for the Update Servers & Daemon, Scan Configuration, and Downloads.
- View the **API Access token generation page**.
- View **Logs** for tracking details of all activities taken by users related to your account.

**Account**

Use the **Account** pages to view your license information, manage your Account options, and edit your security policies.

- **License Status**
- **Account Options**
- **Security Policy**
Chapter 14  Settings

User Management

License Status

Use the License Status page to view your license information, including the expiration date, the modules that you are entitled to use according to your subscription, detailed license attributes, and the number of licenses available, which is tracked as the number of used users.

Account Options

Use the Account Options page to edit your account settings and manage settings that apply to all users, for example, show or hide rejected advisories.

Security Policy

You can edit your security policy by selecting the appropriate box below and clicking Update.

Note • Two factor authentication is considered as a best practice for the application.

User Management

The User Management pages display the Users, User Groups, and Roles associated with your account. You can create active Users up to the license limit of your account.

• Users
• User Groups
Users

The Users page displays the users associated with your account and, if applicable, the User Groups the user belongs to. Click add and enter the required information to add a new user.

A valid email address is required for creating a new user. After a user is created, we will send an email to their email address. After clicking the link in the email, the user will be able to set the password for the account. After successfully registering the account, the user can then log on. Only active users are counted with regards to enforcing the user count. If the user has reached their user count limit, they can disable an unused user to recover a license and create another user.

In addition, if an account has for example five licenses and five active users, the user can create the sixth user. The additional user will be disabled by default when created, and the user will not be able to activate their account until the account manager handles the license issue.

Click download to download a CSV file containing details of all Users associated with your account.

Click a Username in the list and select Edit, Reset two factor login, Disable, or Delete.

Note • Depending on the user profile, the Reset two factor login option may not be available.

Blocked Users

When user enters a wrong credentials for seven times during login to the Software Vulnerability Research application, their credentials will get blocked.

To unblock the blocked users, follow the below steps:

Task

1. Locate the list of user account details in Settings > User Management > Users. In the Blocked column, Yes will be marked for the respective users.

2. Select the user details and click Unblock button.

3. Now in the Blocked column, Yes will be changed to No.
User Groups

Users can be grouped into User Groups, and different user profiles can be assigned to the different User Groups. It is also possible to share data between User Groups for easier collaboration within your organization. There is no limit to the number of User Groups that can be created.

The User Groups page displays the User Group Name, Description, Roles and Users associated with the group. Click and enter the required information to add a new Group. You can select the role or roles to apply to the group from the drop-down list.

User groups can be linked to one or several predefined User profiles for access control.

Click a User Group in the grid to Edit or Delete the User Group or Users to add or delete users to/from the User Group.
Roles

The **Roles** page displays details of the available User Group Roles. Roles are predefined and cannot be changed.

*Note* • Administrator and API User Management users can access complete data of the API.

SSO Settings

On the Settings > User Management tab, you can specify SSO Settings.

**IDP Configuration Instructions**

Under **SSO Settings** on the Settings > User Management tab, you can specify the following **IDP Configuration Instructions** settings.

**Table 14-1 • SSO Settings / IDP Configuration Instructions**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Sign On URL</td>
<td>This field lists the application’s single sign-on URL. You will need to enter this URL into the settings for your chosen Identity Provider.</td>
</tr>
<tr>
<td>Account Key</td>
<td>Set this field in your Identity Provider (IdP) as a SAML attribute named accountKey.</td>
</tr>
<tr>
<td>Generate and Show Key</td>
<td>Click to generate and display the Account Key.</td>
</tr>
</tbody>
</table>

*Note* • This key is not stored on the SVR server. Make sure that you keep it in a safe place. If you lose it, you may regenerate the key, but doing so will invalidate the old key.
Service Provider Configuration

Under SSO Settings on the Settings > User Management tab, you can specify the following Service Provider Configuration settings.

Table 14-2 • SSO Settings / Service Provider Configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO Enabled</td>
<td>Select this option to enable Single Sign-On.</td>
</tr>
<tr>
<td>Disable standard login</td>
<td>If you are using Single Sign-On at your organization, select this option to disable standard login options for all of your users (except root). Important: Before selecting this option, make sure that SSO is working correctly, to prevent user lockout.</td>
</tr>
<tr>
<td>Upload IDP Metadata XML file</td>
<td>Select this option if you want to upload the IDP metadata XML file.</td>
</tr>
<tr>
<td>Provide IDP Metadata URL</td>
<td>Select this option if you want to enter the identity provider metadata URL into the IDP Metadata URL field.</td>
</tr>
<tr>
<td>Automatically create new users</td>
<td>Select this option to automatically create new users.</td>
</tr>
<tr>
<td>Default groups for new users</td>
<td>Specify the default group for new users.</td>
</tr>
</tbody>
</table>

Note • For more information on Single Sign-On, see Configuring Single Sign-On (SSO).

Vulnerability Management

The Vulnerability Management pages display the settings for Watch List Groups and Watch List Subscriptions.

- Watch List Groups
- Watch List Subscriptions
Watch List Groups

Use **Watch List Groups** to group **Watch Lists**, for example All XYZ Products, together. Click ➕ to create a new Watch List Group or click a Watch List Group in the grid to edit or delete the group.

Watch List Subscriptions

This page displays the **Watch Lists** Subscription details including **Watch List**, **Watch List Owner**, **Subscriber**, **Enforced by** admin, **Email Notification level** and **SMS notification level**.

Admin user can add, edit or delete subscriptions to the created watch list.

**Task**  
**Add Subscription to Watch List**

1. Open the **Settings > Vulnerability Management > Watch List Subscriptions** page.

2. To add a new subscription, Click ➕. The **Add subscription** tab opens.

3. Watch List created as shown in **Create Watch Lists** will appear in the **Watch List** drop down, Select the watch list.

4. Add a required user from the **Subscriber** drop down.

5. Select any of the below **Email notification level** from the drop down based on the requirement
   - Extremely Critical
   - Highly Critical and Above
   - Moderately Critical and Above
   - Less Critical and Above
   - Not Critical and Above
Chapter 14  Settings
Vulnerability Management

- Rejected and Above
- None

6. Select any of the below SMS notification level from the drop down based on the requirement:
   - Extremely Critical
   - Highly Critical and Above
   - Moderately Critical and Above
   - Less Critical and Above
   - Not Critical and Above
   - Rejected and Above
   - None

7. Click Save to add the subscription to the watch list.

8. List of added subscriptions will appear in the Settings > Vulnerability Management > Watch List Subscriptions, Admin user can edit or delete any existing subscription from the list.

9. Select the required subscription from the list, you can see the Edit and Delete button.

10. Click Delete button to delete the selected subscription from the list.

11. Click Edit button to edit the Subscriber, Email notification level and SMS notification level of the selected subscription.
Workflow Management

Workflow Management allows you to set up detailed workflows that align with processes already in use within your organization. There is no limit to the number of Workflows that can be created.

