flexera

Software Vulnerability Research

User Guide

Legal Information

Book Name: Software Vulnerability Research User Guide

Part Number: SVR-JUNE2025-UG00

Product Release Date: June 2025

Copyright Notice

Copyright © 2025 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

1 Software Vulnerability Research Help Library 9

Product Support Resources 11

Contact Us 12

2 Introduction 13

About Software Vulnerability Research 13

Software Vulnerability Editions 14

Optional Modules 15

Software Vulnerability Research Life Cycle 15

System Architecture Overview 16

Getting Started with Software Vulnerability Research 17

3 Software Vulnerability Research Quick Start Guide 19

Account Activation 19

Accept the Flexera Sales Token and Create Your Account 19

Configure Two-Factor Authentication (2FA) 22

Token-Based Two-Factor Authentication 22

SMS-Based Two-Factor Authentication 23

Two-Factor Authentication Recovery 24

Configuring Single Sign-On (SSO) 25

Opening a Support Case 32

System Requirements for Software Vulnerability Research 32

Workflow Management Rules 33

Create a Workflow Rule - Overview 34

Rule Triggers 34

Patch Rule Actions 35

Notification Actions 36

Default Workflow Rules 36

Custom Workflow Rules . . . 37
Additional Patching Information . . . 37

4 Dashboard . . . 39
Dashboard with Threat Intelligence Module . . . 39
Dashboard without Threat Intelligence Module . . . 40

5 Notifications . . . 45

6 Vulnerability Manager . . . 47
Overview . . . 47
Watch Lists & Advisories . . . 48
Watch Lists . . . 48
View Watch Lists . . . 49
Create Watch Lists . . . 50
Edit Watch Lists . . . 52
Import a New Watch List . . . 54
Import an Updated Watch List . . . 57
Historic Advisories . . . 58
Product Advisories . . . 59
Shared Watch Lists . . . 60
FlexNet Manager Suite (FNMS) Import . . . 61
Ticketing in Vulnerability Manager . . . 61
Create Tickets in Vulnerability Manager . . . 62
Delete Tickets in Vulnerability Manager . . . 63
Default Ticket Statuses in Vulnerability Manager . . . 64
Approve Advisories . . . 64

7 Research . . . 67
Advisory Database . . . 67
Advisories . . . 68
Advisories with Threat Score . . . 68
Advisories without Threat Score . . . 70
Rejection Advisories . . . 73
Products Database . . . 74
Vendors . . . 74
Product Versions . . . 75
Products . . . 75
Suggest Software . . . 76
Download Software Suggestion Tool . . . 78
Vulnerability Database . . . 80
Vulnerabilities . . . 80

8 Policy Manager . . . 81

Overview 81
Policies 81
Breaches 83

9 Analytics 85
Advisories 85
Advisories by Threat Score 87
Tickets 88
Devices 89
Products 90
Reports 91
LiveUpdate 93

10 Ticket Manager 95
View and Change Tickets Status and Priority 95
Create Tickets in Ticket Manager 96
Delete Tickets in Ticket Manager 97
Default Ticket Statuses in Ticket Manager 97

11 Settings 99
Account 99
License Status 100
Account Options 100
Security Policy 100
User Management 101
Users 101
User Groups 102
Roles 103
SSO Settings 104
Vulnerability Management 105
Watch List Groups 105
Watch List Subscriptions 105
Workflow Management 107
Rules 108
Default Workflow Rule Examples 111
Ticket Queues 113
Ticket Status 114
Ticket Priorities 114
API 114
Service Providers 115
Configure ServiceNow Instance for Service Provider 115
Create Service Method for Service Providers 116
Logs 117

Logins . . . 117
Tickets . . . 118
Watch Lists . . . 118
Email Logs . . . 118
SMS Logs . . . 118
Service Calls . . . 118

12 User Profile . . . 119

13 About Secunia Advisories . . . 121

CVSS (Common Vulnerability Scoring System) . . . 121
CVSSv4 Score . . . 122
CVSSv3 Score . . . 122
CVE References . . . 125
Where (Attack Vector) . . . 126
Criticality (Severity Rating) . . . 127
Impact (Consequence) . . . 127

A Appendix A - Threat Intelligence . . . 131

Evidence of Exploitation . . . 132
Criteria for the Threat Score Calculation . . . 132
Threat Score Calculation - Examples . . . 134
Threat Intelligence Data for Operations and Security . . . 136
Threat Intelligence for Research . . . 136

B Appendix B - Assessment & Patching . . . 149

Assessment Scenarios . . . 149
Agent-Based Scan – Requirements for Windows . . . 150
Agent-Based Scan – Requirements for macOS . . . 151
Prepare Your Mac . . . 152
Install the Vulnerable Software Discovery Tool for Mac . . . 153
Agent-Based Scan – Requirements for Red Hat Enterprise Linux (RHEL) . . . 153
Install the Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM and 7 RPM . . . 154
Vulnerable Software Discovery Tool Command Line Options . . . 156
Help . . . 156
Version . . . 156
Install . . . 156
Uninstall . . . 157
Modify Settings . . . 158
Controlling the Service . . . 158
Scanning from the Command Line . . . 158
Agent Configuration Options . . . 159
Scanning Via Local Agents . . . 165
Scan Types . . . 166

Assessment Reports **166**
Overview 166
Smart Groups 167
Create a Smart Groups Report 170
Devices 170
Device Details 171
Products 173
Product Details 174
Advisories 175
Advisory Details 175
Create Advisory Tickets 177
Patching **178**
Patch Library 178
Templates 179
Packages 179
Deployment 180
Information 181
Update Deployment 181
Patching Tickets 181
Delete Patching Tickets 182
Manual Signatures 183
Enable Manual Signatures 183
Deploy the Agent for a Manual Signature 184
Deploy a Patch Package for a Manual Signature 186
Manual Signature Notifications 187

C Appendix C - ThreatStream **191**
Analyzing Threat Models and Observables **191**
Viewing CVE Details and Associated Flexera Advisories **196**

1

Software Vulnerability Research Help Library

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

Topic	Content
Introduction	Provides an overview of Software Vulnerability Research: • About Software Vulnerability Research • Software Vulnerability Editions • Optional Modules • Software Vulnerability Research Life Cycle • System Architecture Overview • Getting Started with Software Vulnerability Research
Software Vulnerability Research Quick Start Guide	This quick start guide walks you through setting up the key features of Software Vulnerability Research.
Dashboard	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.
Notifications	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.

Table 1-1 • Software Vulnerability Research Help Library (cont.)

Topic	Content
Vulnerability Manager	Vulnerability Manager pages are used to manage the Vulnerability Intelligence associated with your account. ***Note*** • *The Vulnerability Manager module is not available for Software Vulnerability Research - Assessment Only.*
Research	Vulnerability Tracker (VulnTrack) represents our full Vulnerability Database, which has been updated and maintained since the inception of Secunia in 2002. ***Edition*** • *The Research module is not available for Software Vulnerability Research - Assessment Only.*
Policy Manager	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. ***Edition*** • *The Policy Manager module is not available for Software Vulnerability Research - Assessment Only.*
Analytics	The Analytics pages are used to filter data contained in the widgets and to create and save dynamic reports on Advisories.
Ticket Manager	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
Settings	The Settings pages allow the main Administrator account holder to create and manage other accounts. 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.
User Profile	The User Profile page is used to view and edit your account information, including your password, personal details, preferences, and security settings.
About Secunia Advisories	Describes CVSS (Common Vulnerability Scoring System), CVE References, Where (Attack Vector), Criticality (Severity Rating), and Impact (Consequence).

Table 1-1 • Software Vulnerability Research Help Library (cont.)

Topic	Content
Appendix A - Threat Intelligence	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.
Appendix B - Assessment & Patching	This Appendix explains the following: ● The Assessment Scenarios page provides descriptions of the available assessment scenarios. ● 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 **Average System Score**, **Device Details** and **Product Details**. ● 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. ***Edition*** • *The Assessment & Patching module is not available for Software Vulnerability Research.*
	It provides step-by-step process to investigate vulnerabilities and associated threat models through advanced filtering and select capabilities.

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

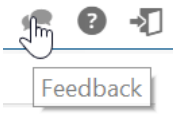
Flexera Support

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

2

Introduction

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
- Software Vulnerability Research Life Cycle
- System Architecture Overview
- 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

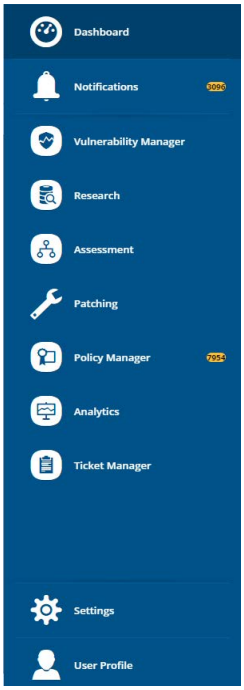
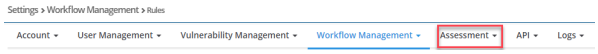
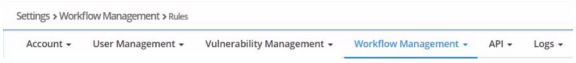
Software Vulnerability Research (includes all modules)	Software Vulnerability Research does not include Assessment or Patching)
 Main Menu	Main Menu

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

Software Vulnerability Research (includes all modules)	Software Vulnerability Research does not include Assessment or Patching)
 Settings Menu	 Settings 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:*

https://www.flexera.com/media/pdfs/datasheet-svm-threat-intelligence-module.pdf

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.

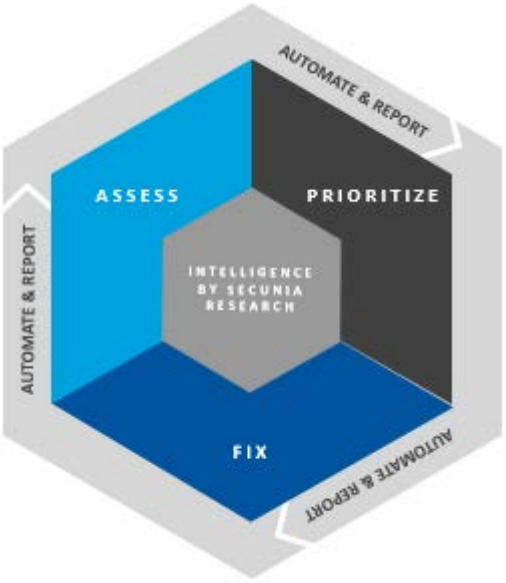


Figure 2-1: Software Vulnerability Research Lifecycle

System Architecture Overview

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

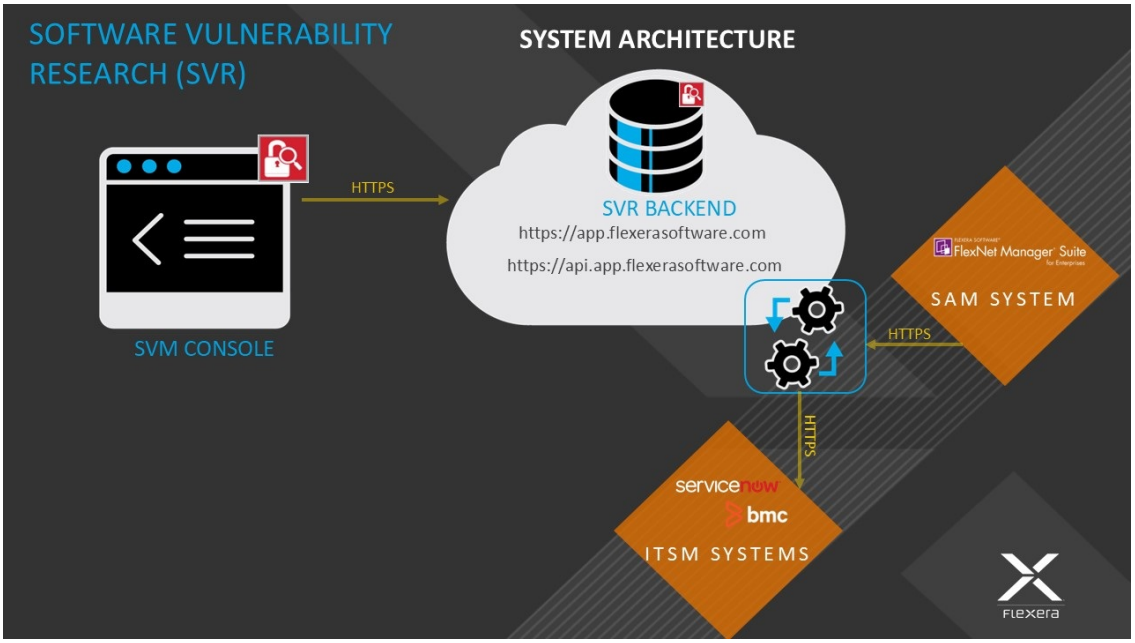


Figure 2-2: System Architecture Overview

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.

3

Software Vulnerability Research Quick Start Guide

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
- Workflow Management Rules

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

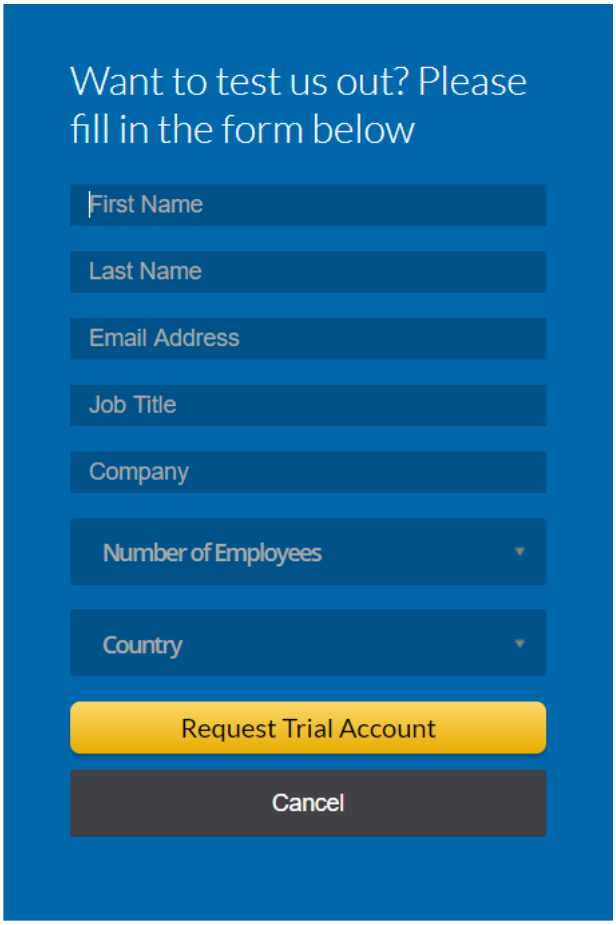
To create your account, perform the following steps.

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

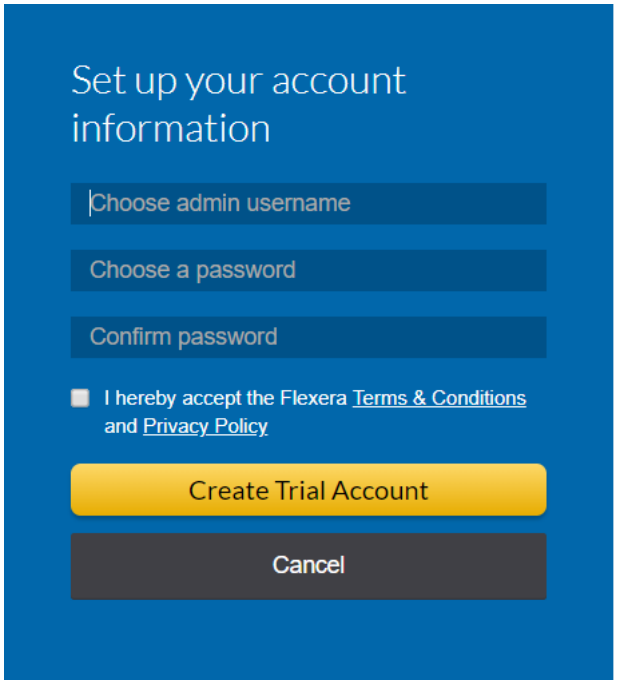
1. After your sales order is complete, you will receive an activation email from Flexera Sales with a customized link to create your account. The link looks similar to the following token:

   `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:



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.

Task ***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 you 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

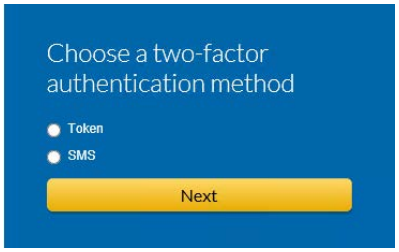


Figure 3-1: Choosing a Two-Factor Authentication Method

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:

  https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

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

  https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8

Logging Into Your Account Using Two-Factor Authentication

To login to your account using two-factor authentication, perform the following steps.

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

1. After entering your username and password, you will be presented with a QR code and a field for the verification code.
2. Open the Google Authenticator application and select the **Scan a Barcode** option.
3. When the application loads the device camera, scan the QR barcode displayed on your computer screen.
4. The mobile application will generate a unique code. Enter this code in the **Verification Code** field at the Software Vulnerability Research Login page.

5. Click **Save** to proceed with logging in to your new account.

SMS-Based Two-Factor Authentication

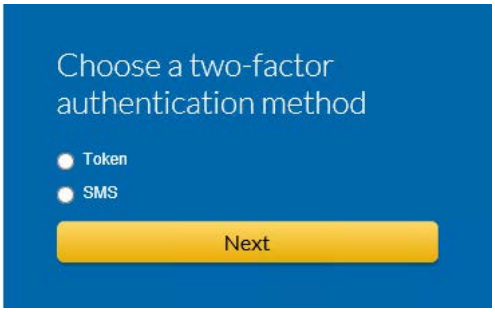
SMS-based two-factor authentication is a less secure and a less reliable method that is available and can be used as a fallback in case your phone does not have an authenticator application.

- 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.

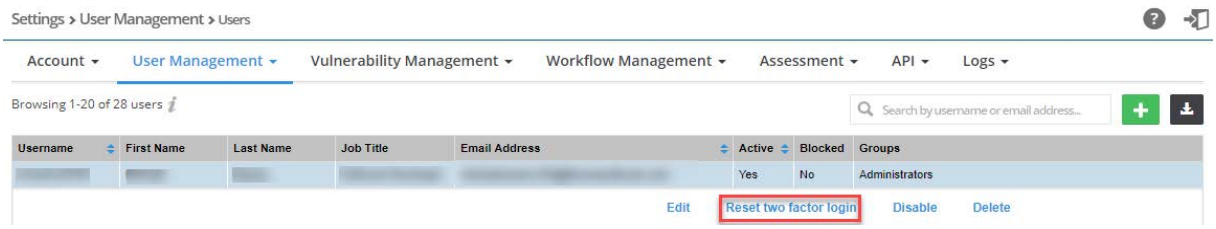
- Recovering Two-Factor Authentication for Main Administrator Accounts
- Recovering Two-Factor Authentication for User Accounts

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.*

Prerequisites

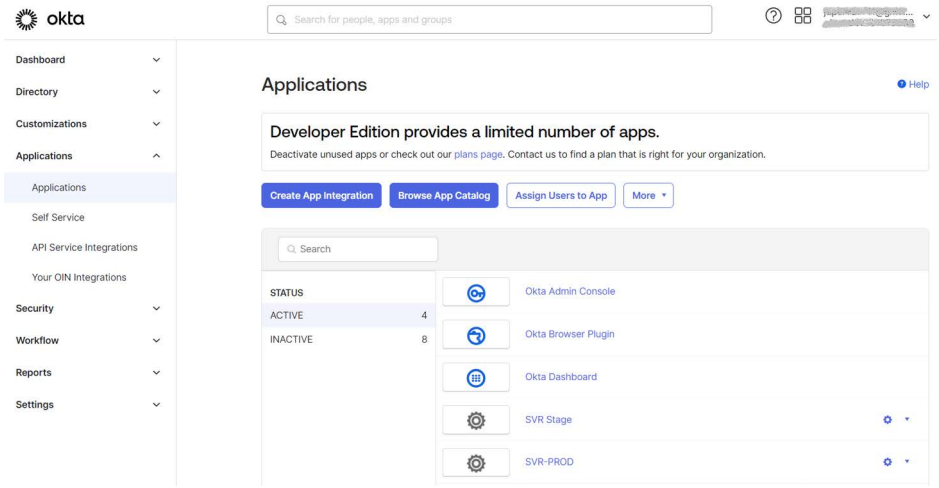
To get started, you need the following:

- An Okta account
- Administrator privileges

To set up Okta (SAML 2.0) to use as a single sign-on (SSO) with Software Vulnerability Research, perform the following steps.