Use the Workflow Management pages to create and edit Rules, Ticket Queues, Ticket Status and Ticket Priorities.

- Rules
- Ticket Queues
- Ticket Status
- Ticket Priorities

Rules

Rules can partially or fully automate workflow. They can only be created by an Administrator and must contain at least one trigger and one action. For a list of rule triggers and actions, see Rule Channels, Triggers, and Actions. If needed, you can configure many different options into one rule.
To create a rule, see Create a Workflow Rule - Overview.

Workflow Rules can be created for many tasks. You can customize your workflow rule or use one of the Software Vulnerability Research Default Workflow Rule Examples.

The Rule channels, their associated triggers, and available actions are shown in the following table.
Table 14-3 • Rule Channels, Triggers, and Actions

<table>
<thead>
<tr>
<th>Channel</th>
<th>Trigger</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advisory</td>
<td>• Advisory for Watch List approved</td>
<td>• Email</td>
</tr>
<tr>
<td></td>
<td>• Any Watch List or select a Watch List from the drop-down list</td>
<td>• SMS</td>
</tr>
<tr>
<td></td>
<td>• Any Watch List Group or select a Watch List Group from the drop-down list</td>
<td>• Notify</td>
</tr>
<tr>
<td></td>
<td>• Select Advisory Condition or select a Advisory Condition from the drop down list</td>
<td>• Create Advisory for Watch List</td>
</tr>
<tr>
<td></td>
<td>• Advisory for Watch List changed</td>
<td>• Create ticket</td>
</tr>
<tr>
<td></td>
<td>• Any Watch List or select a Watch List from the drop-down list</td>
<td>• Change ticket assignment</td>
</tr>
<tr>
<td></td>
<td>• Any Watch List Group or select a Watch List Group from the drop-down list</td>
<td>• Change ticket queue</td>
</tr>
<tr>
<td></td>
<td>• Select Advisory Condition or select a Advisory Condition from the drop down list</td>
<td>• Change ticket status</td>
</tr>
<tr>
<td></td>
<td>• Advisory released for a Watch List with approval flow</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Any Watch List or select a Watch List from the drop-down list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Any Watch List Group or select a Watch List Group from the drop-down list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Select Advisory Condition or select a Advisory Condition from the drop down list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Advisory released for a Watch List</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Any Watch List or select a Watch List from the drop-down list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Any Watch List Group or select a Watch List Group from the drop-down list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Select Advisory Condition or select a Advisory Condition from the drop down list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Product version end-of-life</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Notify for all, default only for my tracked product versions (select Yes or No from the drop-down list)</td>
<td></td>
</tr>
</tbody>
</table>

**Note** • Threat Score details are added in the Email notification for users with the Threat Intelligence Module.
### Table 14-3 • Rule Channels, Triggers, and Actions (cont.)

<table>
<thead>
<tr>
<th>Channel</th>
<th>Trigger</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advisory</strong></td>
<td>• Advisory Threat for Watch List changed</td>
<td>• Email PDF report</td>
</tr>
<tr>
<td>(continued)</td>
<td>• Any Watch List or select a Watch List from the drop-down list</td>
<td>• Email</td>
</tr>
<tr>
<td></td>
<td>• Any Watch List Group or select a Watch List Group from the drop-down list</td>
<td>• SMS</td>
</tr>
<tr>
<td></td>
<td>• Select Advisory Condition or select a Advisory Condition from the drop down list</td>
<td>• Notify</td>
</tr>
<tr>
<td></td>
<td>• Skip trigger if score decreases (Select Yes or No from the drop down list)</td>
<td></td>
</tr>
</tbody>
</table>

**Note** • This add-on requires purchase of the Software Vulnerability Research Threat intelligence Module

<table>
<thead>
<tr>
<th>Analytics</th>
<th>• PDF Report Generated</th>
<th>• Email PDF report</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Email</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SMS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Notify</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Patch</th>
<th>• Patch available, with template</th>
<th>• Email</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Patch available, without template</td>
<td>• SMS</td>
</tr>
<tr>
<td></td>
<td>• Patch affecting my environment (select Yes or No from the drop-down list)</td>
<td>• Notify</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Patch - Create packages</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Patch - Publish packages</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create ticket</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy</th>
<th>• Policy Breached</th>
<th>• Email</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• SMS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Notify</td>
</tr>
</tbody>
</table>

| Release Notes| • New Release arrived                                                   | • Email                                |

SVR-JUNE2023-UG00 Software Vulnerability Research User Guide
Note • The available actions will vary depending on the channel and trigger you select.

Default Workflow Rule Examples

Software Vulnerability Research includes several Default Workflow Rules:

- Create a Workflow Rule to Send an Advisory and Ticket Information After Approval
- Create a Workflow Rule to Create a Patching Ticket
- Create a Workflow Rule to Send a New Release Notes Notification to Non-Administrators

Create a Workflow Rule to Send an Advisory and Ticket Information After Approval

Workflow Rules can be created for many tasks. For example, the Workflow Rule below can be used when Flexera issues an advisory for a Watch List that requires management approval and the communication of management’s approval and ticket information to all Watch List users using email, PDF attachments, and SMS.

Task Create a Workflow Rule to send an advisory and ticket information after approval

1. Follow steps 1-3 from the task Create a Workflow Rule.
2. From the drop-down Rule Trigger List:
   - Select Advisory from the Channel list

Table 14-3 • Rule Channels, Triggers, and Actions (cont.)

<table>
<thead>
<tr>
<th>Channel</th>
<th>Trigger</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticketing</td>
<td>• Ticket assigned to me</td>
<td>• Email</td>
</tr>
<tr>
<td></td>
<td>• Ticket changed</td>
<td>• SMS</td>
</tr>
<tr>
<td></td>
<td>• Changed by me (select Yes or No from the drop-down list)</td>
<td>• Notify</td>
</tr>
<tr>
<td></td>
<td>• Ticket created</td>
<td>• Create ticket</td>
</tr>
<tr>
<td></td>
<td>• Ticket priority changed</td>
<td>• Change ticket status</td>
</tr>
<tr>
<td></td>
<td>• Ticket queue changed</td>
<td>• Change ticket queue</td>
</tr>
<tr>
<td></td>
<td>• Ticket status changed</td>
<td>• Change ticket assignment</td>
</tr>
<tr>
<td>User</td>
<td>• Password changed</td>
<td>• Email</td>
</tr>
<tr>
<td></td>
<td>• User (select from the drop-down list)</td>
<td>• SMS</td>
</tr>
<tr>
<td></td>
<td>• User Logged in</td>
<td>• Notify</td>
</tr>
<tr>
<td></td>
<td>• User (select from the drop-down list)</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 14  Settings
Workflow Management

- Select **Advisory released for a Watch List** from the Trigger list
- Enter the appropriate Watch List and Watch List Group information
- Select **Advisory Condition**
- Click Save

3. For actions, select **Create Ticket** and **Send email**. When an advisory is released, a ticket is created and the Watch List Group users will receive an email with the ticket information and the Advisory as a PDF attachment. See the following screen shot for details.

Note • Customized workflow rules for Watch Lists take precedence over non-customized workflow rules using the following hierarchy from most important to least important:

- Rule for a specified watch list
- Rule for a watch list group
- General rule with no watch list or watch group

For example, if a watch list is in a customized workflow rule with a watch list selected and in a rule with a watch group selected, only the rule specified for the watch list will execute.

However, when you have two identical customized workflow rules that affect the same watch list or the same watch list group, the system will not know which rule takes precedence. Therefore, neither customized workflow rule will execute.

Note • The PDF attachment option is set at the user level. Any user wishing to receive PDF advisory information needs to select this option from the **User Profile** page. Under **Personal settings** ensure the following options have been enabled: **Receive normal emails** for Advisory type email and **Yes** for Attach advisory PDF. See the screen shot below for details.
Create a Workflow Rule to Create a Patching Ticket

You can create a Workflow Rule to create a ticket for when a new patch is available.

**Task** Create a Workflow Rule to create a patching ticket:

1. Select either rule: **Patch available no profile notification** or **Patch Available with custom profile** and click **Edit**.
2. Click **Add action**.
3. When the **Choose Action** pop-up window appears, click **Create ticket**.
4. Enter the **Ticket Status** and **Ticket Queue** information and click **Save**. Add any additional actions required and save the rule.
5. To view and export patching ticket information, see **Patching Tickets** in the **Patching** module or in the **Ticket Manager**.

Create a Workflow Rule to Send a New Release Notes Notification to Non-Administrators

You can create a Workflow Rule to notify non-administrators of the latest Software Vulnerability Research release notes.

**Note** • *All administrator accounts are configured to receive release note notification emails in the Notifications module.*

**Task** To create a Workflow Rule to send a new release notes notification to non-administrators

1. Select **New release notes** rule.
2. Enter the appropriate users to **Notify**.
3. Click **Email**.

Ticket Queues

This page displays the **Ticket Queue** details.
Ticket Queues can be used for sharing and limiting access to tickets for users. You can create ticket queues that are relevant to a limited subset of your users (for instance only for Linux administrators or for Windows administrators) and use Rules to create tickets from special Watch Lists directly on those ticket queues.

Click a queue in the list to edit or delete the queue or click to add a new ticket queue.

**Ticket Status**

This page displays the **Ticket Status** values.

Click to add a ticket status. The default values are:

- Open
- Waiting
- Handled
- Irrelevant

You can click any ticket status that you have added to edit it or delete statuses that do not have tickets assigned.

**Ticket Priorities**

This page displays the **Ticket Priority** values.

Click to add a ticket priority. The default values are:

- Low
You can click any Ticket Priority that you have added to edit or delete priorities that do not have tickets assigned.

Assessment

*Edition • These Assessment settings are not available for Software Vulnerability Research.*

Under Assessment, you can Update Servers & Daemon, perform a Scan Configuration, and perform Downloads of current and older versions of agent installers, agents, and daemons.

- Update Servers & Daemon
- Scan Configuration
- Downloads

Update Servers & Daemon

This page displays details of all Windows Server Update Services (WSUS) servers and how to install, configure and troubleshoot the Software Distribution Daemon for Windows in your environment.

- Daemon Resources
- Daemon and WSUS Troubleshooting
- Certificate Configuration
- Certification Authorities

Daemon Resources

This section explains:

- Daemon Software Requirements
- Certificate Configuration
- Daemon Command Line Switches

Daemon Software Requirements

The Software Distribution Daemon for Windows has the following software requirements.

- 64 Bit Operating System. Windows 7 +
- Windows Server Update Services (WSUS) administrative console needs to be installed. You need to install the admin tools version that corresponds to your WSUS server.
• Access Privileges to run the Daemon as a service
• Access Privileges to makes changes to the WSUS server
• .Net 4.52
• Internet Connection – SSL 443/TCP to https://app.flexerasoftware.com/

Daemon Log File Size

As the Daemon runs, it logs important actions, warnings, and errors. When logging to a file, the size and backup strategy of this file are controlled by the registry values named LogFile, LogMaxKB, and LogBackup. LogFile specifies the name of the active log file. LogMaxKB specifies the size at which the log file is backed up and restarted. LogBackup specifies a date string format that is appended to the name of the log file to create each backup file. If LogMaxKB is 0 or negative, the log file grows forever. If LogBackup is empty, the current log is instead discarded when it grows past the specified size.

The screen shot below lists the default settings for the Daemon log.

Daemon Command Line Switches

Software Vulnerability Research has the following daemon command line switches.

• Help
• Help Text
• Force Daemon to Poll the Server for New Tasks
• Force Daemon to Poll the Server for New Tasks
• Daemon Command Line to Create WSUS Certificate
• Ask Daemon to Display Where an Update Will Be Applied

Help

To access the help command line switch type:

svmpd.exe help

Help Text

To access the help text command line switch type:

SVM Package Daemon Copyright (C) 2012-2017 Flexera Software LLC. All rights reserved.
Usage: svmpd.exe ACTION [OPTIONS]
ACTION is one of:
NewCert: Create a WSUS publishing certificate
Scan: Scan a WSUS server for data
ServiceCommand: Send the service a custom command
ShowPackageStats: Get installation statistics for a package, by group
UseCert: Set the WSUS publishing certificate
Version: Show version information
Or help [ACTION]: Get detailed help for ACTION
All actions support the following global flags in any location:
/cli: One of LogAlways, Critical, Error, Warning, Informational, Verbose
Set the level for console logging
/output or /o: <String>
Save output to specified file
/format or /f: One or more of Raw, Indent, Compress
Control JSON output format. Compress only works with /output.
/wsus: <Uri>
Override the WSUS server

Force Daemon to Poll the Server for New Tasks
To force the daemon to poll the server for new tasks type:
svmpd.exe servicecommand polltasksnow

Daemon Command Line to Create WSUS Certificate
To create a WSUS certificate, type the following Daemon command line:
svmpd.exe newcert