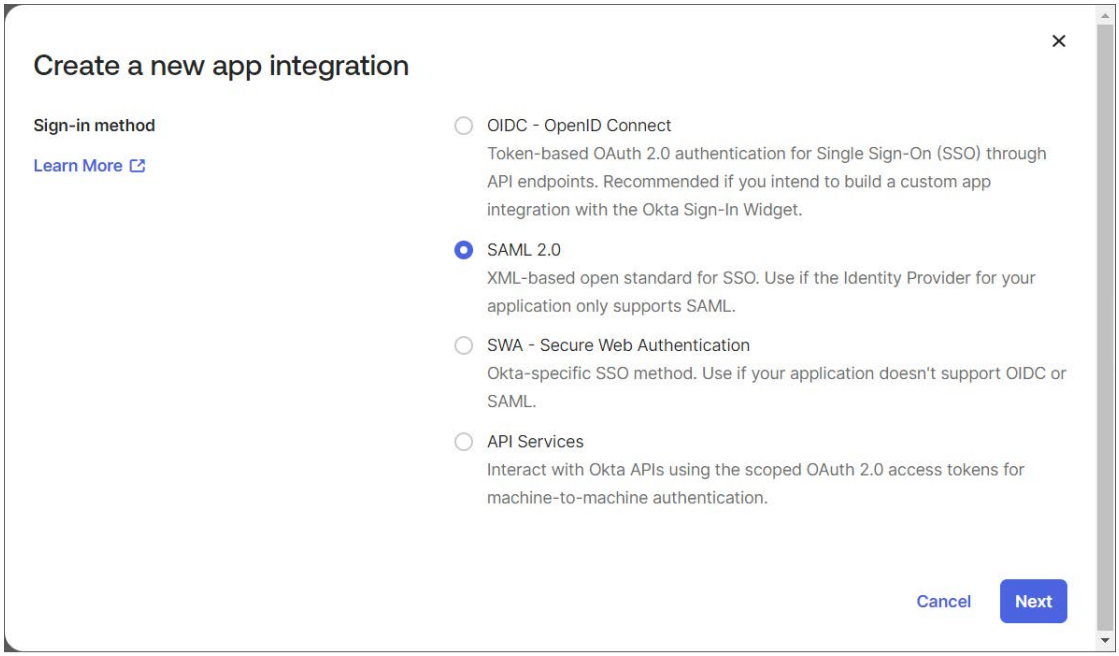
Task ***To set up Okta (SAML 2.0) to use as a single sign-on (SSO) with Software Vulnerability Research:***

1. Sign in to Okta.
2. Navigate to the **Admin** section, choose **Applications**, and select **Applications** to configure the SVR app.
3. Click **Create App Integration** to create a new Okta SSO app.



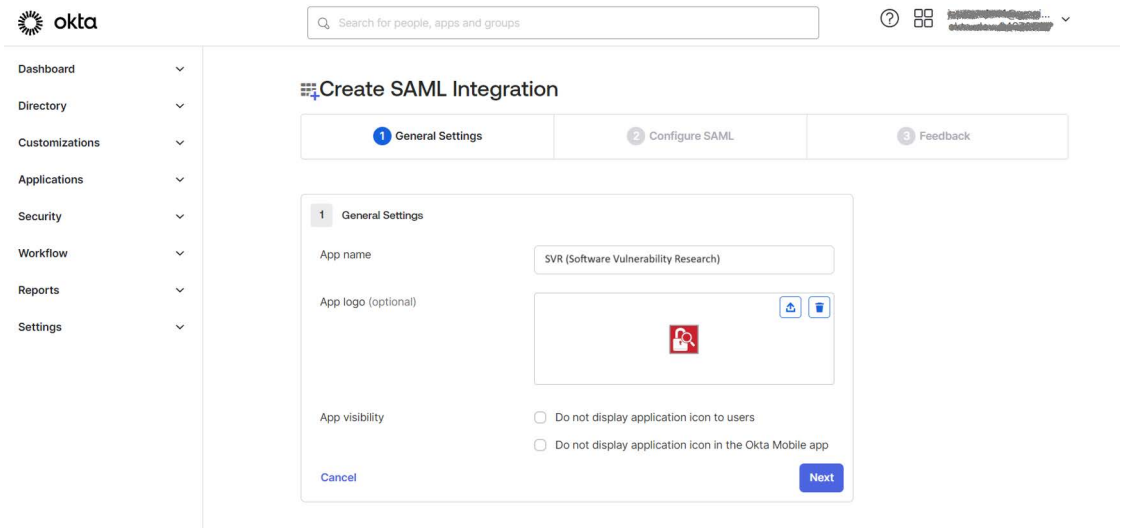
The Create a new app integration wizard opens.

4. Choose **SAML 2.0** for the Sign on method. Then click **Next**.



5. Enter an **App name** (Example: SVR). In the **App Logo** field, click the upload icon, navigate to the location of the logo file, and select the logo (Example: Software Vulnerability Research logo).

   Click **Next** button.



6. Copy the following from the Software Vulnerability Research **Settings > User Management > Single Sign On** fields and paste in the **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 (in Attribute Statements (Optional))

***Note** • The accountkey value is typically provided by your Software Vulnerability Research (SVR) system. You will need to log into your SVR to retrieve it.*

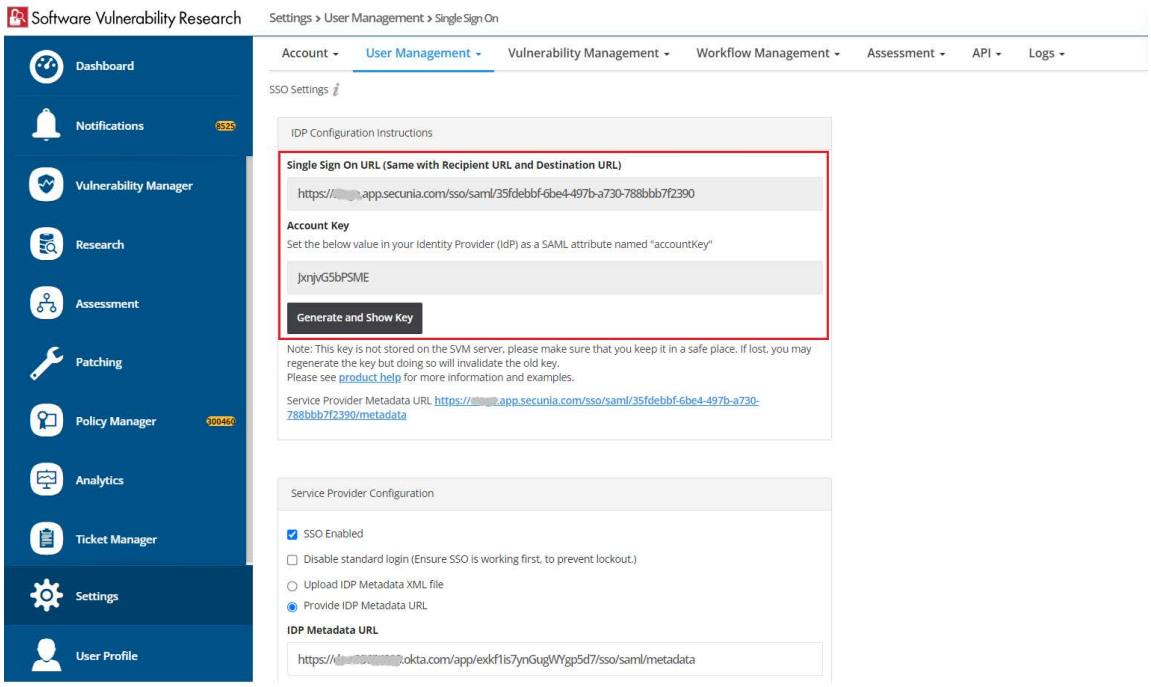
Complete the remaining Okta SAML Settings > Attribute Statements (Optional) name and value fields using the field's drop-down list:

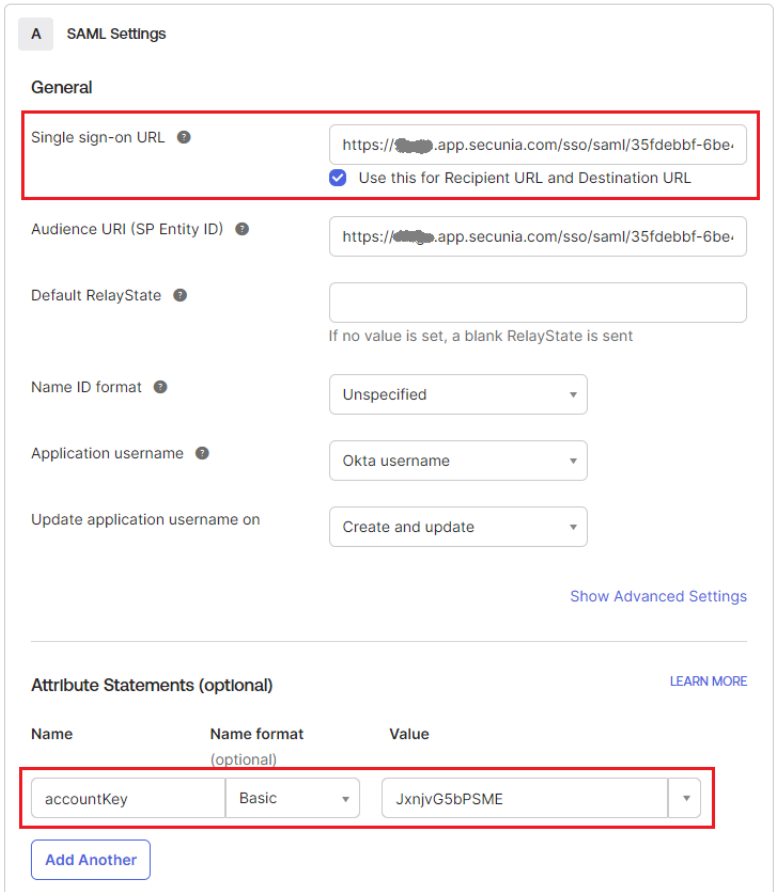
Name	Name format	Values
accountkey	Basic	accountkey ***Note** • The value obtained from SVR.*
firstName	Unspecified	user.firstName
lastName	Unspecified	user.lastName
email	Unspecified	user.email
username	Unspecified	user.login

When configuring attribute statements, you might also need to specify the Name Format. Here are the common formats:

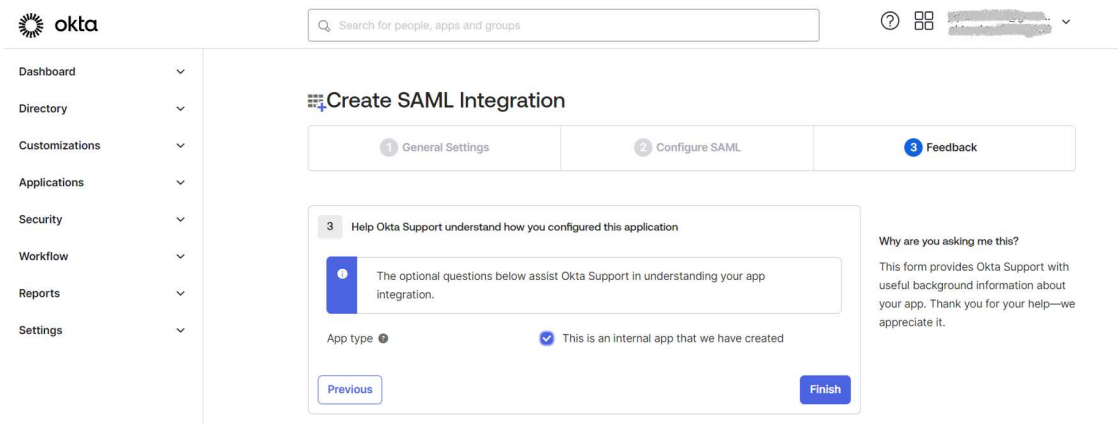
- **Basic—**This is a simple name format used for custom attributes. It doesn't follow any specific URI format.
- **Unspecified—**This format doesn't enforce any particular structure.
- **URI Reference—**This uses a URI to define the attribute name, typically in the form of a URL.

For most custom attributes like accountkey, you can use Basic or Unspecified unless the application specifically requires a URI format.

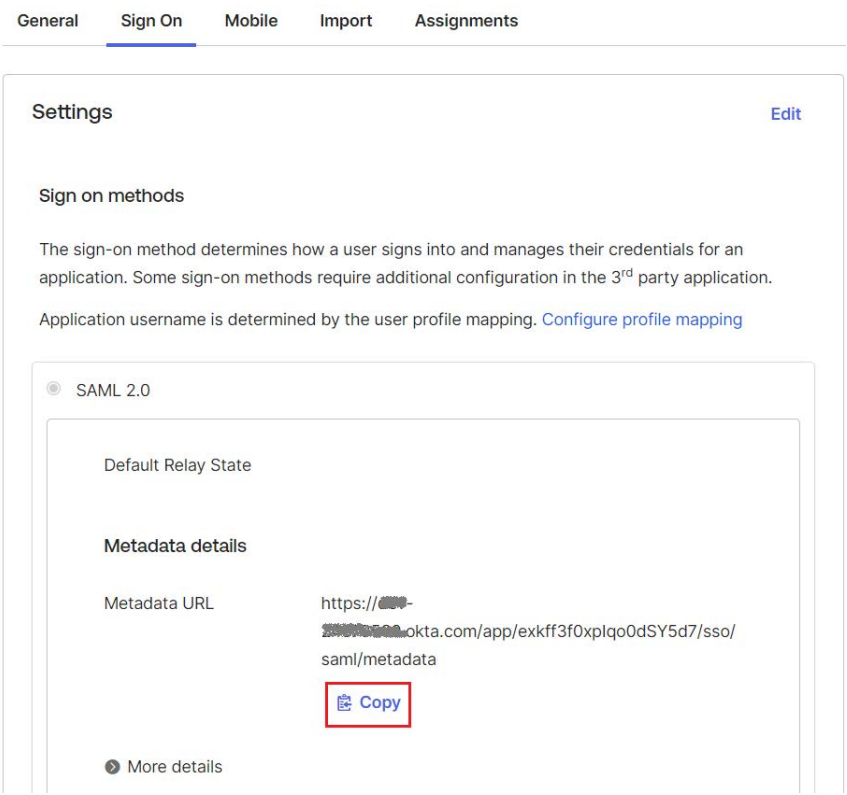




7. In the Create SAML Integration - Step 3 Feedback screen, click **Finish**.

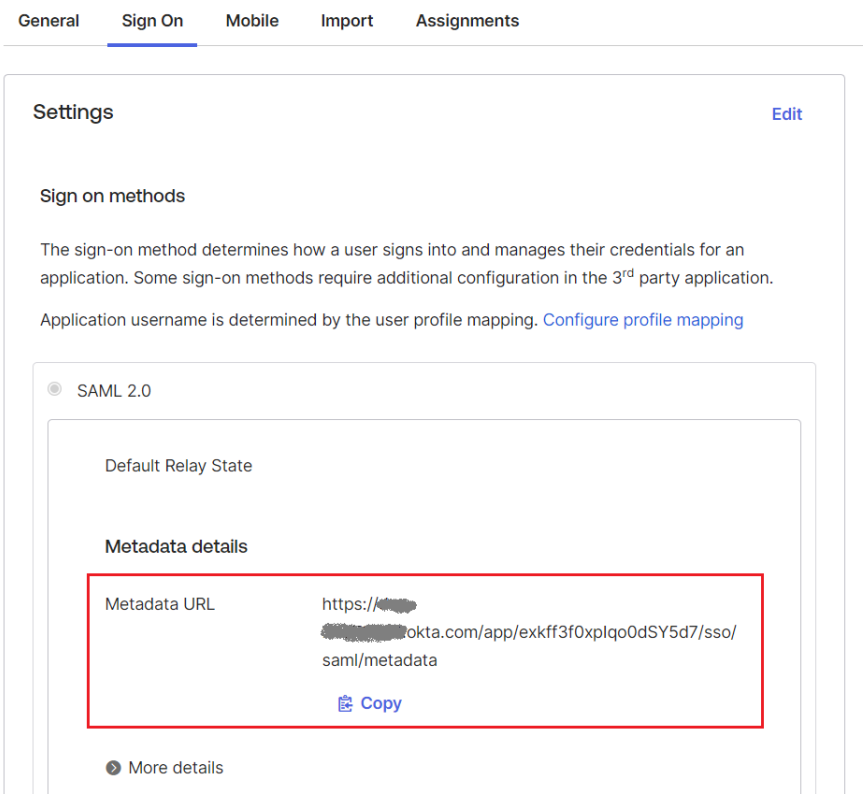


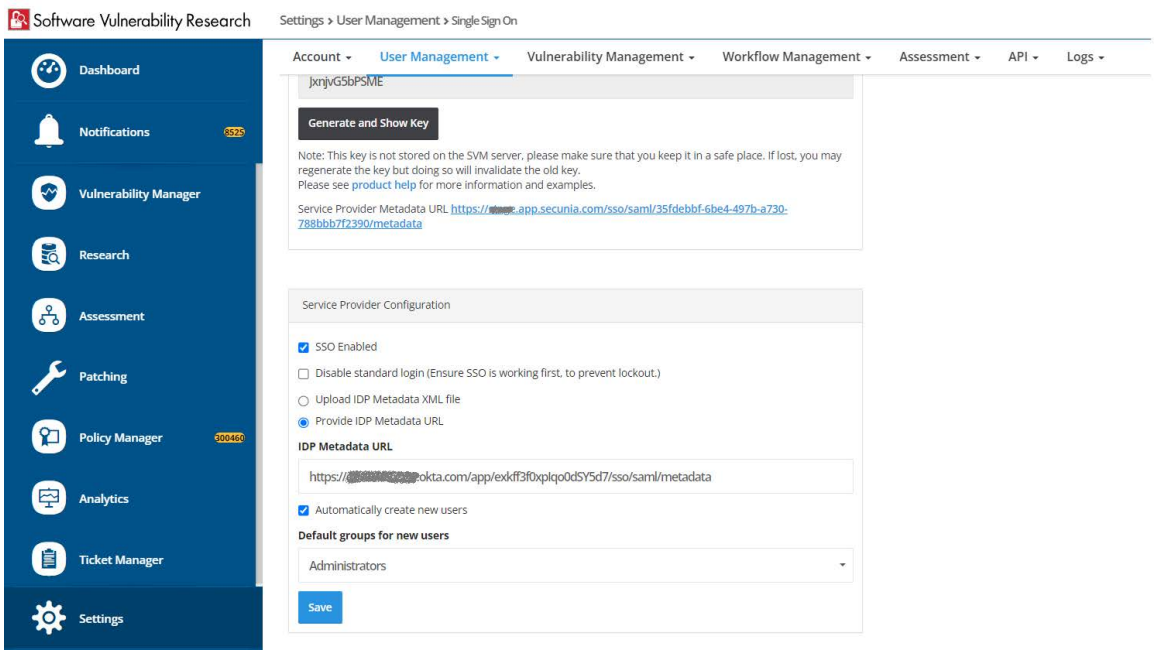
8. At the Okta Sign On Settings screen, click on **Copy** link to copy the metadata URL.



9. Copy the **Identity Provider metadata** URL from Okta into the Software Vulnerability Research **Settings > User Management > Single Sign On > IDP Configuration Instructions** section. In the Service Provider Configuration section, check **SSO Enabled**, check **Automatically create new users**, and assign a **Default group for new users** by selecting from the drop down.