Ask Daemon to Display Where an Update Will Be Applied
The following Daemon command line displays where an update will be applied.
svmpd.exe showpackagestats bc5f5d64-f2aa-4c6d-bd3f-8cf9915cfb82
After typing the above command line, you will see the following output.

```json
{
    "server_name": "svm-w16-wsus.svm.flexdev.com",
    "group_id": "af6f2ec0-b1ce-4344-9f61-9e3e0cb6cda3",
    "group_name": "Windows 8.1",
    "approvals": [
    {
        "by": "SVM\JSmith",
        "at": "2017-05-25T20:58:57.213Z",
        "action": 0,
        "is_optional": false
    }
    ],
    "not_applicable": 0,
    "pending": 4,
    "installed": 0,
    "failed": 0
},
{
    "server_name": "svm-w16-wsus.svm.flexdev.com",
    "group_id": "a0a08746-4dbe-4a37-9ad6-9e7652c0b421",
    "group_name": "All Computers",
...}
```
"approvals": [
  {
    "by": "SVM\JSmith",
    "at": "2017-05-25T20:58:57.193Z",
    "action": 0,
    "is_optional": false
  },
  "not_applicable": 1,
  "pending": 18,
  "installed": 0,
  "failed": 1
},
{
  "server_name": "svm-w16-wsus.svm.flexdev.com",
  "group_id": "b73ca6ed-5727-47f3-84de-015e03f6a88a",
  "group_name": "Unassigned Computers",
  "approvals": [
    {
      "by": "SVM\JSmith",
      "at": "2017-05-25T20:58:57.2Z",
      "action": 0,
      "is_optional": false
    },
    "not_applicable": 0,
    "pending": 2,
    "installed": 0,
    "failed": 0
  },
{
  "server_name": "svm-w16-wsus.svm.flexdev.com",
  "group_id": "8b4b8cf9-4d99-48fc-93ce-bdb16ce624e1",
  "group_name": "Windows 7",
  "approvals": [
    {
      "by": "SVM\JSmith",
      "at": "2017-05-25T20:58:57.21Z",
      "action": 0,
      "is_optional": false
    }
  ],
  "not_applicable": 0,
  "pending": 8,
  "installed": 0,
  "failed": 1
  },
{
  "server_name": "svm-w16-wsus.svm.flexdev.com",
  "group_id": "57c2d480-05c5-4a2a-9a18-df11281559ca",
  "group_name": "Windows 10",
  "approvals": [
    {
      "by": "SVM\JSmith",
      "at": "2017-05-25T20:58:57.203Z",
      "action": 0,
Daemon and WSUS Troubleshooting

This section provides troubleshooting for the following topics:

- Daemon Configuration
- WSUS Configuration and Certificate Troubleshooting
- Daemon Logging

Daemon Configuration

If the User Account you have set up does not have the ability to run a service, the following error message will appear:
**Task**

To troubleshoot the configuration of the Daemon:

1. Leave the error message up.
2. Go to the Services applet and find the Flexera Software Vulnerability Research Daemon.
3. Right click Properties.
4. Go to the Log On tab and set the same user, which will trigger Windows to add that account to the correct group. When the Services window appears, click OK.
5. Go back to the error message and click Retry to complete the installation.

WSUS Configuration and Certificate Troubleshooting

If you enter the incorrect WSUS server settings in the registry, you will see an error message like the one below.

```
c:\Program Files\Flexera Software\SVM Daemon>svmpd.exe scan Groups System.NotSupportedException
Error providing service IWsusApi
```

Before you enter the correct registry key and WSUS Server, make sure the service is STOPPED. Otherwise, the registry key value will be erased when you do stop the service, and you will need to reenter the registry key.

To create WSUS certificates, see:

- Daemon Command Line to Create WSUS Certificate
- Saving Successful WSUS Self-Signed Certificates

Daemon Logging

Logs are written here:

C:\ProgramData\Flexera Software\SVM

You can customize the following logging level settings.

- Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Flexera\SVMPD
- LogLevel: Can be Informational, Verbose
- WSUSServer: Scheme, URL and Port for WSUS. Example: http://svm-w16-wwsus.svm.flexdev.com:8530/
Successful Publishing Log Example

Below is an example of a successful publishing log.


```
{   "SvmServer": "https://uat-agent.app.flexerasoftware.com/api/",
    "WsusServer": "http://svm-w16-wsus.svm.flexdev.com:8530/",
    "AccountAuthToken": "01019198908c81ef89330d2f913d0fe05f13619a2a34c5dd23821f3b009cb8872a0381e4daa4a05e33e68c4a53a4ca36e48680b22522c73cb003e65f6e6bcbbd726787dd5d8be31fd4bca67ac77fc2d128b46f50a9f2df512433f9f512777f15ad9d5e5a9b20c8517d14570fca7a669787bd39bc529a4393cf70024f472737f87a9797705737c78be366efa19450d6dbd9783ff2cc7",
    "RefreshToken": "01019198908c81ef89330d6d013d0ffd51f3619a2a34c5dd23821f3b009cb8872a0381e4daa4a05e33e68c4a53a4ca36e48680b22522c73cb003e65f6e6bcbbd726787dd5d8be31fd4bca67ac77fc2d128b46f50a9f2df512433f9f512777f15ad9d5e5a9b20c8517d14570fca7a669787bd39bc529a4393cf70024f472737f87a9797705737c78be366efa19450d6dbd9783ff2cc7",
    "TempToken": "01019198908c81ef89330d6d013d0ffd51f3619a2a34c5dd23821f3b009cb8872a0381e4daa4a05e33e68c4a53a4ca36e48680b22522c73cb003e65f6e6bcbbd726787dd5d8be31fd4bca67ac77fc2d128b46f50a9f2df512433f9f512777f15ad9d5e5a9b20c8517d14570fca7a669787bd39bc529a4393cf70024f472737f87a9797705737c78be366efa19450d6dbd9783ff2cc7",
    "GUID": "dbbad2b3-b298-4f01-ad4b-717df294f6f2",
    "LogMethod": "File",
    "LogLevel": "Verbose",
    "LogFile": "<CommonApplicationData>\Flexera Software\SVM\svmpd.log",
    "LogMaxKB": "16384",
    "LogBackup": "-yyyyMMdd-HHmm",
    "SvmLastPolled": "5/24/2017 6:01:54 PM +00:00",
    "SvmLastPollSuccess": "5/24/2017 6:01:54 PM +00:00",
    "SvmPollPeriod": "00:10:00"
}
--- Configuration Ends ---
**Certificate Configuration**

Certificates are saved based on the certificate process used:

- Saving Successful WSUS Self-Signed Certificates
- Saving Manual Self-Signed Certificates

### Saving Successful WSUS Self-Signed Certificates

A successful WSUS self-signed certificate must be saved in the following three locations: Trusted Root Certification, Trusted Publishers, and WSUS. The "Trusted Root Certification Authority" should contain the relevant Root certificate.
Not copying the certificate’s public key to any one of the three locations (in particular the Trusted Publishers location), or not having the private key in the WSUS location, may cause publishing to fail with the following error message.

[5/22/2017 7:03:30 PM[C] Task execution faulted (id: adc97f47-5c41-442b-b19d-f266a2d8adec): Verification of file signature failed for file: \\win2008r2sccm12.isas.flexdev.com\UpdateServicesPackages\6e16403a-042f-49db-9106-7d0fab24bf9\bbee425c-fa3d-46dd-a793-065fd184fe86_1.cab

InvalidOperationException: Verification of file signature failed for file: \\win2008r2sccm12.isas.flexdev.com\UpdateServicesPackages\6e16403a-042f-49db-9106-7d0fab24bf9\bbee425c-fa3d-46dd-a793-065fd184fe86_1.cab


Troubleshooting Options for WSUS Self-Signed Certificate Error Message

You have two options to create the new certification if this error message appears:

c:\Program Files\Flexera Software\SVM Daemon>svmpd.exe newcert

This WSUS server cannot issue a self-signed certificate. To import a signing certificate into the WSUS server, use one of the following supported methods:
1. SetSigningCertificate(string, string)
2. SetSigningCertificate(string, SecureString)

**Task**

**To create a WSUS self-signed certificate:**

1. Enable self-signing on the server. While the WSUS will not generate self-signed certificates by default, it is possible to restore the legacy behavior by setting the following registry key.

   - HKEY_LOCAL_MACHINE\Software\Microsoft\Update Services\Server\Setup\
   - Create DWORD value: EnableSelfSignedCertificates = 1

   *Note* • The CreateSelfSignedCertificate API is still considered deprecated and may be removed in a future version of Windows. For further details, see [https://blogs.technet.microsoft.com/wsus/2013/08/15/wsus-no-longer-issues-self-signed-certificates/](https://blogs.technet.microsoft.com/wsus/2013/08/15/wsus-no-longer-issues-self-signed-certificates/)

2. Use a real certificate, and use the `svmpd.exe` option **UseCert**.

**Saving Manual Self-Signed Certificates**

The certificate used to sign packages must be saved on the machine with the Software Distribution Daemon for Windows (`SVMDaemonINstall.msi`).

**Certification Authorities**

If you see the following Windows Update 800b0109 error message, this means your WSUS certificate is not installed on the machine trying to install the update.
Scan Configuration

Use this page to view, configure and edit the:

- Scan Configuration
- Microsoft Update Options
- Add Custom Scan Paths
Scan Configuration

Click **Edit** and select:

- Scan type (select Disabled (do not scan), Minimal scan, Optimal scan or Full scan from the drop-down list). For details, see Scan Types.
- Scan day(s) (select the day or days to perform scans from the drop-down list)
- Scan time

**Note** • The selected Scan Type does not overwrite custom scan paths you create, which are saved to every Scan Agent you have deployed to your environment.

Microsoft Update Options

Click **Edit** and select:

- **Configure the behavior of the Windows Update (WUA)** (select Check for missing security updates from Windows Update. If your organization blocks updates from Windows Update, select Check for missing security updates from Microsoft System Center).
- **Update Server Type** (select OS Default, Managed Windows Update, Official Windows Update, Official Microsoft Update or Use offline method (CAB) from the drop-down list):
  - **OS Default**: allows the Windows Update Agent on a device being scanned to use whatever option is currently registered. This option can be controlled by enterprise policy settings or locally on the machine, depending on the environment the device is running in.
  - **Managed Windows Update**: the SVMScan.exe agent will request a check for updates through an enterprise managed WSUS instance. On machines not configured through WSUS, this check for updates will result in the error: 0x80244011 "WUServer policy value is missing in the registry".
• **Official Windows Update:** the SVMScan.exe agent will request a check for updates through the public Windows Update server. This check will only return updates related to Windows.

• **Official Microsoft Update:** the SVMScan.exe agent will request a check for updates through the public Windows Update server. This check will return a superset of the "Windows Update server" results that include Windows updates and updates for Microsoft products such as Office (non App-V, non App-X installs only) and MSVC redistributables.

• **Use offline method (CAB):** you should implement the .cab file scanning of windows update for clients that are not connected to the Internet and cannot access WSUS or MU/WU. In such situations, Microsoft provides a .cab file that can be used to scan the system. There are limitations to this feature:
  
  - You are responsible for placing the file in a location accessible by Windows Update Services. The file must be on the local file system; placing the file on a shared drive is not supported by Windows Update Services.
  