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

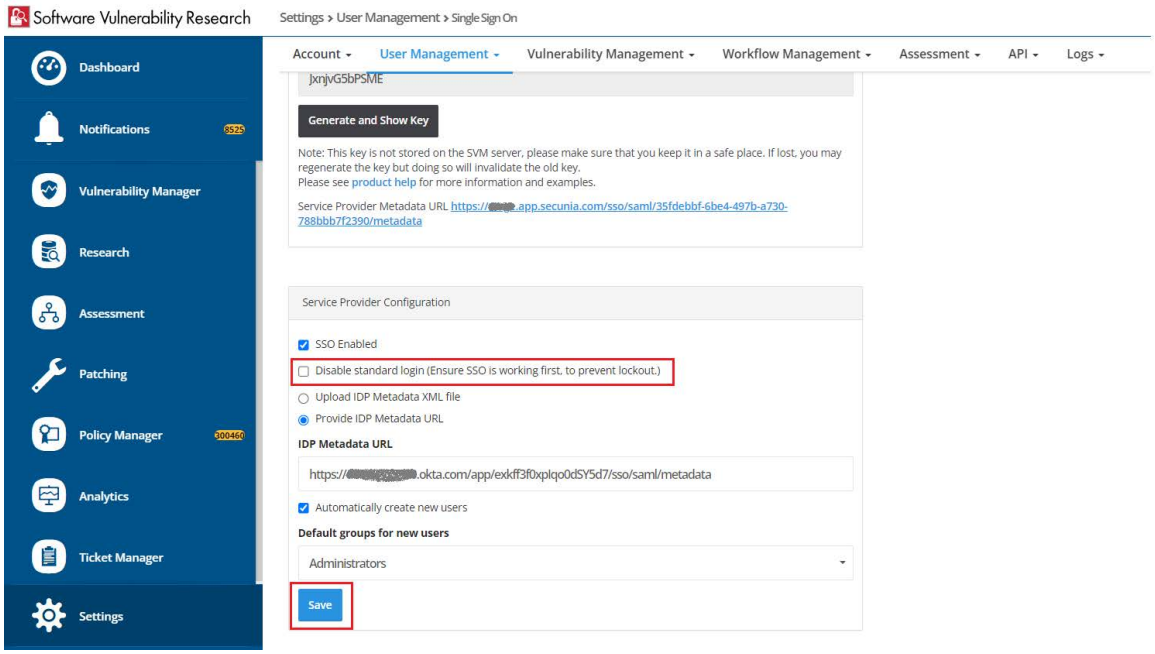




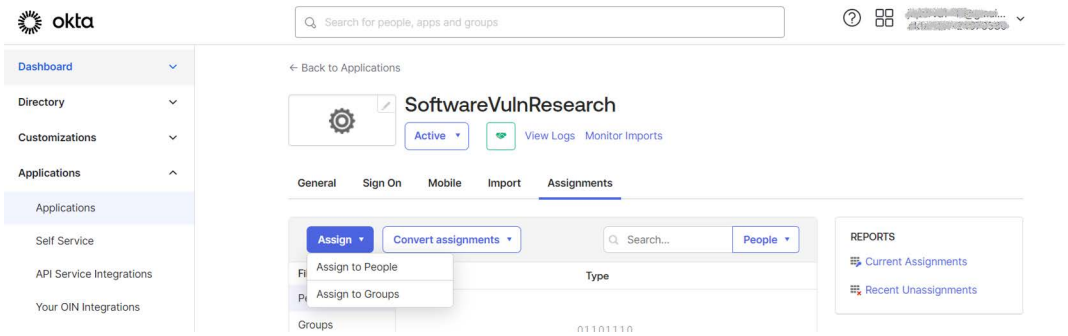
10. If you want to disable standard login options for all of your users (except root), select the **Disable standard login (Ensure SSO is working first, to prevent lockout.)** option under **Settings > User Management > SSO Settings > Service Provider Configuration**.

    Click **Save** to on the **Settings > User Management** page.

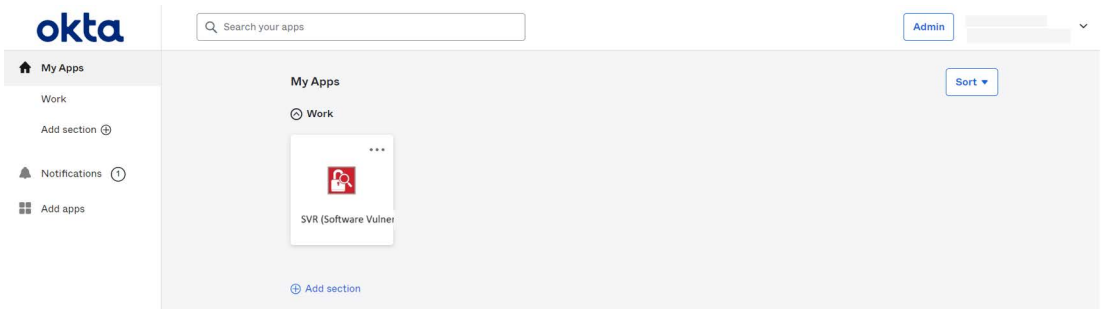
Important • *Before selecting this option, make sure that SSO is working correctly, to prevent user lockout.*



11. Add Software Vulnerability Research users to the Okta SSO account.
12. Assign Software Vulnerability Research users to the Okta SSO app. A reset password link is sent to each user.



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



14. 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:

https://community.flexera.com/t5/Using-the-Case-Portal/tkb-p/case-portal-help

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

Requirement	Description
Monitor resolution	The minimum resolution required is 1280 x 1024.
Browser	The following browsers are supported: • Microsoft Edge • Apple Safari • Google Chrome • Microsoft Edge • Mozilla Firefox • Opera
Internet connection	Internet connection capable of connecting to https://app.flexerasoftware.com/ is required.

Table 3-1 • System Requirements

Requirement	Description

Allow Listed sites	The following addresses should be Allow-listed in the Firewall/Proxy configuration:
	• New CRL distribution URLs:
	  • https://*.app.flexerasoftware.com
	  • http://*.amazontrust.com
	Software Vulnerability Research uses Amazon Certificate Authority for TLS security certificates. Amazon can change their certificate revocation list - crl - occasionally.
	Amazon root certificates are trusted by default by most common browsers, including Google Chrome, Microsoft Internet Explorer and Microsoft Edge, Mozilla Firefox, and Apple Safari.
	For the latest certificate revocation lists and firewall rules, refer to Amazon ACM documentation.
	• If you require explicit URLs then allow below URLs:
	  • http://crt.r2m02.amazontrust.com/r2m02.cer
	  • http://crl.r2m02.amazontrust.com/r2m02.crl
	  • http://ocsp.r2m02.amazontrust.com

First-party cookie settings	First-party cookie settings should be set to at least **Prompt** (in Internet Explorer).
Session cookie settings	The option to allow session cookies should be selected.
PDF reader	A PDF reader is required.

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.*

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
- Default Workflow Rules
- Custom Workflow Rules

Create a Workflow Rule - Overview

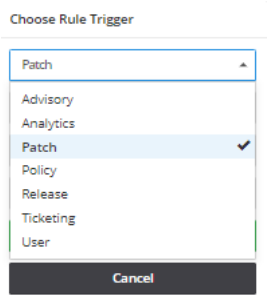
To create a workflow rule, perform the following steps.

Task ***To create a Workflow Rule:***

1. Click to create a new Workflow Rule.
2. Enter the **Rule** name and click **Choose Rule Trigger**. For details, see Rule Triggers.
3. 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.
4. 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.
5. 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.
6. Click **Edit** to change and to **Enable** or **Disable** a rule.

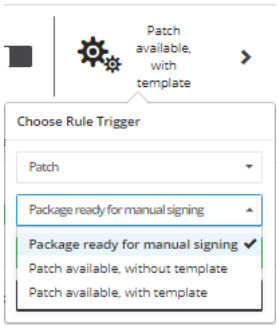
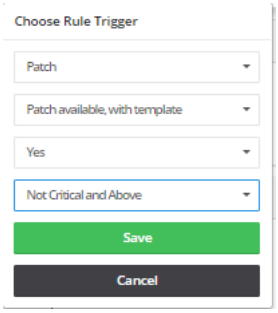
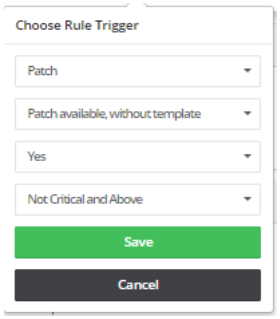
Rule Triggers

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:

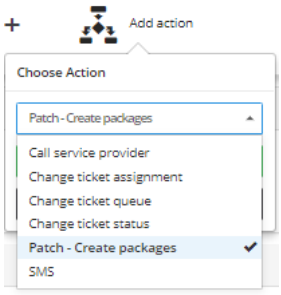
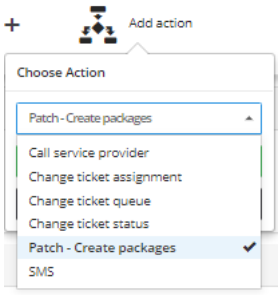
Table 3-2 • Patch Rule Trigger Options

Option 1: Patch ready for manual signing	Option 2: Patch available with template, affecting my environment = Yes, Not Critical or Above	Option 3: Patch available without template, affecting my environment = Yes, Not Critical or Above
		

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.

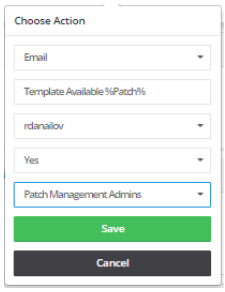
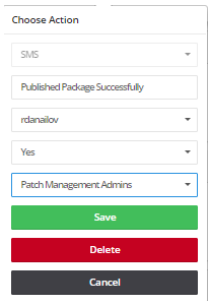
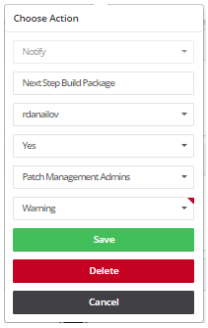
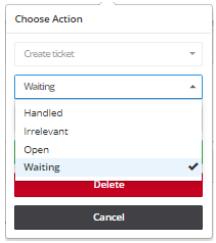
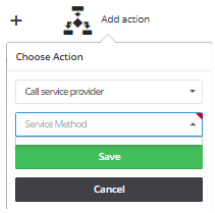
Table 3-3 • Patch Rule Action Options

Patch - Create Packages	Patch - Publish to deployment servers
	

Notification Actions

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

Table 3-4 • Notification Actions

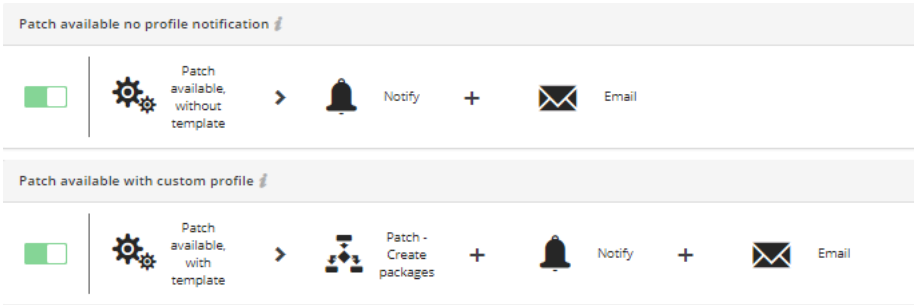
Email the user with custom message and broadcast the email to members of a particular group	SMS the user with custom message and broadcast the text to members of a particular group	Notify the user with custom message and broadcast the email to members of a particular group	Create ticket with status Waiting for handling	Call Service Provider
				 ***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.



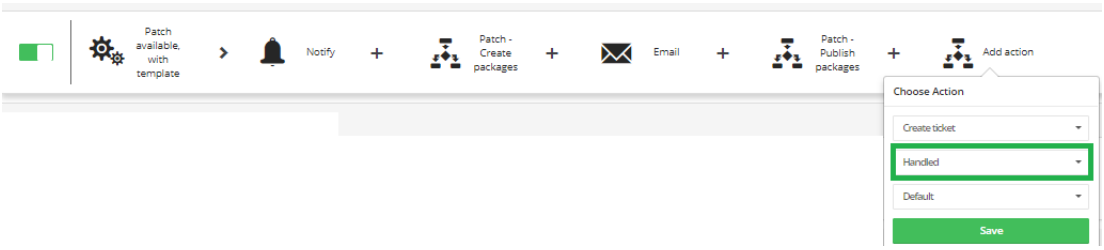
The default workflow rules should be used as a template. It's good practice to disable the default workflow rules to make custom workflow rules with the same settings. Custom rules cancel out default rules, which might cause unforeseen issues. For additional information, see Default Workflow Rule Examples.

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****.*

Additional Patching Information

For additional Patching information, see:

- Patching Tickets
- Manual Signatures

4

Dashboard

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.

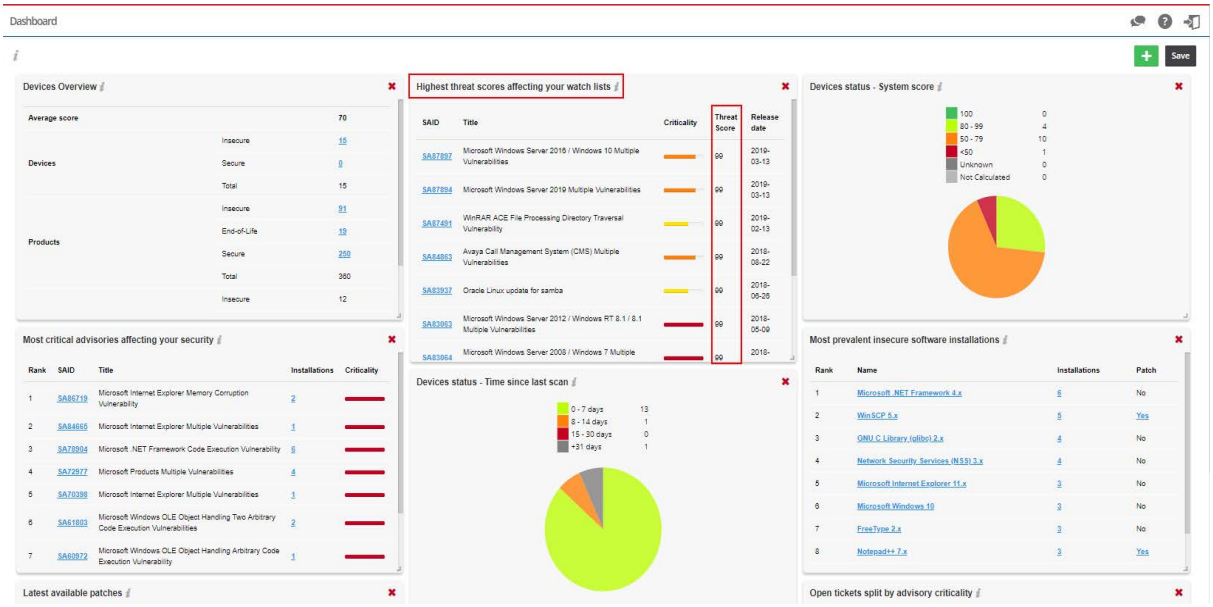
- Dashboard with Threat Intelligence Module
- Dashboard without Threat Intelligence Module

Dashboard with Threat Intelligence Module

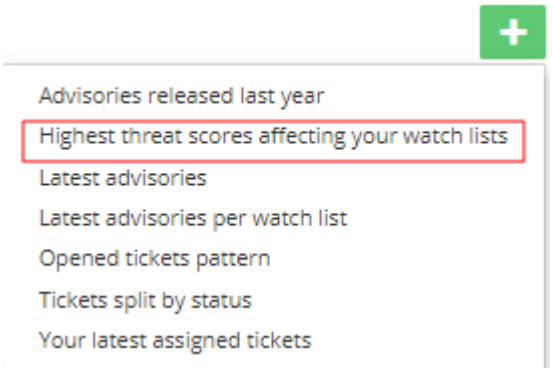
The below figure shows the Dashboard with the Threat Intelligence Module, the additional widget **Highest threat scores affecting your watch lists** get included in the main page.

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*



Click + to add the **Highest threat scores affecting your watch lists** widget and Save to save the changes you made.



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

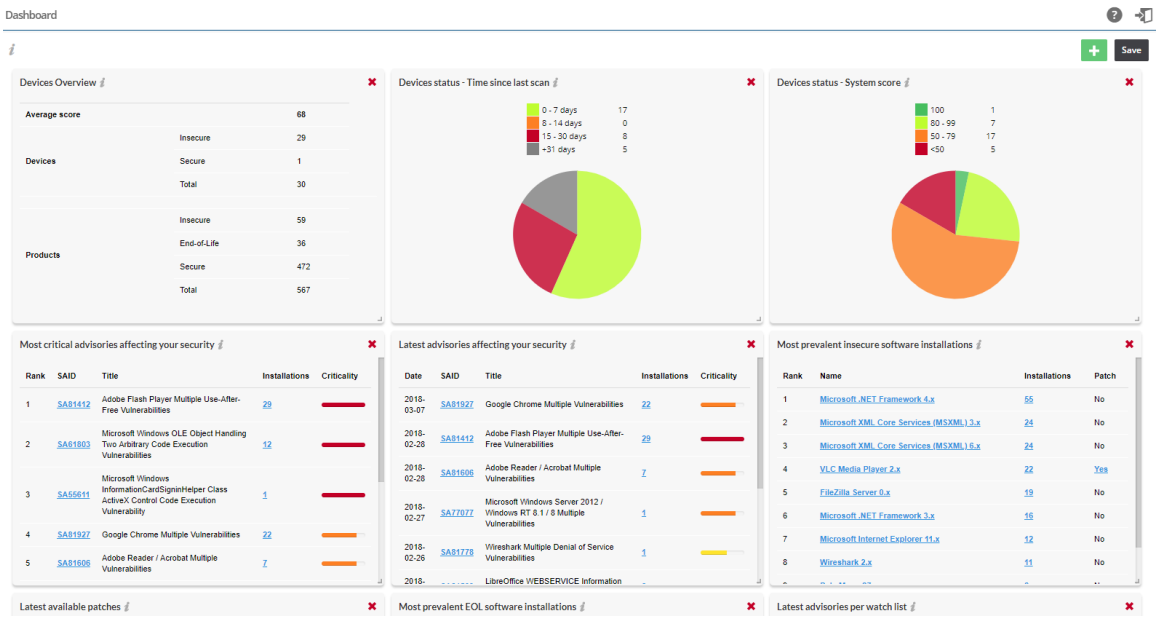
Dashboard Widget

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

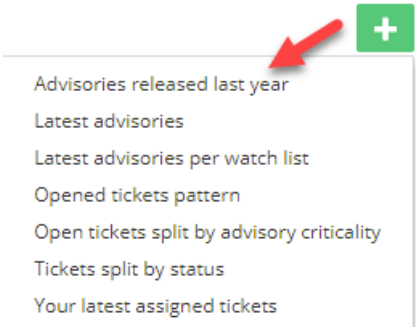
- **Highest threat scores affecting your watch lists** - displays those advisories with the highest threat scores affecting the watch lists.

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 i 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

Item	Description
Devices Overview	Displays an overview of the average security score (current verses last week) for the Devices, Products and Operating Systems within your environment.
Devices status - Time since last scan	Displays the number of devices that have been scanned within a given time frame.
Devices status - System Score	Displays how your devices rank based on the computed system score.

Table 4-1 • Dashboard Widgets

Item	Description
Most critical advisories affecting your security	Displays the most critical Advisories based on all software detected within your environment.
Latest advisories affecting your security	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.
Latest advisories affecting your security	Displays the most recent Advisories affecting software from your Devices.
Latest advisories per watch list	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.
Advisories released last year	Displays a month-by-month graph of the total number of advisories released by Secunia over the previous 12 months.
Your latest assigned tickets	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.
Open tickets split by advisory criticality	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.
Tickets split by status	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.
Open tickets pattern	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).
Most prevalent EOL software installations	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.
Most prevalent insecure software installations	Displays the most insecure software based on the number of Devices within your environment.

Table 4-1 • Dashboard Widgets

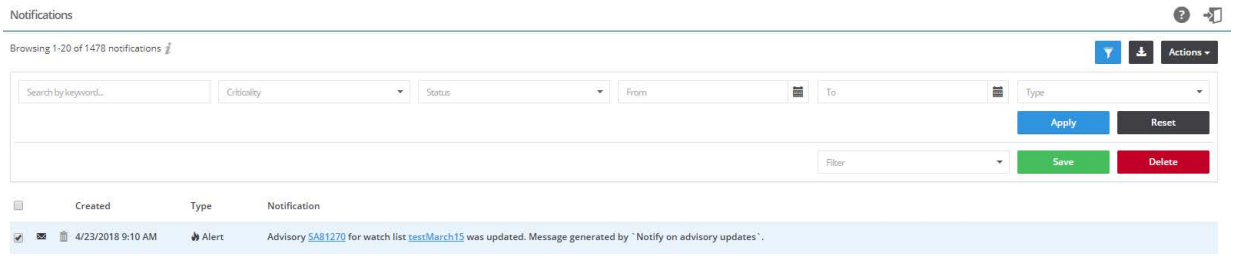
Item	Description
Latest available patches	Displays the latest available patches based on your scan results.

5

Notifications

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.*



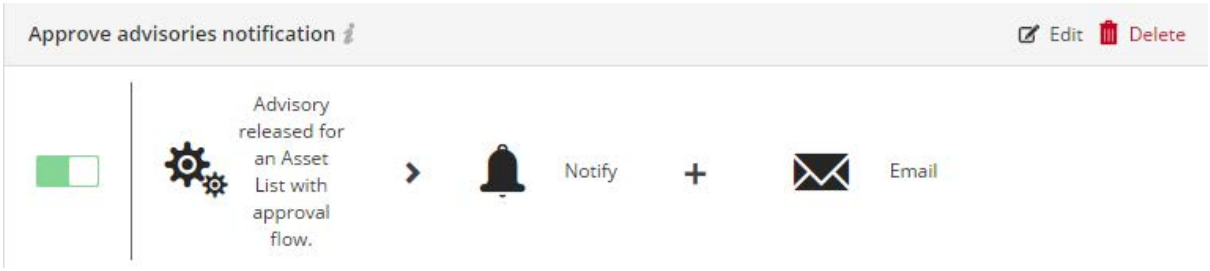
Task ***To view notifications:***

1. Open the **Notifications** page.
2. Click 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.



6

Vulnerability Manager

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.

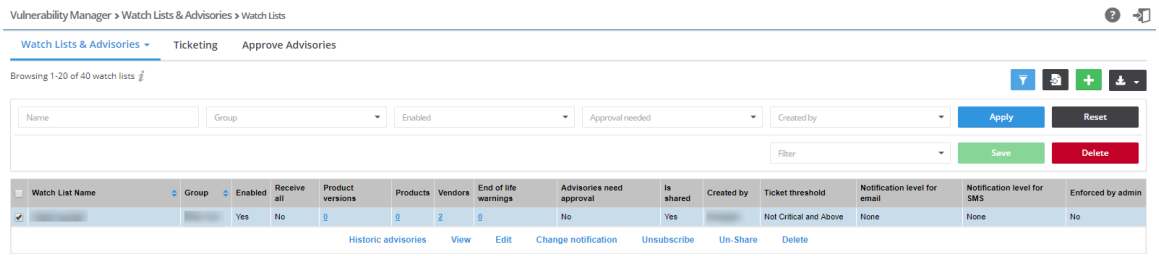
The monitored Vendors (all products from the vendor), Products (all versions) and specific Product Versions are organized into Watch Lists. Each Watch List can have different notification levels, can be grouped into Watch List Groups and can be shared with all Users and User Groups associated with your 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 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 drop-down menu.
4. Click 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**.

   Note • *When selecting Groups or Users, you can either choose directly from the drop down list or enter keywords into the search box. Matching results will be displayed in the grid and select the desired group.*
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:*

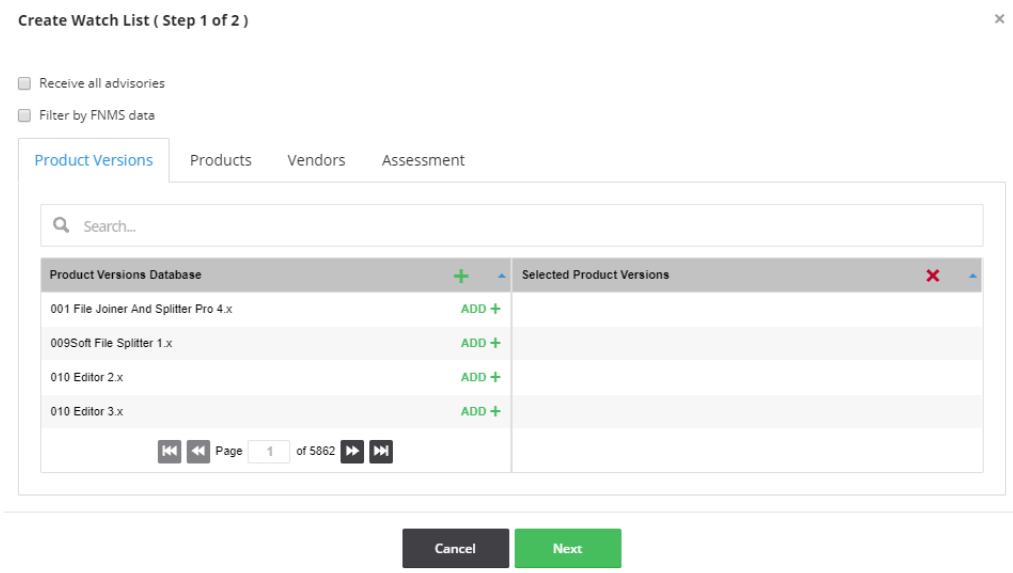
- ***Create new Watch List****—The field Advisories need approval will be checked and cannot be disabled.*
- ***Edit existing Watch List****—The field Advisories need approval cannot be edited (either enabled or disabled).*
- *Shared Watch Lists for the user will have the normal behavior. It is the responsibility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

Create Watch Lists

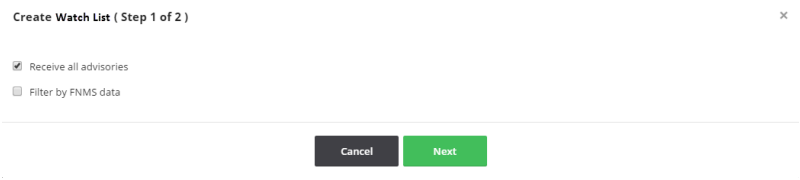
To create a watch list, perform the following steps.

Task ***To create a Watch List***

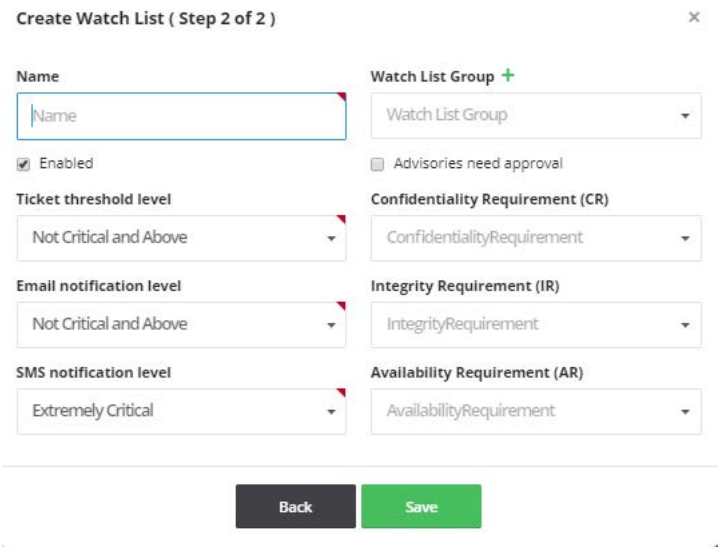
1. Open the **Vulnerability Manager > Watch Lists & Advisories > Watch Lists** page.
2. To create a new Watch List, click . The **Create Watch List (Step 1 of 2)** page opens. On this page, you can select **Product Versions**, **Products**, **Vendors**, or **Assessment**.



Note • *You can select the Receive all advisories check box to receive Secunia Advisories for all Product Versions, Products, and Vendors.*



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.
5. Click × 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.
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.

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)**, I**ntegrity 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.

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

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.

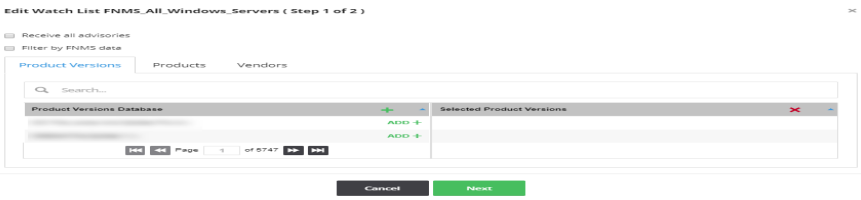
13. Click **Save** to save the Watch List. Once saved, you will begin to receive alerts and advisories based on your configuration.

Edit Watch Lists

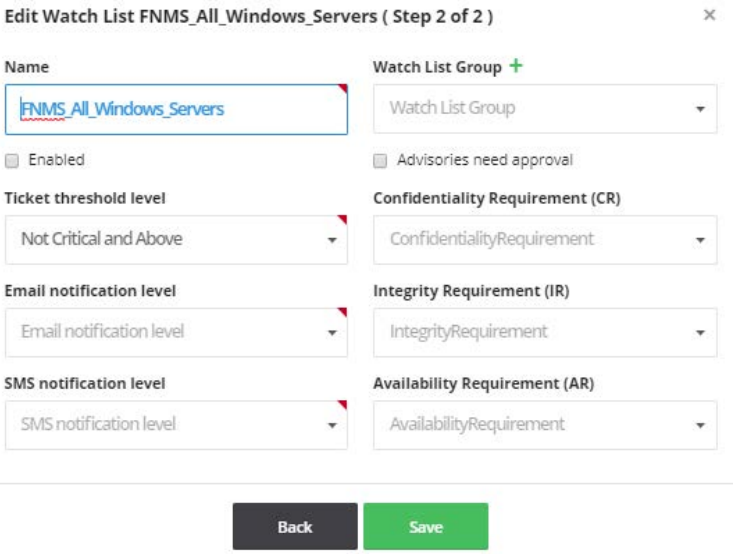
To edit a watch list, perform the following steps.

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.

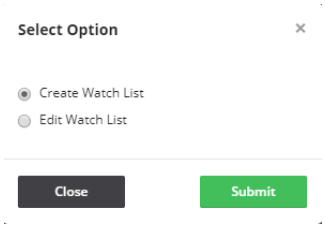
8. You can optionally select the impact that a vulnerability in any item in the Watch List will have to your environment (Low, Medium or High) by **Confidentiality Requirement (CR)**, I**ntegrity Requirement (IR)** and **Availability Requirement (AR)** from the drop-down lists (optional).
9. Click **Save**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

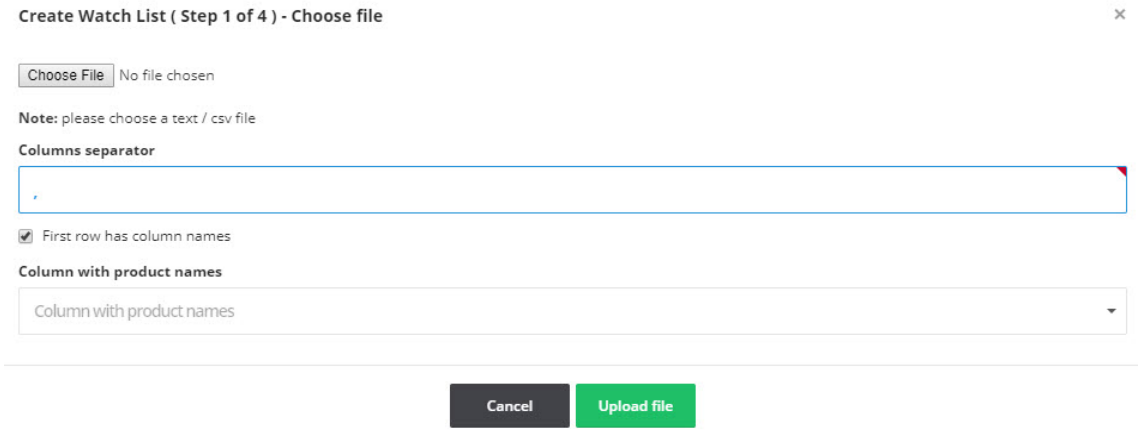
To import a new Watch List, perform the following steps.

Task ***To import a new Watch List:***

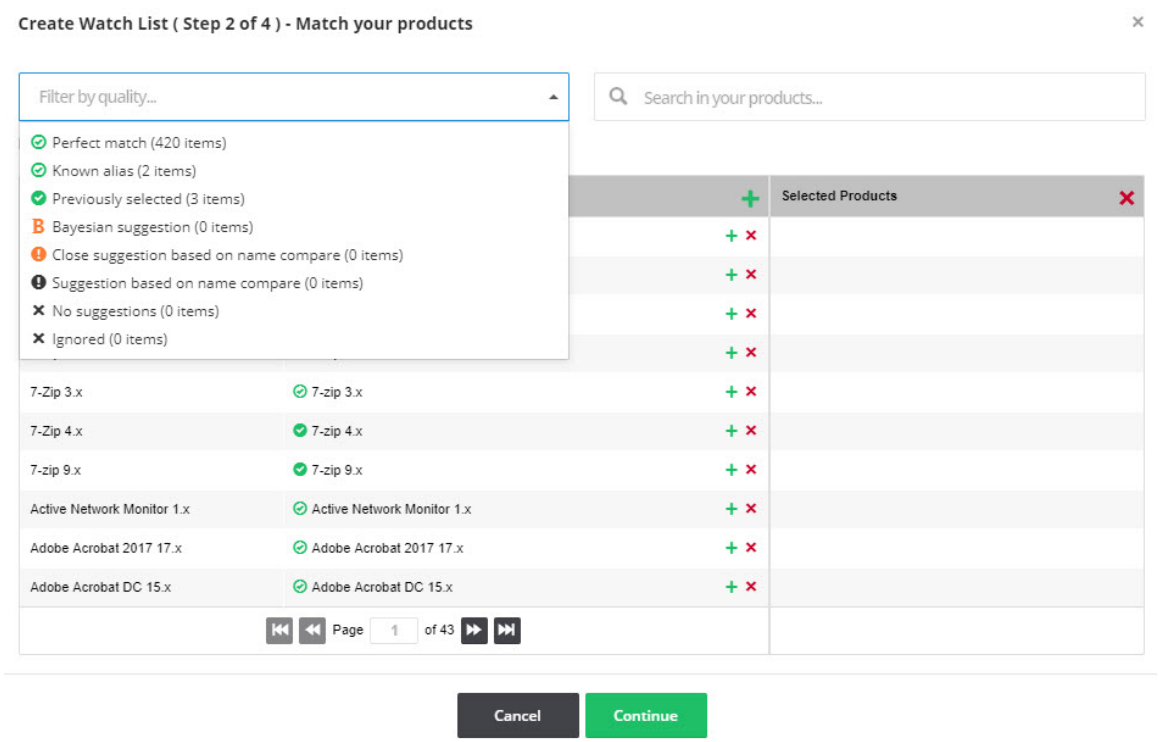
1. Open the **Vulnerability Manager > Watch Lists & Advisories > Watch Lists** page.
2. Click .
3. Choose **Create Watch List** and **Submit**.



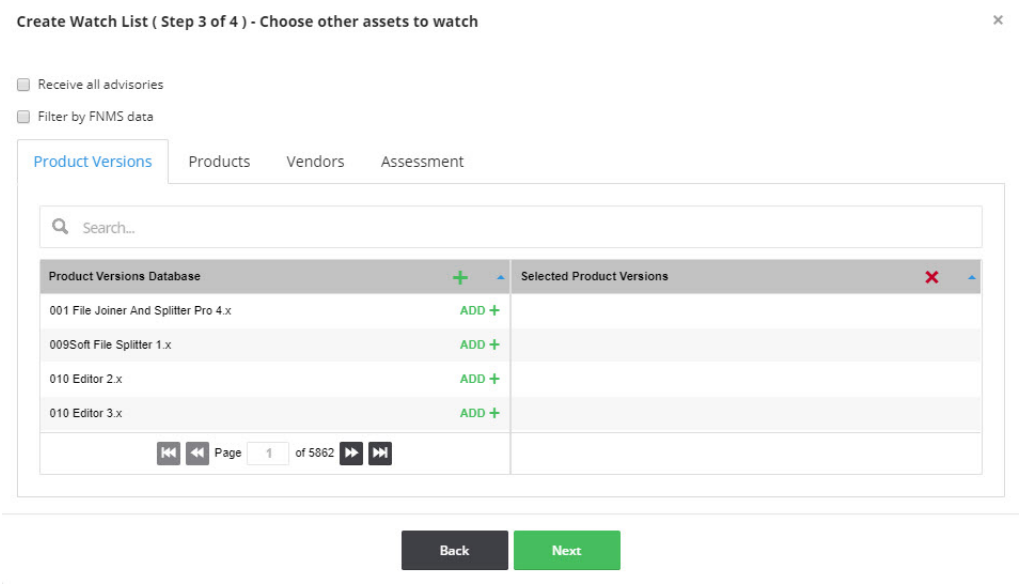
The **Create Watch List (Step 1 of 4)** dialog box opens.



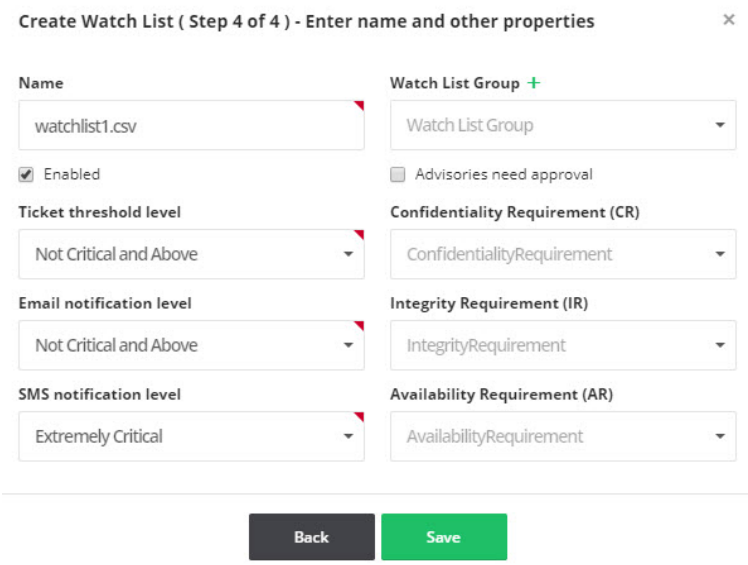
4. Define the **Columns separator** (“,” is the default) for the file you are importing.
5. Select **First row has column names**, if applicable.
6. Click **Upload file**. The **Create Watch List (Step 2 of 4)** dialog box opens.



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 × 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).

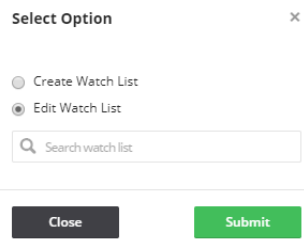
17. Click **Save** to save the Watch List. Once saved, you will begin to receive alerts and advisories based on your configuration.

Import an Updated Watch List

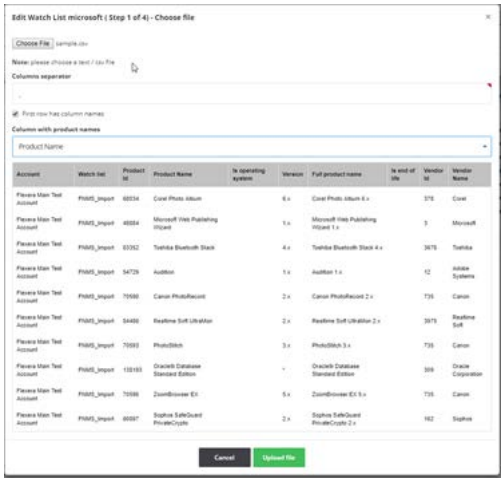
To import an updated Watch List, perform the following steps.

Task ***To import an updated Watch List:***

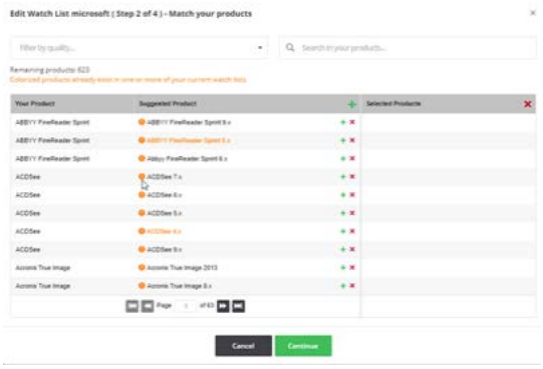
1. Open the **Vulnerability Manager > Watch Lists & Advisories > Watch Lists** page.
2. Click .
3. Choose **Edit Watch List**, enter the Watch List to update in the search field, and click **Submit**.