  - The alternate scan data source (.cab file) only includes high priority updates (security bulletins, critical updates, update rollups) and some service packs. It does not include optional updates (such as updates, feature packs, and tools) and some service packs. If a machine uses this source for scanning, then it is likely that fewer patches will be detected.
  
  - Software Vulnerability Research should be run as administrator.

• **Update Proxy Settings** (select Use default WUA proxy settings, Use the same proxy as http or Use a custom proxy for WUA from the drop-down list).

• If you selected Use a custom proxy for WUA, enter the Proxy Settings domain port.

Add Custom Scan Paths

Click **+** to add custom scan paths. Select the Type (Allow list or Block List) from the drop-down list, enter the Filename and Path and click Save.

**Note** • Mixing block List and allow list rules is not supported. Allow List will take precedence.

**Note** • All paths must be hard coded paths. Example: C:\Users\Public\Libraries
Downloads

This page displays the Software Vulnerability Research download links for:

- Vulnerable Software Discovery Tool Installer for Windows
- Vulnerable Software Discovery Tool for Windows
- Software Distribution Daemon for Windows
- Vulnerable Software Discovery Tool for Mac
- Vulnerable Software Discovery Tool for Red Hat Linux 7 RPM
- Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM

You can select Show older versions, click an item in the list, and select Download.

To download and deploy the appropriate item below, see Agent Deployment and Daemon Deployment.
API

Use the API page to view your API Access token generation page, XML Feeds, and Service Providers.

XML feed shows advisory information for tickets created. If no tickets are created, no advisory information will appear in the XML feed. XML feed is not connected to Historic Advisories in the Vulnerability Manager module.

To access the Software Vulnerability Research APIs, see https://api.app.flexerasoftware.com/api/. For additional API information, see the Software Vulnerability Research API Help Library:

https://docs.flexera.com/svr/api/Default.htm

Logs

Use the Logs pages to track details of all activities taken by users related to your account, such as:

- Logins
- Tickets
- Watch Lists
- Email Logs
- SMS Logs
- Service Calls

Logins

The Logins page displays the Date, User, IP Address and User Agent details for all successful logins.

Click to filter the results displayed by User and From and To dates
Chapter 14  Settings
Logs

Click ▼ to export Logins to a CSV file.

Tickets

The Tickets page displays the Date, Ticket, Change Type, Change Description and User details for all ticket changes related to your account.

Click ▼ to filter the results displayed by User, Ticket ID and From and To dates.

Click ▼ to export Tickets to a CSV file.

Watch Lists

The Watch Lists page displays the Date, Watch List, Change Type, Change Description and User for all Watch List changes related to your account.

Click ▼ to filter the results displayed by User, Watch List, and From and To dates.

Click a Watch List name to view the details of the Watch List.

Click ▼ to export Watch Lists to a CSV file.

Email Logs

The Email Logs page displays the history of sent emails including Date, User, Email Category, Email Address, Status, and Subject.

Click ▼ to filter the results displayed by User and From and To dates.

Click ▼ to export Email Logs to a CSV file.

SMS Logs

The SMS Logs page displays the history of sent SMS, including Date, User, SMS Category, Phone Number, Status, and Message.

Click ▼ to filter the results displayed by User and From and To dates.

Click ▼ to export SMS Logs to a CSV file.

Service Calls

If service calls were made, the Service Calls page displays the history of changes, including Date, Provider, URL, Method, Ref_object_id, Status code, Our entity, and Call status.

Click ▼ to resend failed service calls.

Click ▼ to filter the results displayed by From and To dates.
Click to export Service Calls to a CSV file.
Use the **User Profile** page to view and edit your account information, including your password, personal details, preferences, security settings, and personal settings.

After saving your phone number, you need to validate your phone number. Otherwise you will not receive SMS notifications for the advisories.

If you change your email address, you need to validate your email address immediately after. Otherwise you will not receive an email notification.
Figure 15-1: User Profile Page
About Secunia Advisories

This section includes the following articles:

- CVSS (Common Vulnerability Scoring System)
- CVE References
- Where (Attack Vector)
- Criticality (Severity Rating)
- Impact (Consequence)

CVSS (Common Vulnerability Scoring System)

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities (see https://nvd.nist.gov/vuln-metrics/cvss).

CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors, and researchers to all benefit by adopting this common language of scoring IT vulnerabilities.

CVSS consists of three groups: Base, Temporal, and Environmental. Each group produces a numeric score ranging from 0 to 10, and a Vector; a compressed textual representation that reflects the values used to derive the score.

- **The Base group** represents the intrinsic qualities of a vulnerability.
- **The Temporal group** reflects the characteristics of a vulnerability that changes over time.
- **The Environmental group** represents the characteristics of a vulnerability that are unique to any user’s environment.

For details on interpreting a CVSS vector, refer to https://www.first.org/cvss/specification-document.

Secunia Advisories include a Secunia derived CVSS score and vector, as well as a link to an implementation of the NIST CVSS calculator so that a user can adjust temporal and environmental metrics for advisories that match your Watch Lists. For more information, see CVSSv3 Score.

The National Vulnerability Database (NVD) CVSS score/vector for each relevant CVE contained in an Advisory is also shown, and is similarly linked to the NIST CVSS calculator.
CVSSv3 Score

On May 18, 2018 Flexera’s Secunia Research began entering all new CVSS scores using the v3 standard. After a CVSSv3 score is entered, the score appears in the User Interface (UI), API, XML, email notifications, and PDF reports.

In the User Interface

The CVSSv3 score is noted with a green “v3” after the score.

In the API

API calls returning CVSS data return a second set of values for CVSSv3, so that you can programatically differentiate between CVSSv2 and CVSSv3 scores. When CVSSv3 scores are available, the cvss_score value is blank and the value will appear as cvss3_score. The label cvss_score represents CVSSv2 (it was not renamed to avoid breaking existing scripts).
In the XML

A change to the schema is necessary to add specific values for CVSSv3 scores. As with the json API values above, a second cvss3 labeled value was added to distinguish v3 scores. Depending on how any scripts or processes consuming this data parse the information, this has the potential to result in a breaking change.