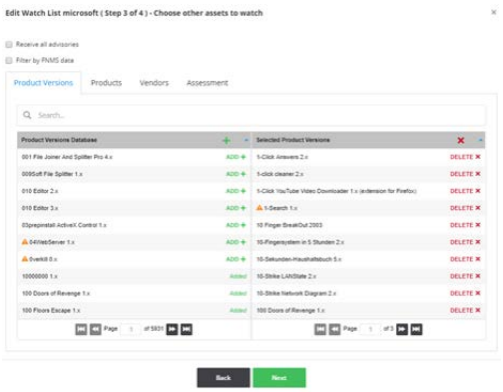
The **Edit Watch List (Step 1 of 4)** dialog box opens.



4. **Choose File** to import and click **Upload file**. The **Edit Watch List (Step 2 of 4)** dialog box opens.



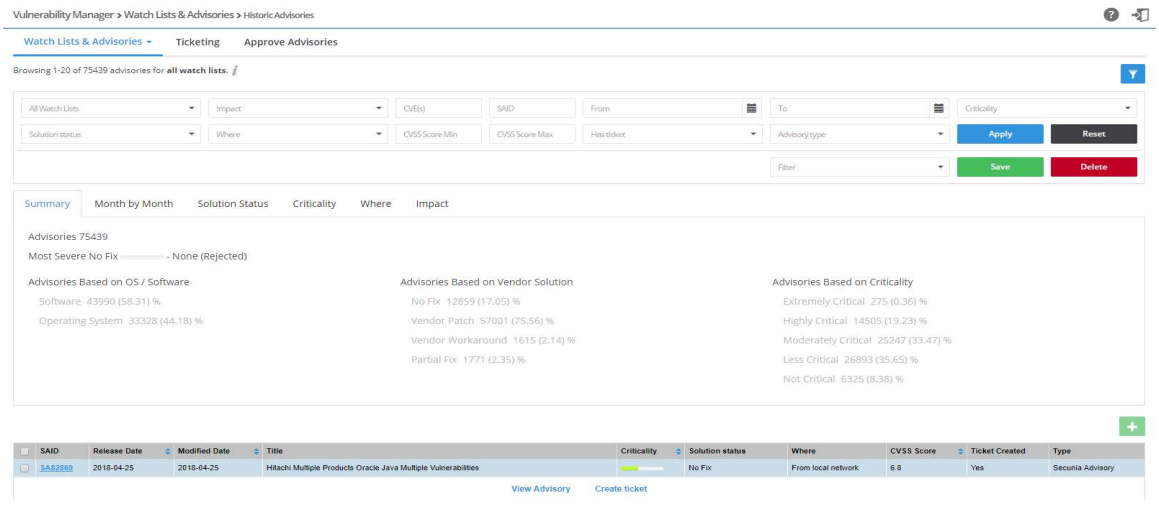
5. Make the necessary edits and click **Continue**. The **Edit Watch List (Step 3 of 4)** dialog box opens.



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:***

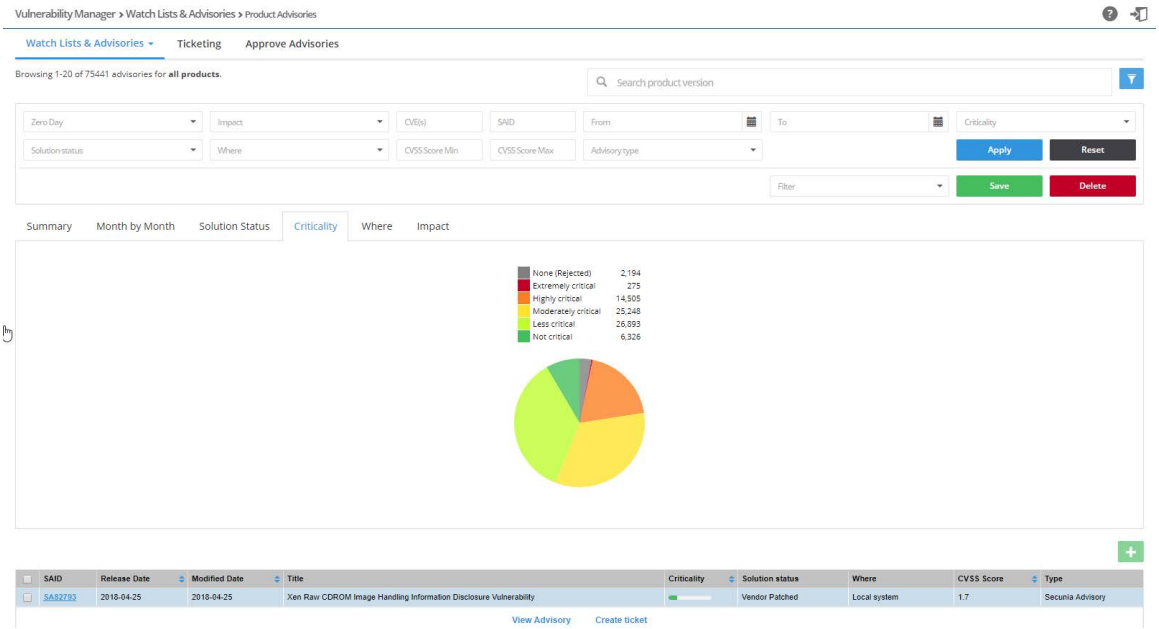
1. Open the **Vulnerability Manager > Watch Lists & Advisories > Historic Advisories** page.
2. Click to filter the advisories by **All Watch Lists**, **Impact**, **CVE(s)**, **SAID**, **From** and **To** dates, **Criticality**, **Solution status**, **Where**, **CVSS Score Minimum and Maximum values**, **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**.

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.*

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.



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**.

Note • *When selecting Groups or Users, you can either choose directly from the drop down list or enter keywords into the search box. Matching results will be displayed in the grid and select the desired group.*

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.*

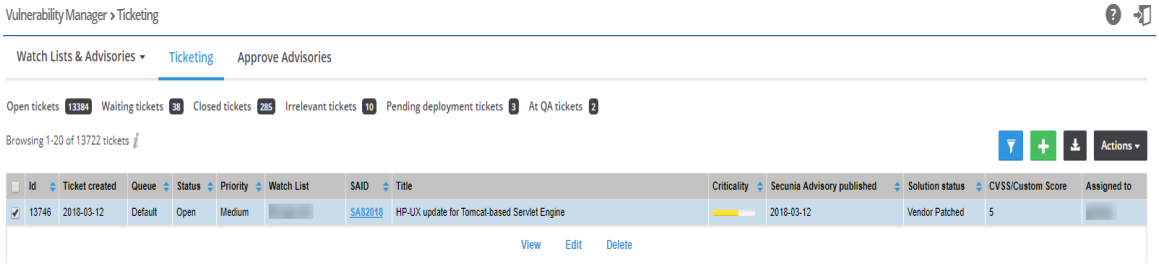
***Important** • The minimum version of FlexNet Manager Suite supported by the Software Vulnerability Research import tool is 2015 R2 SP2.*

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***

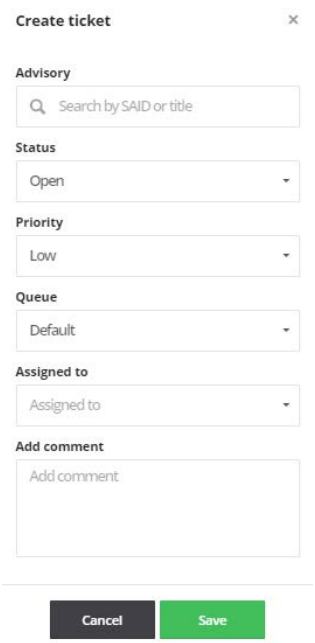
1. Open the **Vulnerability Manager > Ticketing** page.
2. To filter the results by ticket status, select one of the bold ticket statuses in the upper-left-hand corner followed by a ticket count. The default ticket statuses are **Open**, **Waiting**, **Handled**, and **Irrelevant**. See Default Ticket 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.



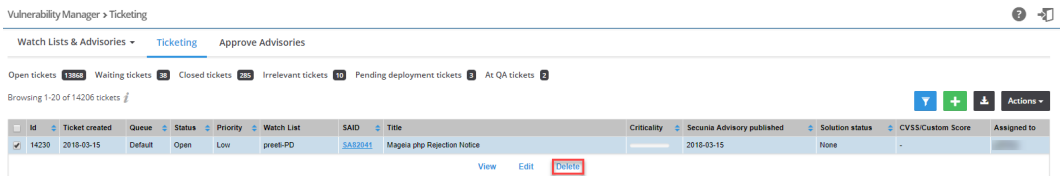
3. From the **Status** drop-down list, select the appropriate status. The default ticket statuses are **Open**, **Handled**, **Closed**, or **Irrelevant**. See Default Ticket Statuses in Vulnerability Manager for more information.
4. From the **Priority** drop-down list, select the appropriate priority.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

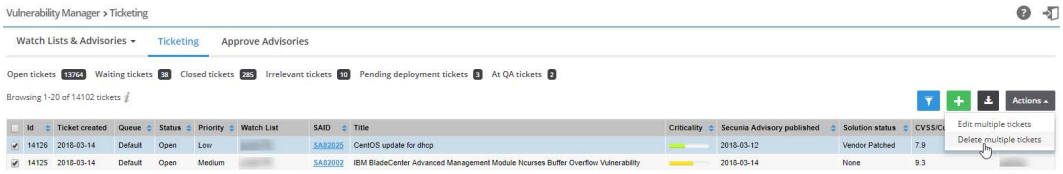
To delete tickets in Vulnerability Manager, perform the following steps.

Task ***To delete tickets in Vulnerability Manager:***

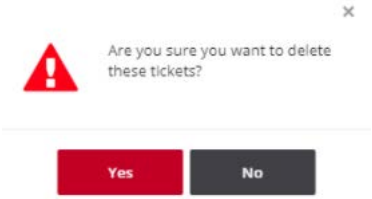
1. Open the **Vulnerability Manager > Ticketing** page.
2. Insert a check mark in front of the ticket or tickets to delete.
3. To delete one ticket, select **Delete** under the listed ticket in the grid.



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 6-1 • Default Ticket Statuses

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

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

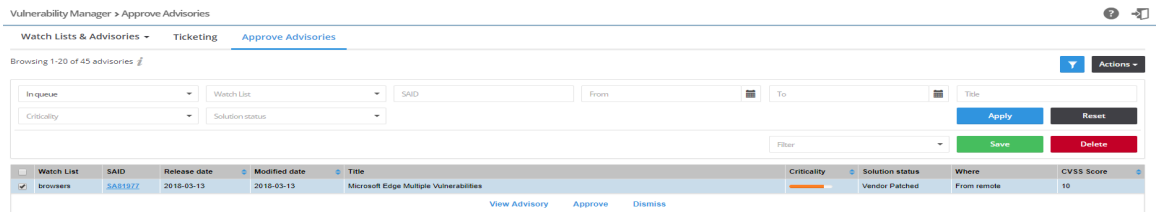
Approve Advisories

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.

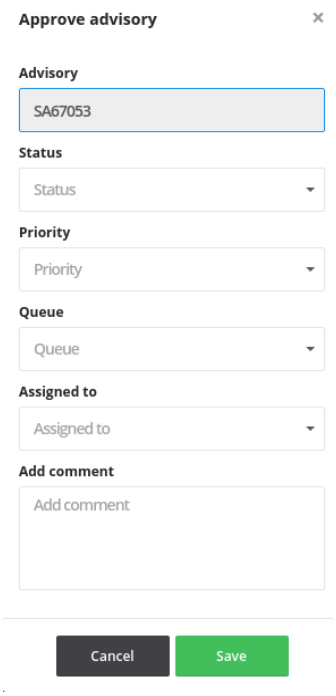


2. Click to filter the Advisories by **In queue**, **Watch List**, **SAID**, **From** and **To** dates, **Title**, **Criticality**, and **Solution status**.

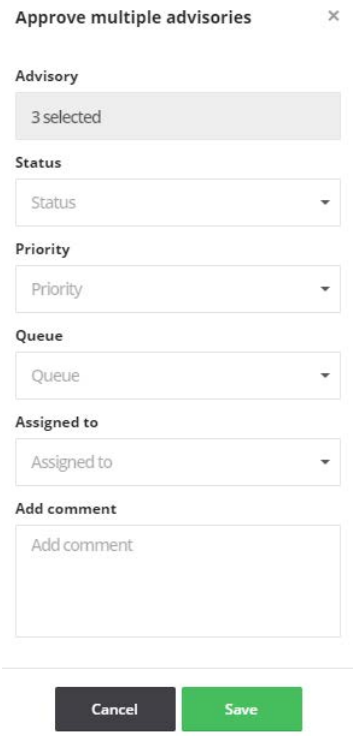
3. Click the **Apply** or **Reset** buttons to apply or reset the filters.

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****.*

7

Research

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

The Research menu consists of the following tabs:

- Advisory Database
- Products Database
- Vulnerability Database

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.

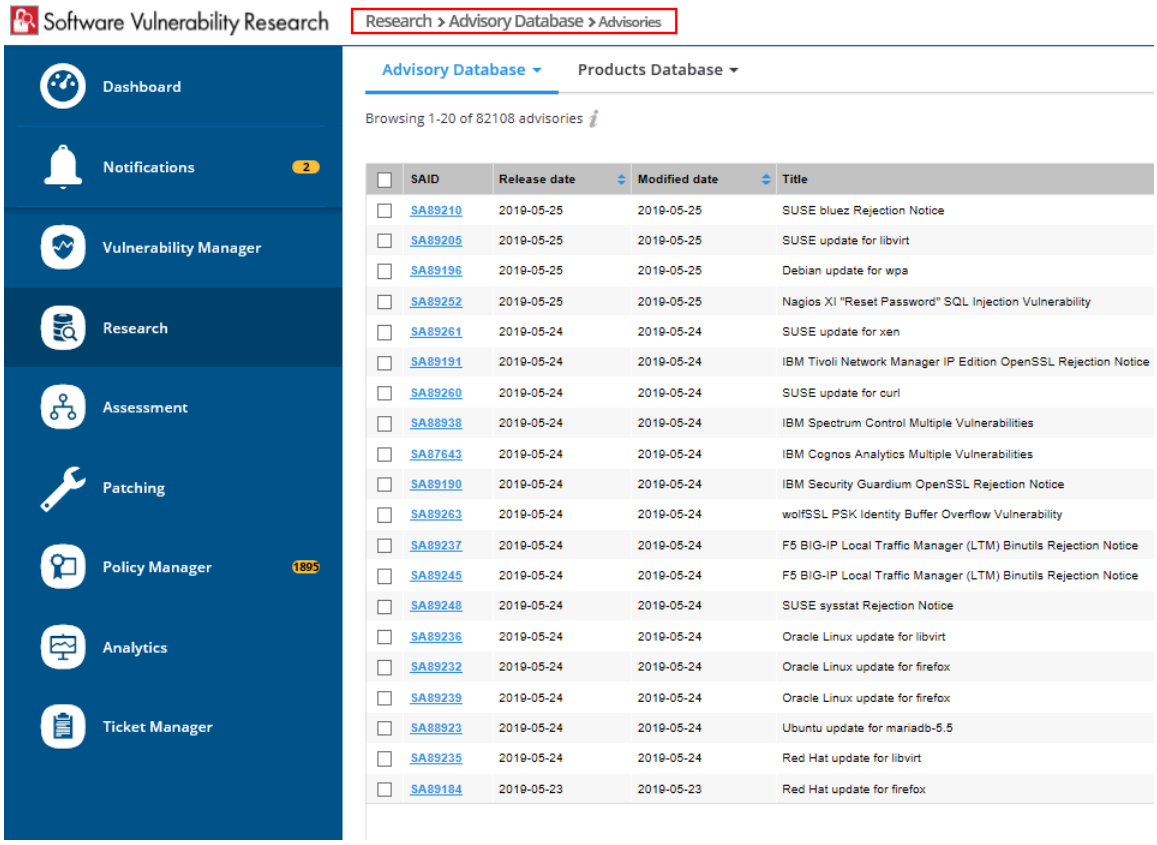
Advisories

The **Advisories** page displays details of all the advisories released.

The **Advisories** page can be,

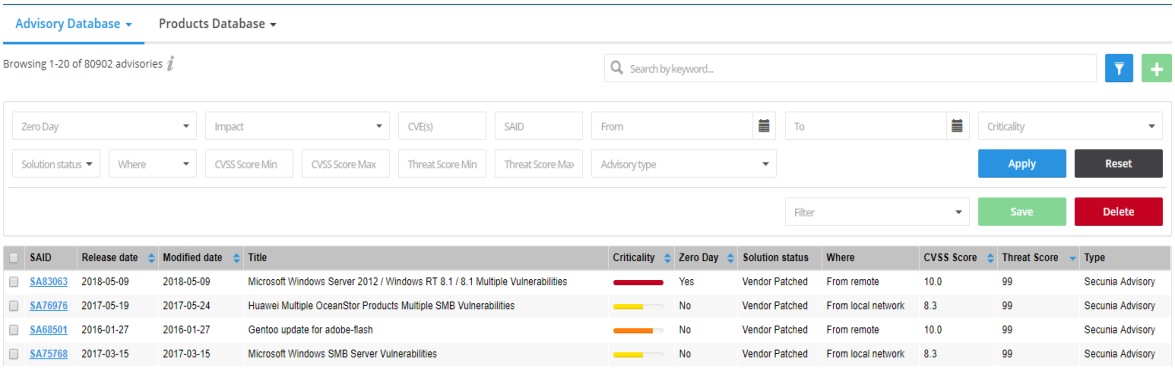
- Advisories with Threat Score
- Advisories without Threat Score

To open the **Advisories** page, **Research >> Advisory Database >> Advisories**



Advisories with Threat Score

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

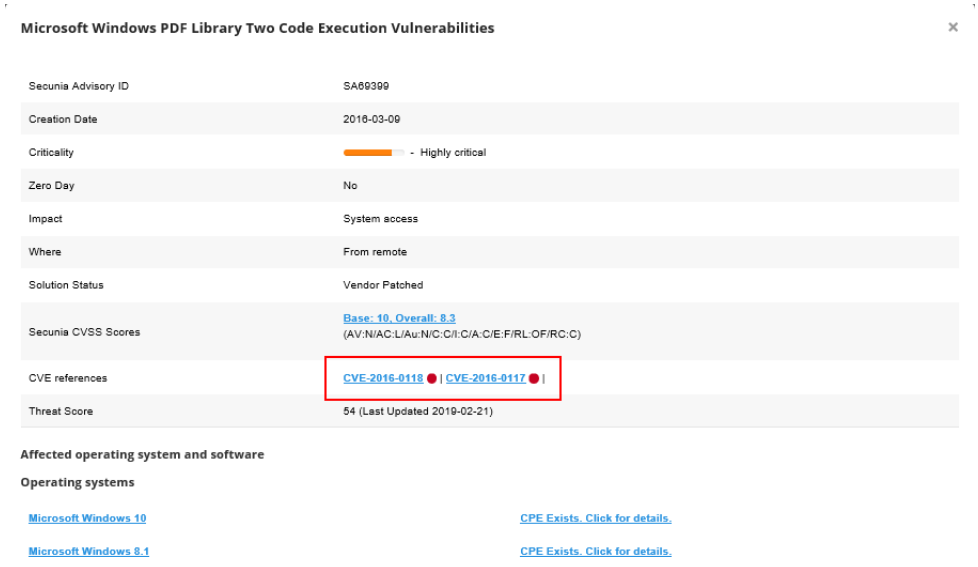


Note • *Please note the following:*

- *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*

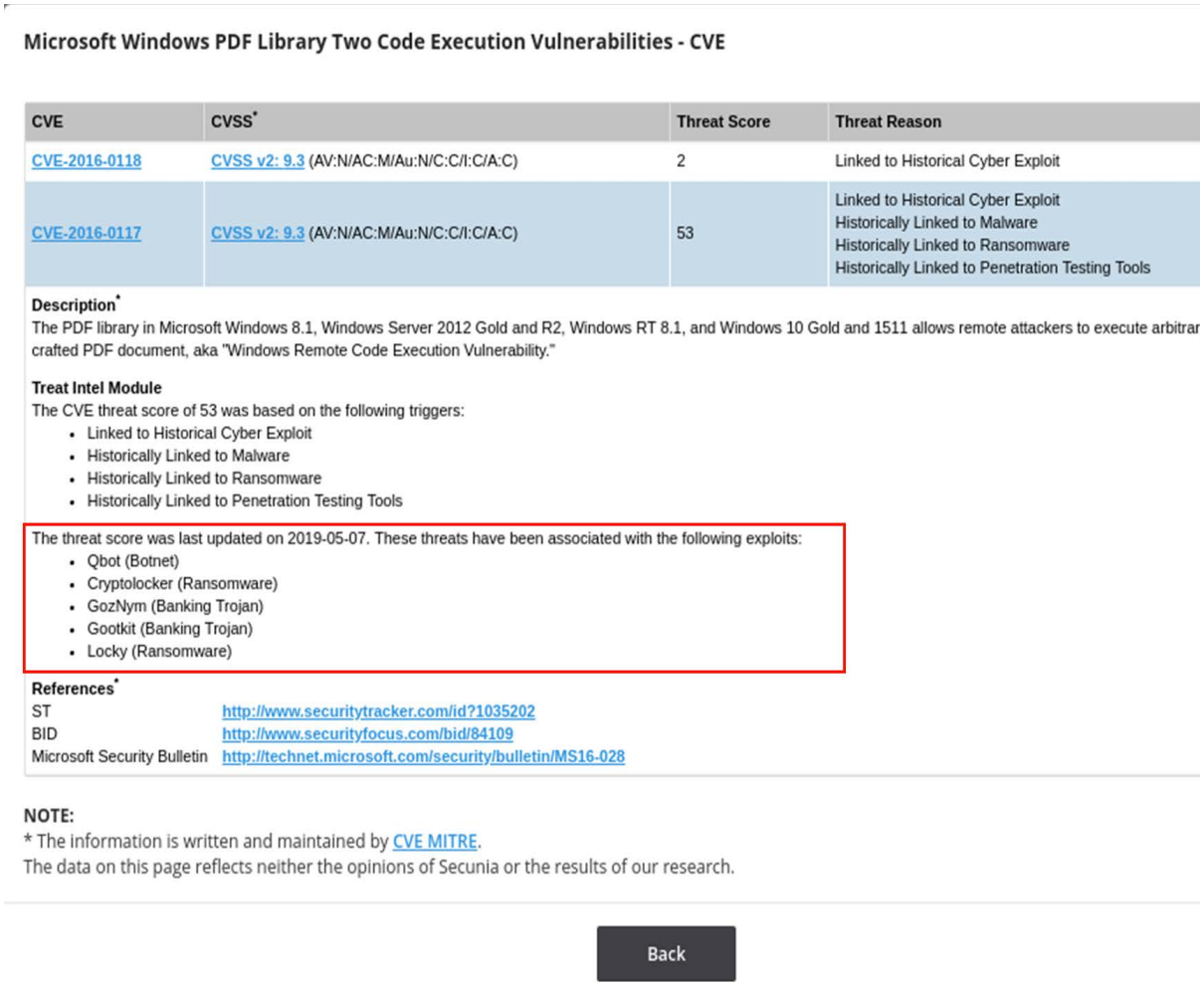
In additional to the features explained in the **Advisories Page >** Advisories without Threat Score, the following features are added:

- **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:



Note • *Effective December 15, 2023, NVD will retire the CPE v2.2 legacy feed. Consequently, current products in SVR will be visible in both CPE v2.2 and CPE v2.3 naming formats during this transitional period. However, it's important to note that any new products added to SVR in the future will be displayed in the CPE v2.3 naming format, and the CPE v2.2 format only if available.*

- **To see the threat Score, threat Reason and their associated exploits**, click on the **CVE references**, as shown below:



Microsoft Windows PDF Library Two Code Execution Vulnerabilities - CVE

CVE	CVSS*	Threat Score	Threat Reason
CVE-2016-0118	CVSS v2: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	2	Linked to Historical Cyber Exploit
CVE-2016-0117	CVSS v2: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	53	Linked to Historical Cyber Exploit Historically Linked to Malware Historically Linked to Ransomware Historically Linked to Penetration Testing Tools

Description*
The PDF library in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrar
crafted PDF document, aka "Windows Remote Code Execution Vulnerability."

Treat Intel Module
The CVE threat score of 53 was based on the following triggers:

- Linked to Historical Cyber Exploit
- Historically Linked to Malware
- Historically Linked to Ransomware
- Historically Linked to Penetration Testing Tools

The threat score was last updated on 2019-05-07. These threats have been associated with the following exploits:

- Qbot (Botnet)
- Cryptolocker (Ransomware)
- GozNym (Banking Trojan)
- Gootkit (Banking Trojan)
- Locky (Ransomware)

References*

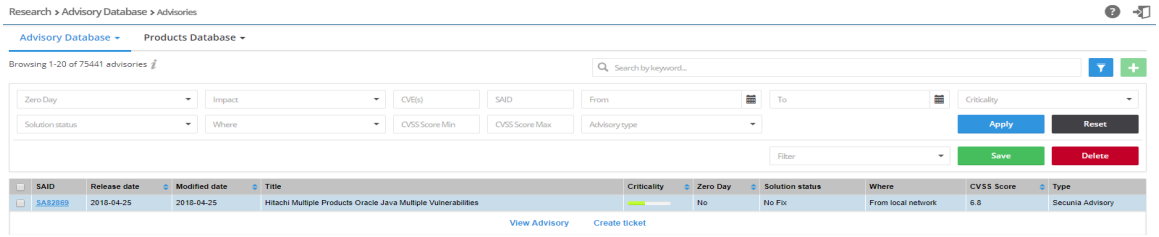
ST	http://www.securitytracker.com/id?1035202
BID	http://www.securityfocus.com/bid/84109
Microsoft Security Bulletin	http://technet.microsoft.com/security/bulletin/MS16-028

NOTE:
* The information is written and maintained by CVE MITRE.
The data on this page reflects neither the opinions of Secunia or the results of our research.

Back

Advisories without Threat Score

The **Advisories** page without the Threat Score is shown below:



Task ***To view advisories***

1. Open the **Research > Advisory Database > Advisories** page.
2. Use Search by keyword to filter the Advisories by the text you enter.

3. Click 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.

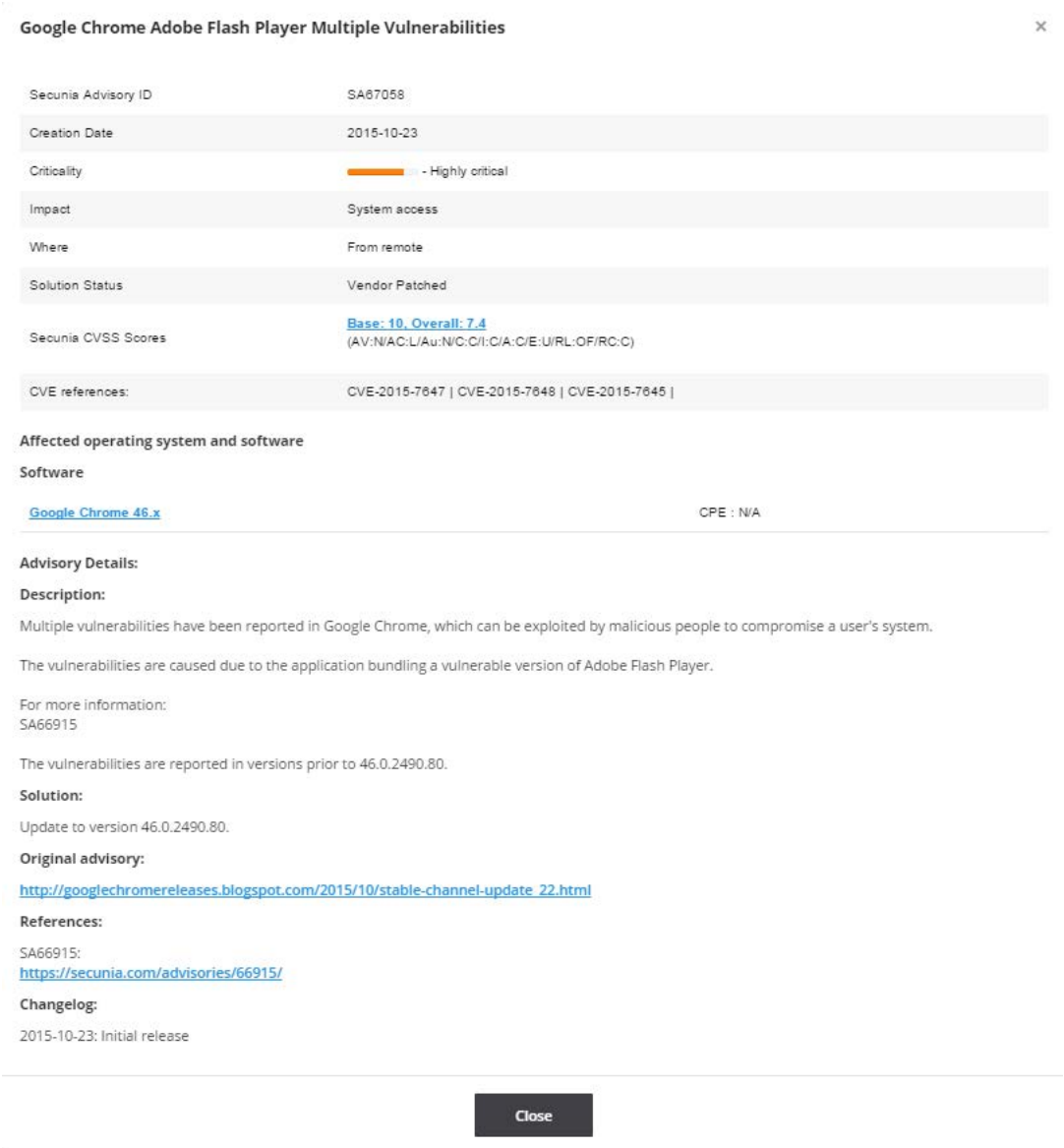
5. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

   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.



Google Chrome Adobe Flash Player Multiple Vulnerabilities

Secunia Advisory ID	SA67058
Creation Date	2015-10-23
Criticality	- Highly critical
Impact	System access
Where	From remote
Solution Status	Vendor Patched
Secunia CVSS Scores	Base: 10, Overall: 7.4 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C)
CVE references:	CVE-2015-7647 | CVE-2015-7648 | CVE-2015-7645 |

Affected operating system and software

Software

Google Chrome 46.x — 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:
SA66915

The vulnerabilities are reported in versions prior to 46.0.2490.80.

Solution:

Update to version 46.0.2490.80.

Original advisory:

http://googlechromereleases.blogspot.com/2015/10/stable-channel-update_22.html

References:

SA66915:
https://secunia.com/advisories/66915/

Changelog:

2015-10-23: Initial release

Close

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.

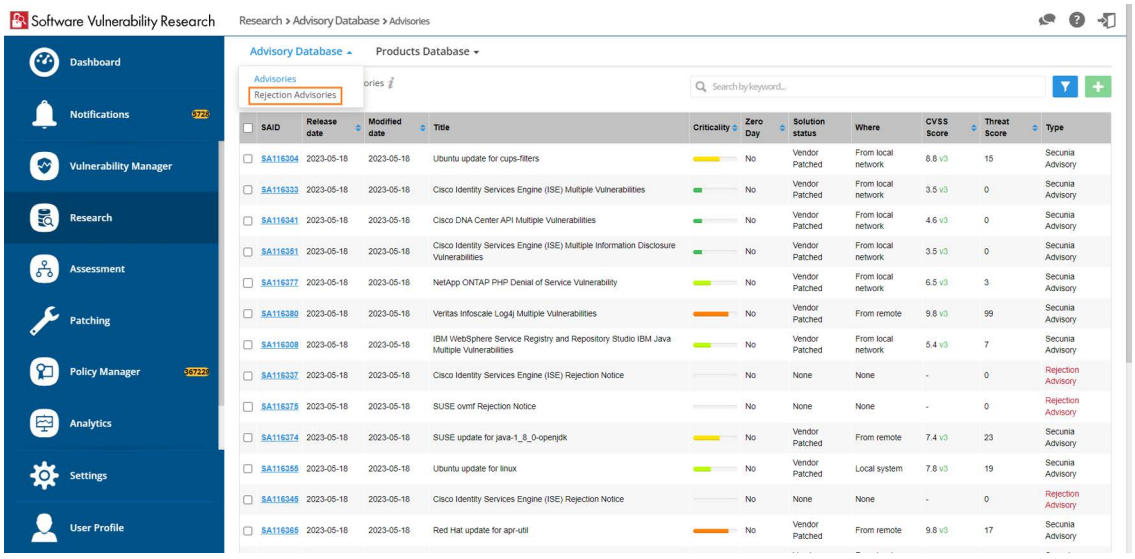
An advisory can be rejected for one of many reasons. The most common are:

- **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. The **Solution Status** of a rejected advisory will show **Possibly Fixed** for the following two conditions:
   - The Link to Original Advisory field is populated (non-empty).
   - The CPE (Common Platform Enumeration) field is populated (non-empty).

   If either of these fields is empty, the solution status will remain **None**.
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 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.*

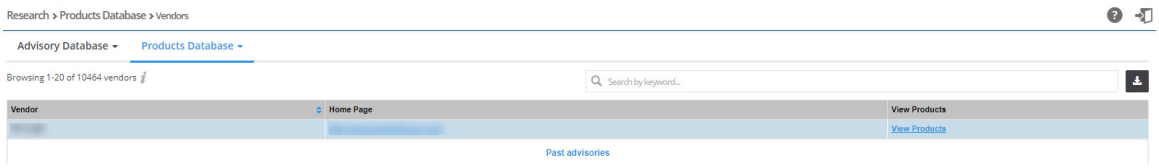
Products Database

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***

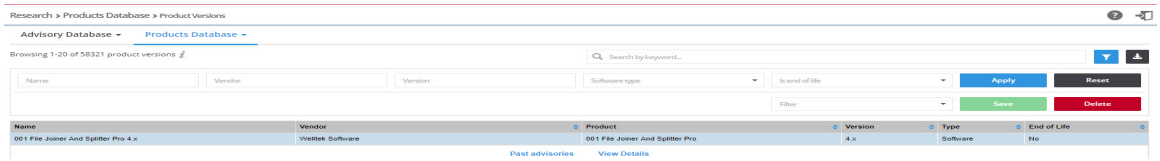
1. Open the **Research > Products Database > Vendors** page.
2. To search for a specific vendor, pick a name from the **Vendor** column, enter it in the **Search by keyword** field and press **Enter**.
3. Click to download a CSV file containing details of all vendors.

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.



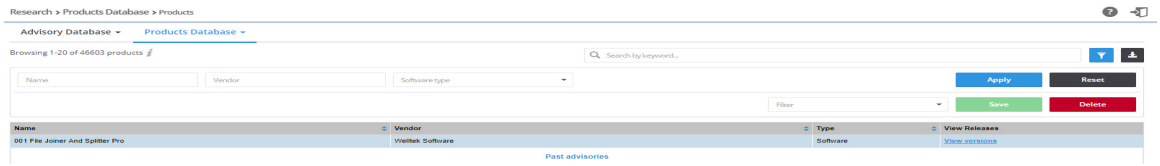
2. Click a product version in the grid to view past advisories related to the product version.
3. To search for a specific product version, pick a number from the **Version** column, enter it in the **Search by keyword** field and press **Enter**.
4. Click to filter the results by **Name**, **Vendor**, **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.

Task ***To view products***

1. Open the **Products** page.

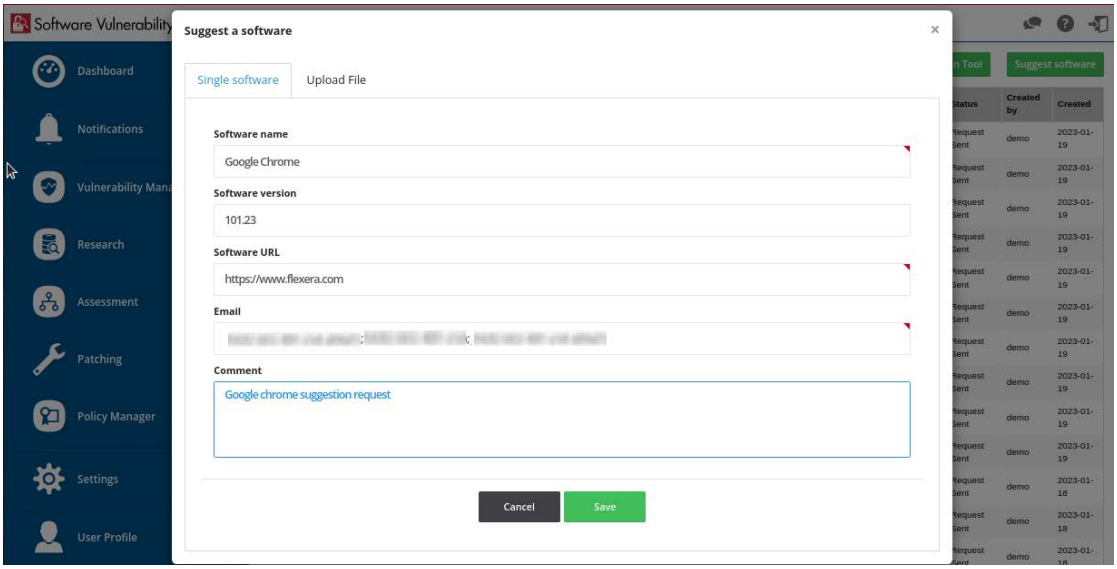


2. Click a product in the grid to view past advisories related to the product.
3. To search for a specific product, pick a name from the Name column, enter it in the **Search by keyword** field and press **Enter**.
4. Click to filter the results by **Name**, **Vendor**, and **Software type** (Software/Operating 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 detail**s.
8. Click to download a CSV file containing details of all products.