```xml
<cvss_base_score>0</cvss_base_score>
<cvss_overall_score>0</cvss_overall_score>
<cvss_vector></cvss_vector>
<custom_cvss_overall_score>0.0</custom_cvss_overall_score>
<custom_cvss_vector></custom_cvss_vector>
<cvss3_base_score>7.8</cvss3_base_score>
<cvss3_overall_score>6.8</cvss3_overall_score>
<custom_cvss3_overall_score>5.9</custom_cvss3_overall_score>
```

In Email Notifications

Emails contain CVSSv2 (displayed as CVSS) and CVSSv3 (displayed as CVSS3) labels. The CVSSv3 value will be empty until a v3 value is entered, at which time the v2 (CVSS) value will be empty.

<table>
<thead>
<tr>
<th>Criticallity</th>
<th>Not critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>03/11/2022</td>
</tr>
<tr>
<td>Last Update</td>
<td>03/11/2022</td>
</tr>
<tr>
<td>Solution Status</td>
<td>Vendor Patched</td>
</tr>
<tr>
<td>SAID</td>
<td>SA112006</td>
</tr>
<tr>
<td>CVSS</td>
<td>0.0 (E:U/RL:OF/RC:C)</td>
</tr>
<tr>
<td>CVSS3</td>
<td>Base: 4.7, Overall: 4.1</td>
</tr>
<tr>
<td>Impact</td>
<td>Spoofing</td>
</tr>
<tr>
<td>Where</td>
<td>From remote</td>
</tr>
<tr>
<td>Threat Score</td>
<td>0</td>
</tr>
</tbody>
</table>

Note • Email notifications will include CVSS overall score.

In a PDF Report

PDF reports containing CVSS values will show CVSSv2 (displayed as CVSS) or CVSSv3 (displayed as CVSS3) as appropriate.
**CVE References**

A CVE (Common Vulnerabilities and Exposures) name represents a unique, standardized name and description for a given vulnerability or exposure.

Searching on a CVE reference (for example CVE-2009-3793 or simply 2009-3793) will find all Secunia Advisories in the database that list that particular CVE as a reference.

An Advisory can contain more than one CVE reference, and not every Advisory has an associated CVE reference.
Where (Attack Vector)

The following are Where (Attack Vector) values.

Local System

Local system describes vulnerabilities where the attack vector requires that the attacker is a local user on the system.

Local Network

From local network describes vulnerabilities where the attack vector requires that an attacker is situated on the same network as a vulnerable system (not necessarily a LAN).

This category covers vulnerabilities in certain services (for example, DHCP, RPC, administrative services, and so on), which should not be accessible from the Internet, but only from a local network and optionally a restricted set of external systems.

Remote

From remote describes vulnerabilities where the attack vector does not require access to the system nor a local network.

This category covers services, which are acceptable to expose to the Internet (for example, HTTP, HTTPS, SMTP) as well as client applications used on the Internet and certain vulnerabilities, where it is reasonable to assume that a security conscious user can be tricked into performing certain actions.
Criticality (Severity Rating)

The following are Severity Rating values.

**Extremely Critical**
This value is typically used for remotely and easily exploitable vulnerabilities that are otherwise designated “highly critical” but also have been exploited in the wild before their publication (zero-day). These vulnerabilities typically exist in services like FTP, HTTP and SMTP or specific client systems such as email programs or browsers. Operating systems can also be prone to them—e.g., when font handling is performed on operating system level.

**Highly Critical**
- This value is generally used for remotely and easily exploitable vulnerabilities that can lead to system compromise.
- Successful exploitation doesn’t usually require any interaction, but there are no known exploits available at the time of disclosure.
- These vulnerabilities typically exist in services like FTP, HTTP and SMTP or specific client systems such as email programs or browsers. Operating systems can also be prone to them—e.g., when font handling is performed on operating system level.

**Moderately Critical**
This value is usually used for remotely and easily exploitable denial-of-service vulnerabilities against services like FTP, HTTP and SMTP. Additionally, easily exploitable vulnerabilities that could lead to information disclosure or affect the integrity of a product can result in this criticality level.

This rating is also used for vulnerabilities allowing system compromise on LANs in services like SMB, RPC, NFS, LPD and similar services that are not intended for use over the Internet.

**Less Critical**
This value is typically used for cross-site scripting and local privilege escalation vulnerabilities.

This rating is also used for vulnerabilities allowing exposure of sensitive data to local users.

**Not Critical**
This value is typically used for very limited privilege escalation vulnerabilities and locally exploitable Denial of Service vulnerabilities.

This rating is also used for non-sensitive system information disclosure vulnerabilities (for example, remote disclosure of installation path of applications).

Impact (Consequence)

The following are Consequence values.

**Brute Force**
Used in cases where an application or an algorithm allows an attacker to guess passwords in an easy manner.
**Cross-Site Scripting**

Cross-Site Scripting vulnerabilities allow a third party to manipulate the content or behavior of a web application in a user's browser, without compromising the underlying system.

Different Cross-Site Scripting related vulnerabilities are also classified under this category, including "script insertion" and "cross-site request forgery".

Cross-Site Scripting vulnerabilities are often used against specific users of a website to steal their credentials or to conduct spoofing attacks.

**DoS (Denial of Service)**

This includes vulnerabilities ranging from excessive resource consumption (for example, causing a system to use a lot of memory) to crashing an application or an entire system.

**Exposure of Sensitive Information**

Vulnerabilities where documents or credentials are leaked or can be revealed either locally or remotely.

**Exposure of System Information**

Vulnerabilities where excessive information about the system (for example, version numbers, running services, installation paths, and similar) are exposed and can be revealed from remote and, in some cases, locally.

**Hijacking**

Covers vulnerabilities where a user session or a communication channel can be taken over by other users or remote attackers.

**Manipulation of Data**

This includes vulnerabilities where a user or a remote attacker can manipulate local data on a system, but not necessarily be able to gain escalated privileges or system access.

The most frequent type of vulnerabilities with this impact are SQL-injection vulnerabilities, where a malicious user or person can manipulate SQL queries.

**Privilege Escalation**

Covers vulnerabilities where a user is able to conduct certain tasks with the privileges of other users or administrative users.

This typically includes cases where a local user on a client or server system can gain access to the administrator or root account, thus taking full control of the system.

**Security Bypass**

Covers vulnerabilities or security issues where malicious users or people can bypass certain security mechanisms of the application. The actual impact varies significantly depending on the design and purpose of the affected application.

**Spoofing**

Covers various vulnerabilities where it is possible for malicious users or people to impersonate other users or systems.
**System Access**

Covers vulnerabilities where malicious people are able to gain system access and execute arbitrary code with the privileges of a local user.

**Unknown**

Covers various weaknesses, security issues, and vulnerabilities not covered by the other impact types, or where the impact is not known due to insufficient information from vendors and researchers.
Appendix A - Threat Intelligence

Software Vulnerability Research Threat Intelligence directs your attention towards the vulnerabilities affecting your watch lists.

In a world where there are more than 18,000 new vulnerabilities every year, being smart about prioritizing remediation efforts is essential. Leveraging our optional Threat Intelligence Module, another valuable layer of insight is provided to help you understand which of the vulnerabilities affecting your environment are actually being exploited in the wild.

Industry reports, including Gartner shows that between 6%-10% of the vulnerabilities disclosed each year actually are exploited in the wild. Turns out that most of these have medium CVSS scores, which are typically overlooked by organizations. With the insights provided by threat intelligence, it is possible better optimize the time spent remediating software vulnerabilities. Avoid spending time and resources in patching vulnerabilities that do not have evidence of exploitation, and favor those that do. Prioritization is crucial for effective risk mitigation and resource utilization.