Suggest Software

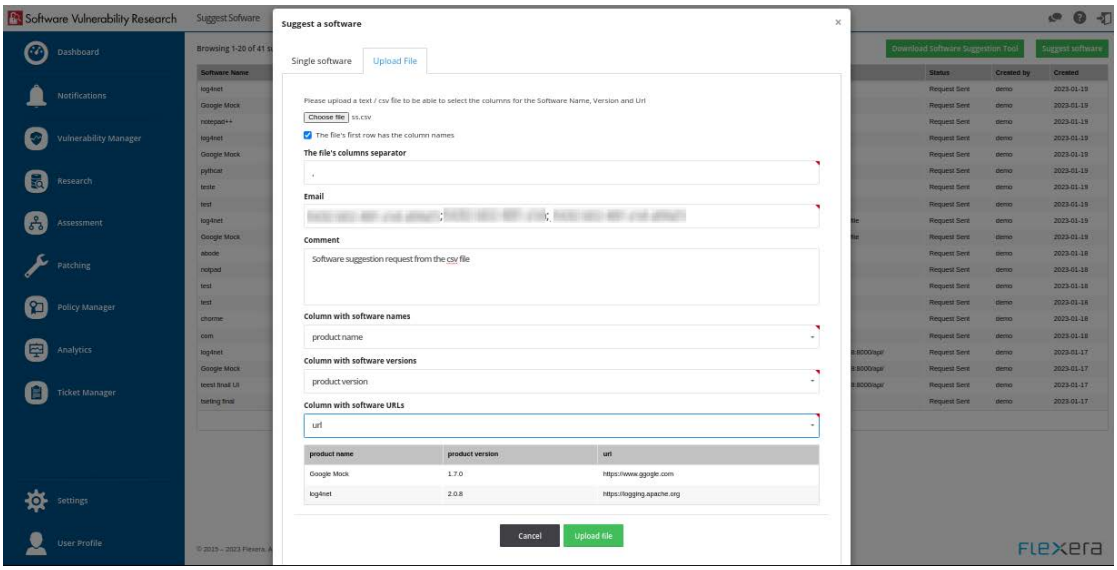
Use the **Suggest Software** page to suggest new software to our Research Team. After clicking the **Suggest Software** button, the **Suggest a software** window appears. You must provide a Software name, Software version, a valid URL to the software Internet page, valid email addresses, and an optional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



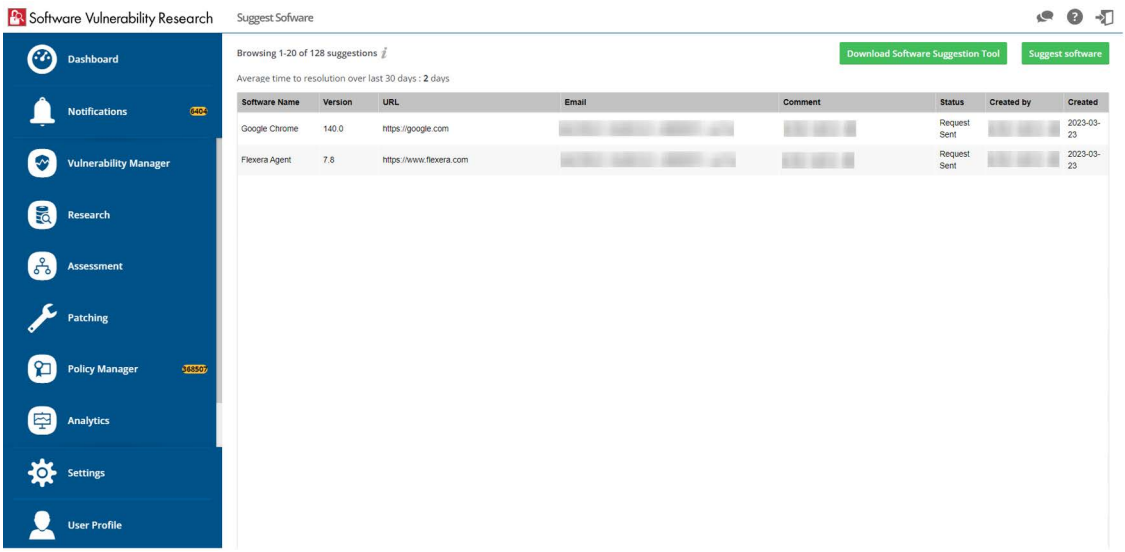
Upon successful import, all entries present in the CSV file will be displayed in the Suggest Software page. Under **Status** column you can view the status as given below:

Table 7-1 • Suggest Software Status Column Details

Status	Description
Request Sent	Indicates the suggested software request as been sent to SVR.

Table 7-1 • Suggest Software Status Column Details

Status	Description
Needs Clarification	Indicates that the suggested software request needs clarification.
In Progress	Indicates the suggested software request is In progress.
Not Applicable	Indicates that the suggested software suggestions can not be tracked.
Pending Review	Indicates that the suggested software review in pending
Completed	Indicates that the suggested software is added to SVR.
Rejected	Indicates that the suggested software request is rejected.



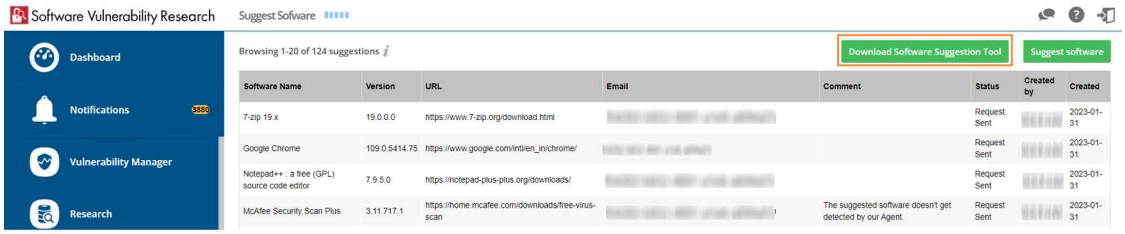
You can view the average resolution time for addressing suggested software.

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.

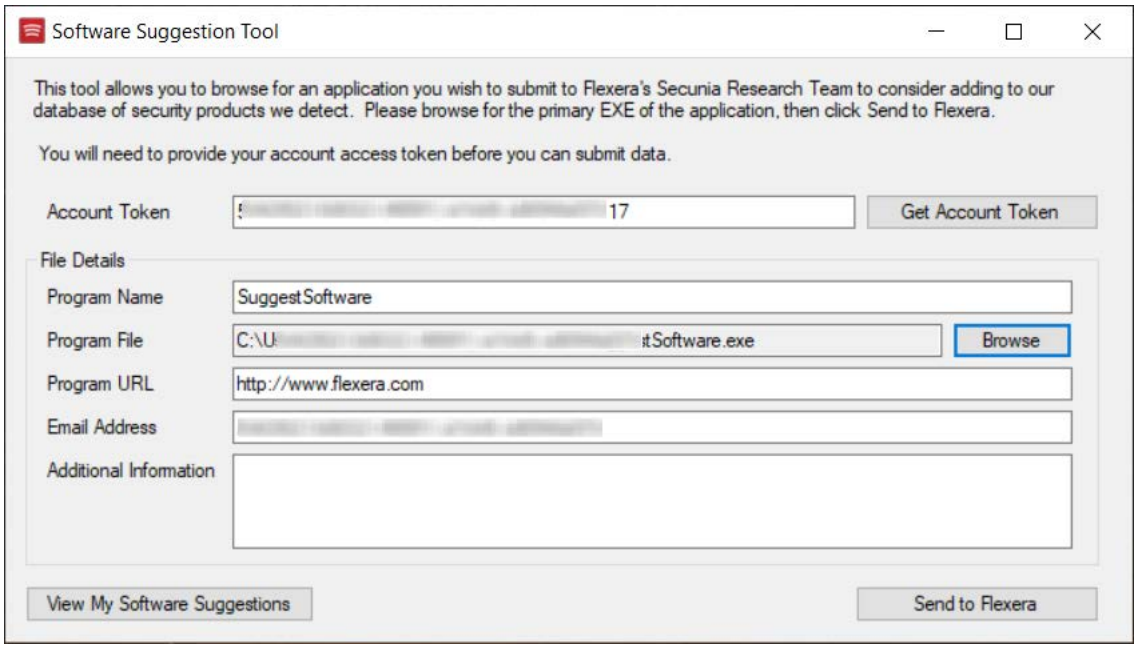


3. Open the Software Suggestion Tool.

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

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

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.

Vulnerability Database

The Vulnerability Database represents the full list of Vulnerabilities tracked by our database.

- Vulnerabilities

Vulnerabilities

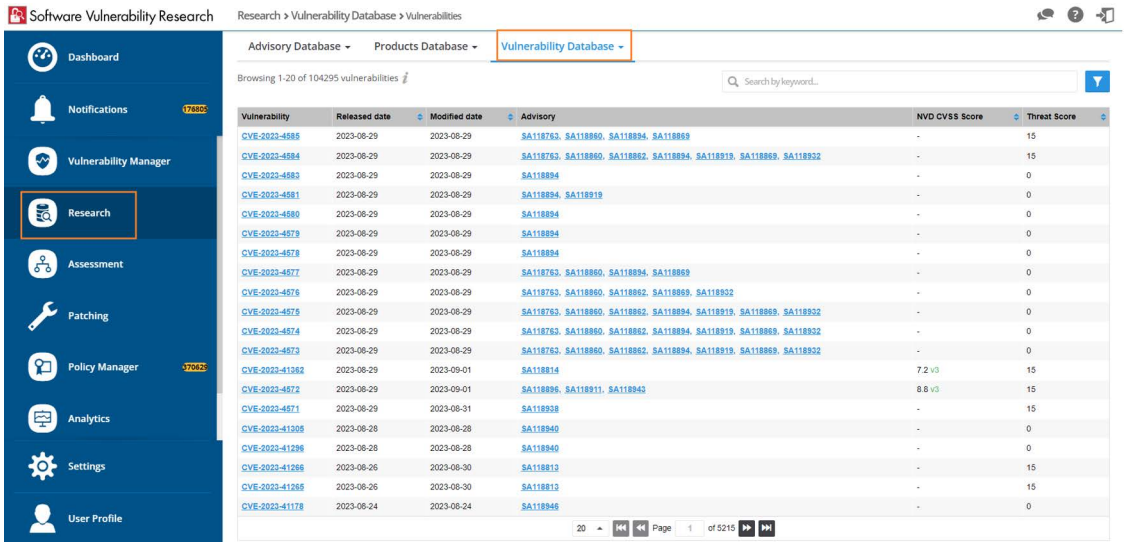
The **Vulnerabilities** page displays a list of all available NVD Vulnerability (CVE) references and associated Secunia Advisories in the database.

Searching on a CVE reference 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.

Task ***To view:***

1. Open the **Research > Vulnerability Database > Vulnerabilities** page. The Vulnerabilities page appears.



2. Click CVE reference link and then click **View Vulnerability**. A popup appears with the detailed information related to the CVE and associated Advisories.
3. Clicking CVE Reference link navigates to the cve.mitre.org website for cybersecurity vulnerabilities information.
4. Clicking Secunia Advisory ID (SAID) link to view detailed information related to the Advisory.

8

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*

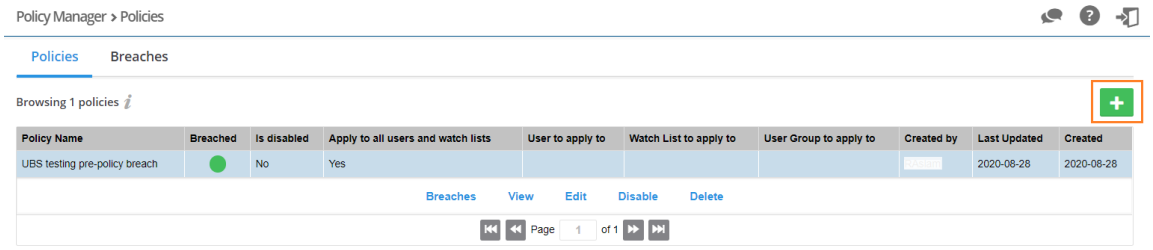
Policies

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:***

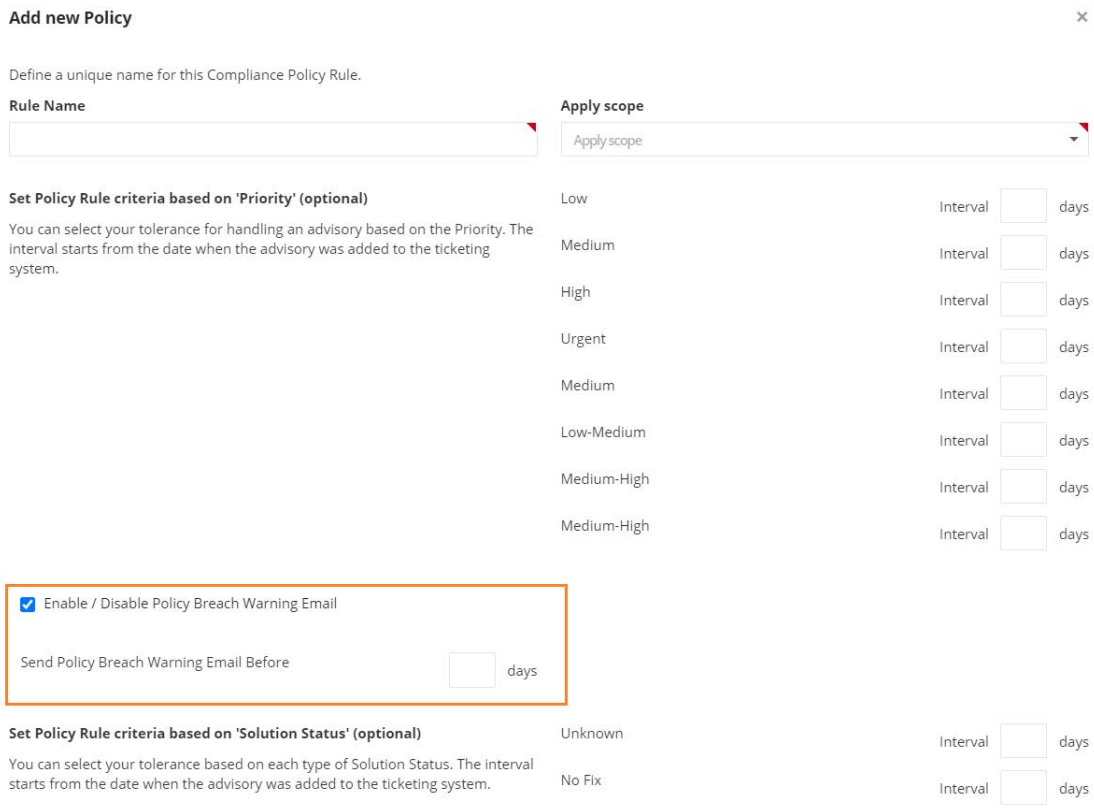
1. To create a new policy, click .



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 specif 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 to export the results to a CSV file.

9

Analytics

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

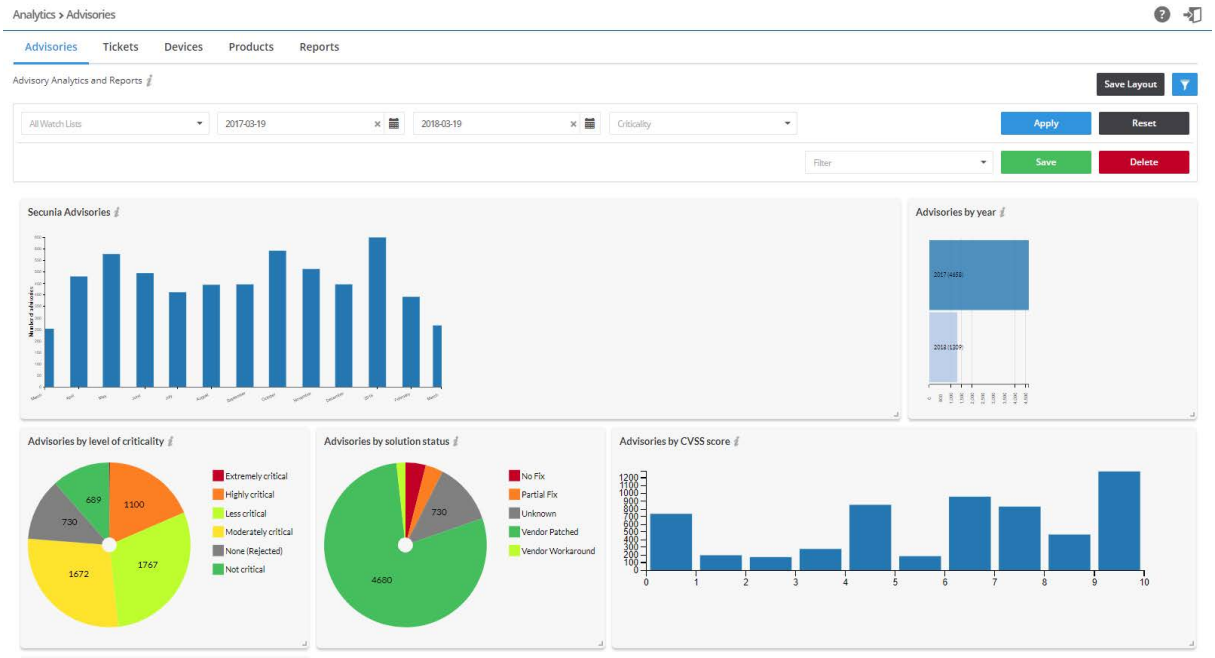
The **Advisories** page displays widgets that contain information regarding:

- **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.*



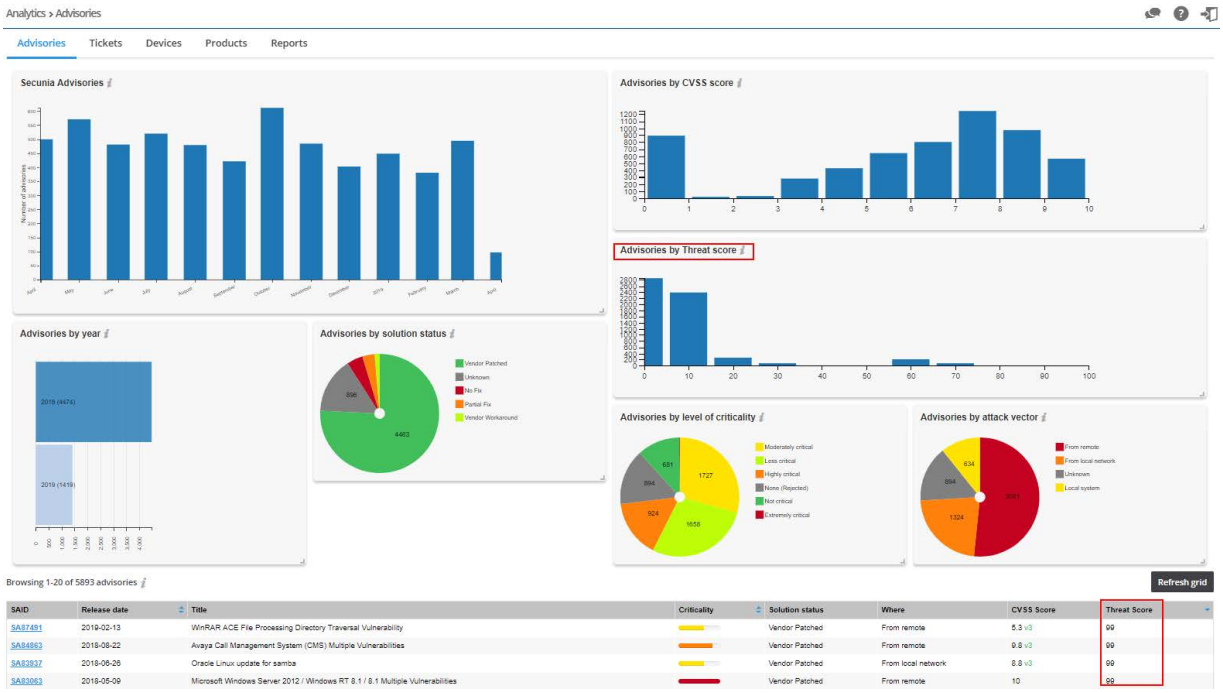
Task ***To view analytics for advisories:***

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*
- *For more details about the Threat Intelligence Modules, see our datasheet: https://www.flexera.com/media/pdfs/datasheet-svm-threat-intelligence-module.pdf*

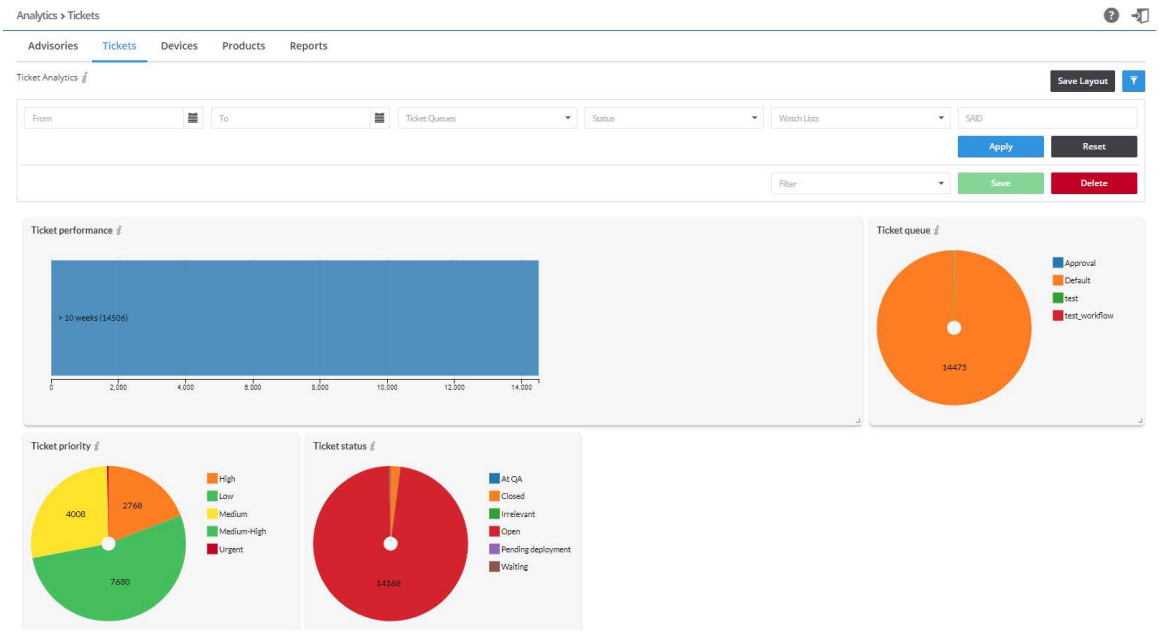
Tickets

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* ℹ *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.