Leveraging machine learning, artificial intelligence, and human curation from thousands of sources in the open, deep and dark web, our Threat Intelligence Module augments Software Vulnerability Research’s vulnerability intelligence with a Threat Score that provides the ultimate prioritization tool for your busy desktop operations teams.

This appendix explains how the Software Vulnerability Research Threat Intelligence module helps the enterprises to manage their resources and Patching Vulnerabilities more effectively, the following topics are discussed in this section:

- Evidence of Exploitation
- Criteria for the Threat Score Calculation
- Threat Score Calculation - Examples
- Threat Intelligence Data for Operations and Security
- Threat Intelligence for Research

**Note** • Please note the following:

- **Secunia Advisory Threat Scores and Vulnerability (CVE) Threat Scores** are each calculated as described in the **Criteria for the Threat Score Calculation** section (an Advisory score is not determined by simply adding related CVE Threat Scores).
- For pricing and availability, please contact your sales representative or contact us online at: [https://www.flexera.com/about-us/contact-us.html](https://www.flexera.com/about-us/contact-us.html)
Evidence of Exploitation

There are 10 primary rules that can impact the assigned Threat score and they are:

- It has been linked to remote access Trojan
- It has been linked to ransomware
- It has been linked to penetration testing tools
- It has been linked to malware
- It has been linked to an exploit kit
- It has been linked to a cyber exploit
- It has been linked to an exploit wild
- It has been linked to POC verified
- It has been linked to vulnerability developed tools
- It has been linked to verified intelligence

Criteria for the Threat Score Calculation

Triggered rules increase the score by the values identified in the chart below based on the highest severity level triggered.

Table A-1 • Rules, Severity and Value

<table>
<thead>
<tr>
<th>Rule</th>
<th>Severity</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recently Linked to Remote Access Trojan</td>
<td>Medium</td>
<td>+2</td>
</tr>
<tr>
<td>Historically Linked to Remote Access Trojan</td>
<td>Low</td>
<td>+1</td>
</tr>
<tr>
<td>Recently Linked to Ransomware</td>
<td>Medium</td>
<td>+2</td>
</tr>
<tr>
<td>Historically Linked to Ransomware</td>
<td>Low</td>
<td>+1</td>
</tr>
<tr>
<td>Recently Linked to Penetration Testing Tools</td>
<td>Medium</td>
<td>+2</td>
</tr>
<tr>
<td>Historically Linked to Penetration Testing Tools</td>
<td>Low</td>
<td>+1</td>
</tr>
<tr>
<td>Recently Linked to Malware</td>
<td>Medium</td>
<td>+2</td>
</tr>
<tr>
<td>Historically Linked to Malware</td>
<td>Low</td>
<td>+1</td>
</tr>
<tr>
<td>Recently Linked to Exploit Kit</td>
<td>Medium</td>
<td>+2</td>
</tr>
</tbody>
</table>
### Table A-1 • Rules, Severity and Value

<table>
<thead>
<tr>
<th>Rule</th>
<th>Severity</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Historically Linked to Exploit Kit</td>
<td>Low</td>
<td>+1</td>
</tr>
<tr>
<td>Linked to Recent Cyber Exploit</td>
<td>Low</td>
<td>+1</td>
</tr>
<tr>
<td>Linked to Historical Cyber Exploit</td>
<td>Low</td>
<td>+1</td>
</tr>
<tr>
<td>Recently exploited in the wild</td>
<td>Very Critical</td>
<td>+5</td>
</tr>
<tr>
<td>Exploited in the wild in the past year</td>
<td>Critical</td>
<td>+4</td>
</tr>
<tr>
<td>Historically exploited in the wild</td>
<td>High</td>
<td>+3</td>
</tr>
<tr>
<td>Recent remote code execution POC verified</td>
<td>Critical</td>
<td>+4</td>
</tr>
<tr>
<td>Recent POC verified</td>
<td>High</td>
<td>+3</td>
</tr>
<tr>
<td>Historical remote code execution POC verified</td>
<td>Medium</td>
<td>+2</td>
</tr>
<tr>
<td>Recent possible POC</td>
<td>Medium</td>
<td>+2</td>
</tr>
<tr>
<td>Historical POC verified</td>
<td>Low</td>
<td>+1</td>
</tr>
<tr>
<td>Tools to exploit the vulnerability developed recently</td>
<td>Medium</td>
<td>+2</td>
</tr>
<tr>
<td>Tools to exploit the vulnerability developed historically</td>
<td>Low</td>
<td>+1</td>
</tr>
<tr>
<td>Recently verified intelligence</td>
<td>High</td>
<td>+3</td>
</tr>
<tr>
<td>Historically Verified intelligence</td>
<td>Low</td>
<td>+1</td>
</tr>
</tbody>
</table>

The rule with the highest criticality determines the point range and the starting value for the Threat Score. The ranges for each are as follows:

### Table A-2 • Criticality - Ranges

<table>
<thead>
<tr>
<th>Criticality</th>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Critical</td>
<td>71</td>
<td>99</td>
</tr>
<tr>
<td>Critical</td>
<td>45</td>
<td>70</td>
</tr>
<tr>
<td>High</td>
<td>24</td>
<td>44</td>
</tr>
<tr>
<td>Medium</td>
<td>13</td>
<td>23</td>
</tr>
<tr>
<td>Low</td>
<td>1</td>
<td>12</td>
</tr>
</tbody>
</table>
Table A-2 • Criticality - Ranges

<table>
<thead>
<tr>
<th>Criticality</th>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Note • when assigning a Threat Score to the SAID, we do not simply add up the scores for each associated vulnerability, but rather follow the same rules outlined here to calculate the Security Advisory threat score.

### Threat Score Calculation - Examples

Some examples to explain how we would arrive at a Threat Score.

#### Example 1

A SAID has two CVEs; two come back as exploited.

**Triggered Rules**

The following rules are triggered:

- **CVE1 triggers**
  - Historically Linked to Remote Access Trojan
  - Recent remote code execution POC verified
- **CVE2 triggers**
  - Historically Linked to Exploit Kit

The Threat Score would be **51**.

**Calculating the Score**

The criticality range is set by the most critical rule triggered, which is critical. This sets the score's maximum and minimum range as between 45 and 70.

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score</td>
<td>+45</td>
</tr>
<tr>
<td>Recent remote code execution POC verified</td>
<td>+4</td>
</tr>
<tr>
<td>Linked to Recent Cyber Exploit</td>
<td>+1</td>
</tr>
<tr>
<td>Historically Linked to Remote Access Trojan</td>
<td>+1</td>
</tr>
<tr>
<td><strong>Threat Score (Sum of above values)</strong></td>
<td><strong>51</strong></td>
</tr>
</tbody>
</table>
Example 2
A SAID has seven CVEs; and all come back as exploited.

Triggered Rules
The following rule is triggered by all CVEs:

- CVE1, CVE2, CVE3, CVE4, CVE5, CVE6 and CVE7 triggers
  - Recently Linked to Malware

The Threat Score would be 23.

Calculating the Score
The criticality range is set by the most critical rule triggered, which is critical. This sets the score's maximum and minimum range as between 13 and 23.

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score</td>
<td>+13</td>
</tr>
<tr>
<td>Recently Linked to Malware</td>
<td>+2 * 7 CVE = +14</td>
</tr>
<tr>
<td>Threat Score (Sum of above values)</td>
<td>27</td>
</tr>
</tbody>
</table>

Note • At this point, we have exceeded the maximum for a critical threat, which is 23, so the score is 23.

Example 3
A SAID has one CVE and it comes back as exploited.

Triggered Rules
The following rule is triggered:

- CVE1 triggers
  - Historically exploited in the wild

The Threat Score would be 27.

Calculating the Score
The criticality range is set by the most critical rule triggered, which is high. This sets the score's maximum and minimum range as between 24 and 44.

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score</td>
<td>+24</td>
</tr>
</tbody>
</table>
Threat Intelligence Data for Operations and Security

Software Vulnerability Research and Software Vulnerability Research cater to different audiences with different needs. Software Vulnerability Research (for operations) provides what is needed for Operations to better prioritize remediation efforts. Whereas Software Vulnerability Research (for security) provides more detail to meet the needs of security teams.

Table A-3 • Software Vulnerability Manager vs. Software Vulnerability Research

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Historically exploited in the wild</td>
<td>+3</td>
</tr>
<tr>
<td>Threat Score (Sum of above values)</td>
<td>27</td>
</tr>
</tbody>
</table>

Example 4

A SAID has many CVEs, none come back as exploited.

The score would be 0 because there are no rules triggered.

Advisory with Multiple Vulnerabilities

An advisory Threat Score is based upon each of the CVEs included in an Advisory as specified above. In Software Vulnerability Research, the vulnerabilities that have exploits are indicated with a red circle for easier identification.

Threat Intelligence for Research

The user who purchased the Software Vulnerability Research Threat Intelligence Module, can see the threat intelligence add on feature in the following places:

- Dashboard > Dashboard with Threat Intelligence Module
- Research > Advisories > Advisories with Threat Score
- Analytics > Advisories > Advisories by Threat Score