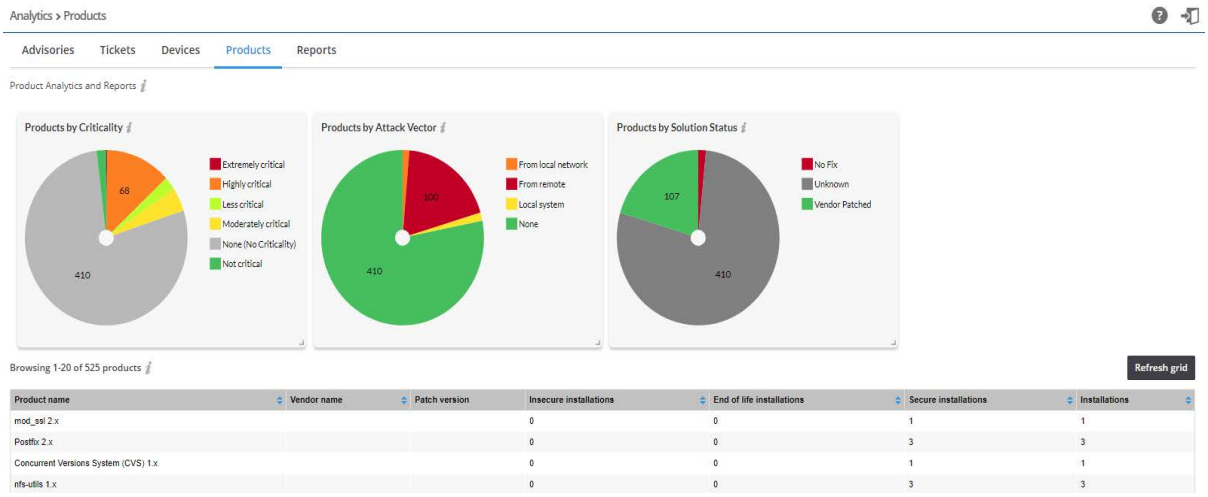
The Devices widgets are dynamic, and you can segment information by clicking the individual chart legends or segments in any widget to alter the data displayed.

Note • *Click the* ℹ *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* ℹ *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.

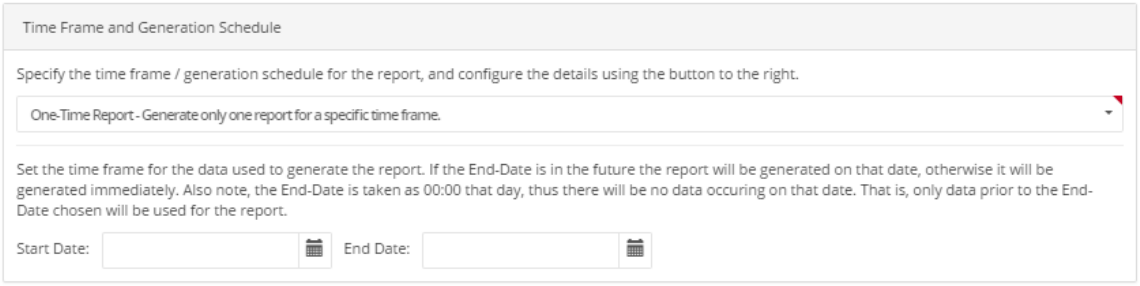
The Reports page displays a list of reports that have been configured and scheduled for generation.

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.

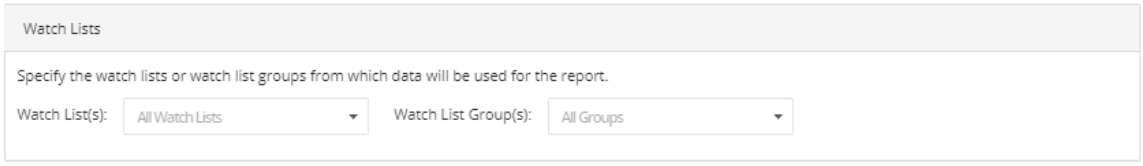
Task ***To create a new Research report:***

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:

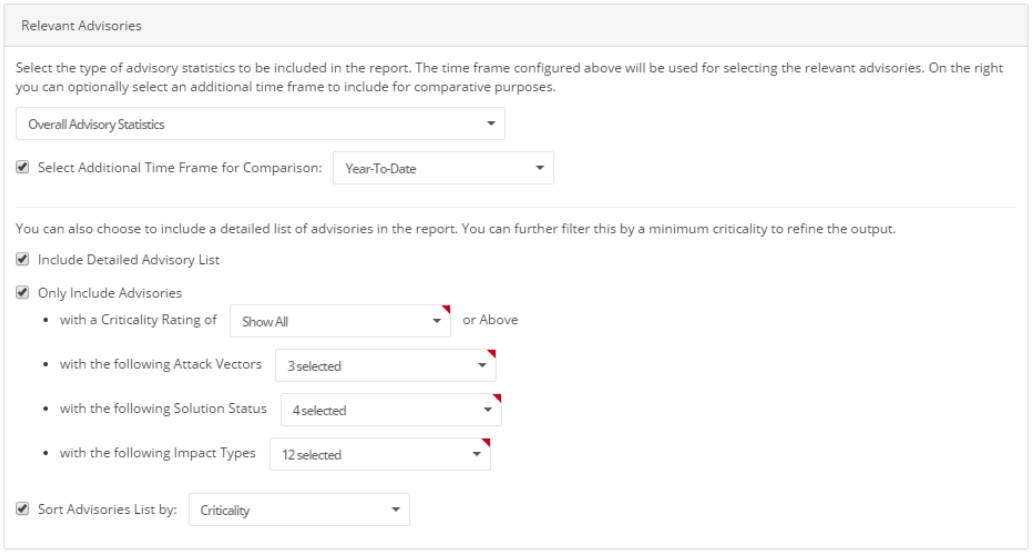


5. Select the **Relevant Advisories** to be included in the report. The time frame configured above will be used for selecting the relevant advisories. You can optionally select an additional time frame to include for comparative purposes. You can select:

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

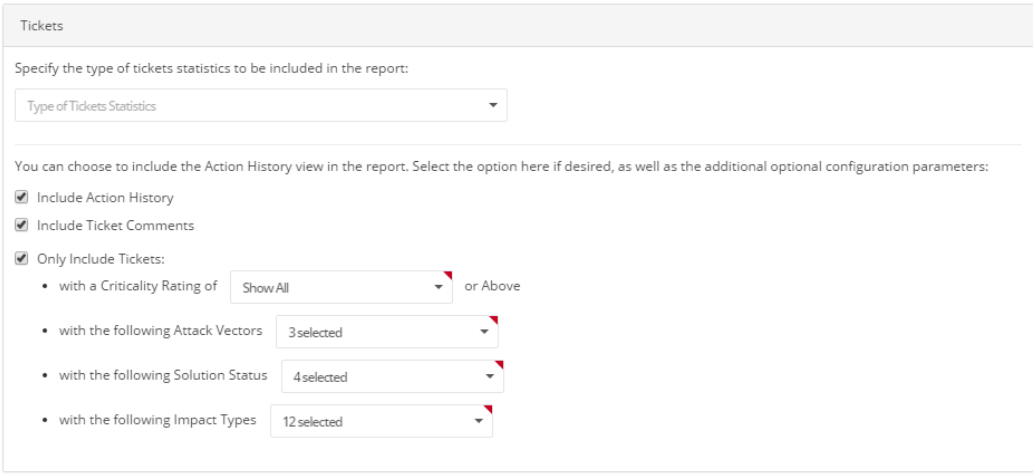
You can choose to include a detailed list of advisories in the report. You can further filter this option by a minimum criticality to refine the output:

- **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)

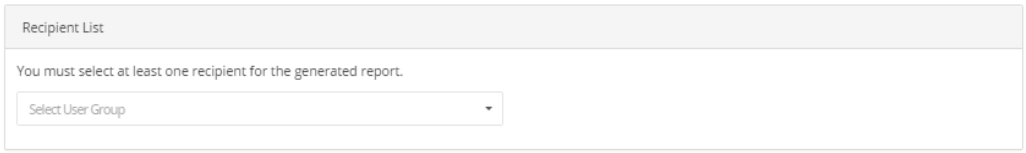


6. Specify the type of Tickets statistics to be included in the report:
   - **Type of Tickets Statistics** (choose from the drop-down list)
   - Include **Action History**

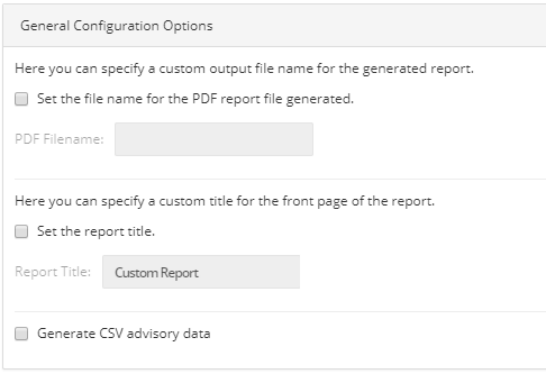
     You can choose to include the Action History view in the report. Select the option here if desired, as well as the additional optional configuration parameters:
   - **Include Ticket Comments**
   - **Only Include Tickets**:
     - with a Criticality Rating of (choose from the drop-down list) or Above
     - 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.

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.*

10

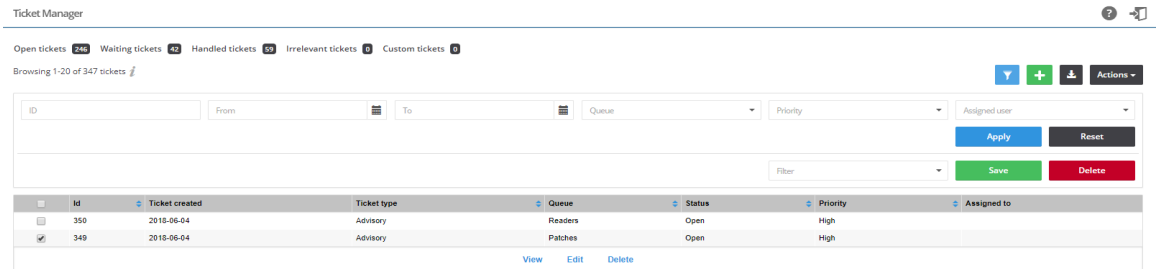
Ticket Manager

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**.

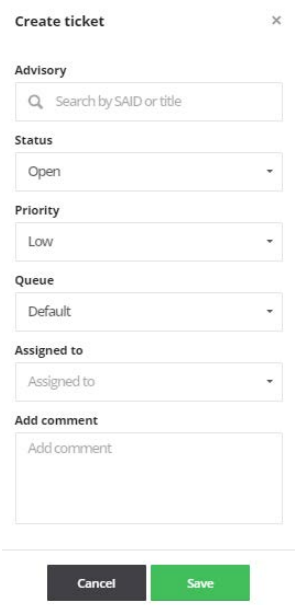
4. Click the **Apply** or **Reset** buttons to apply or reset the filters.
5. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
6. To view one ticket, click the appropriate ticket check box in the grid to **View**, **Edit**, 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.

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.

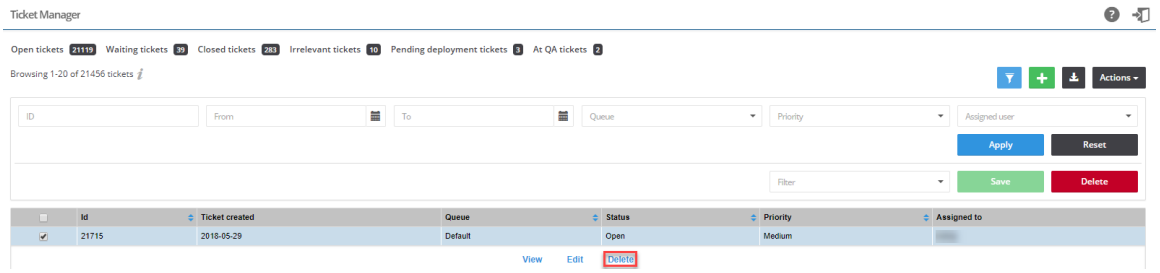
7. In the **Add comment** field, add an appropriate comment to the ticket (mandatory).
8. Click **Save**.

Delete Tickets in Ticket Manager

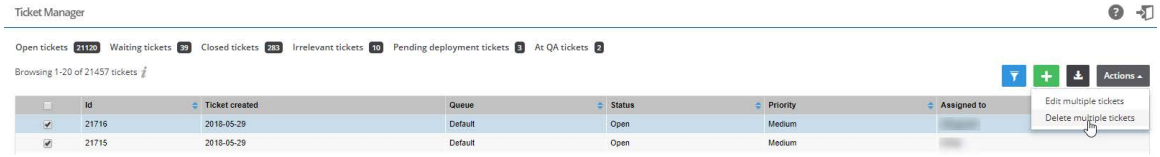
To delete Tickets in Ticket Manager, perform the following steps.

Task ***To delete tickets in Ticket Manager:***

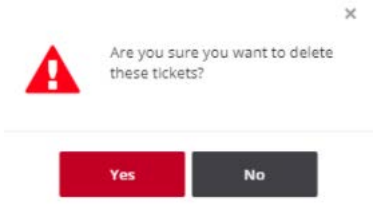
1. Open the **Ticket Manager** page.
2. Insert a check mark in front of the ticket or tickets to delete.
3. To delete one ticket, select **Delete** under the listed ticket in the grid.



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 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 10-1 • Default Ticket Statuses

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

11

Settings

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 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.

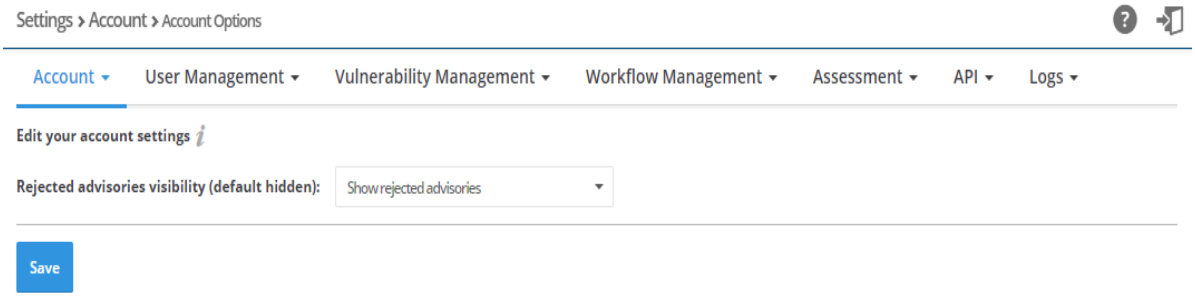
- License Status
- Account Options
- Security Policy

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.



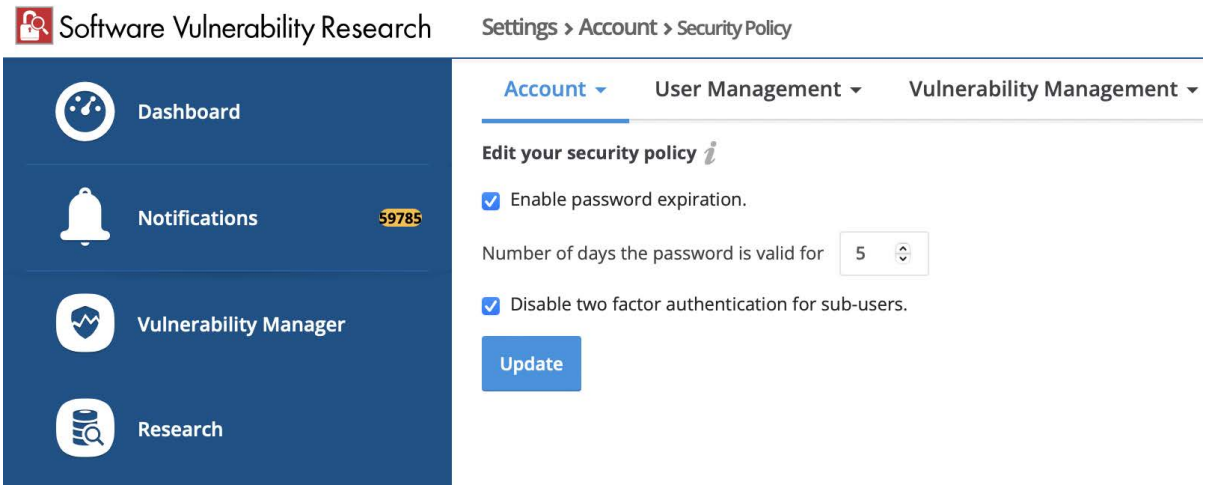
Security Policy

In the **Security Policy** page, you can edit the security policies.

The **Enable Password Expiration** option allows you to activate password expiration for user accounts. If you select this option, passwords will automatically expire after a specified period, requiring users to update their passwords regularly. By default, this option is unselected.

The **Number of days the Password is valid for** option populates only when **Enable Password Expiration** option is selected. You can specify the number of days by entering the desired value directly or by adjusting the value using the up and down arrows. Once the specified number of days has passed, the password will expire, and the user will be prompted to create a new password.

The **Disable Two-Factor Authentication for Sub-Users** option allows you to turn off the two-factor authentication requirement for sub-user accounts. When you select this option, sub-users can log in using only their username and password without needing an additional verification step, such as a code sent to their phone or email. If you unselect this option, Two-Factor Authentication can make the login process. By default, this option is unselected.



Note • *Two factor authentication is considered as a best practice for the application.*

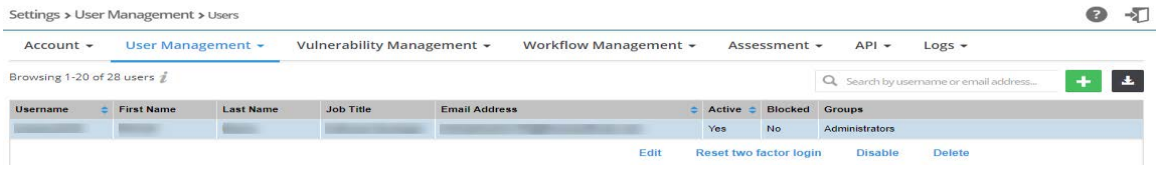
User Management

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
- Roles
- SSO Settings

Users

The **Users** page displays the users associated with your account and, if applicable, the User Groups the user belongs to. Click + 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 a 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 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.*

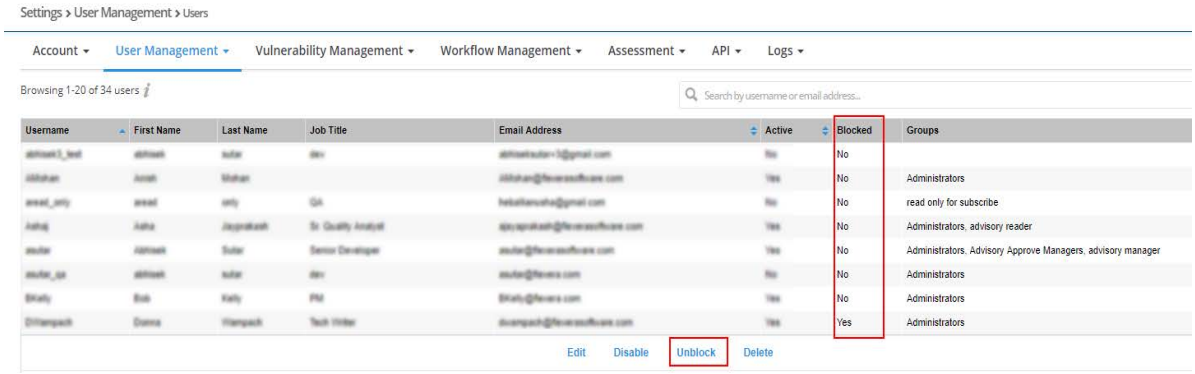
Blocked Users

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 ***To unblock blocked users:***

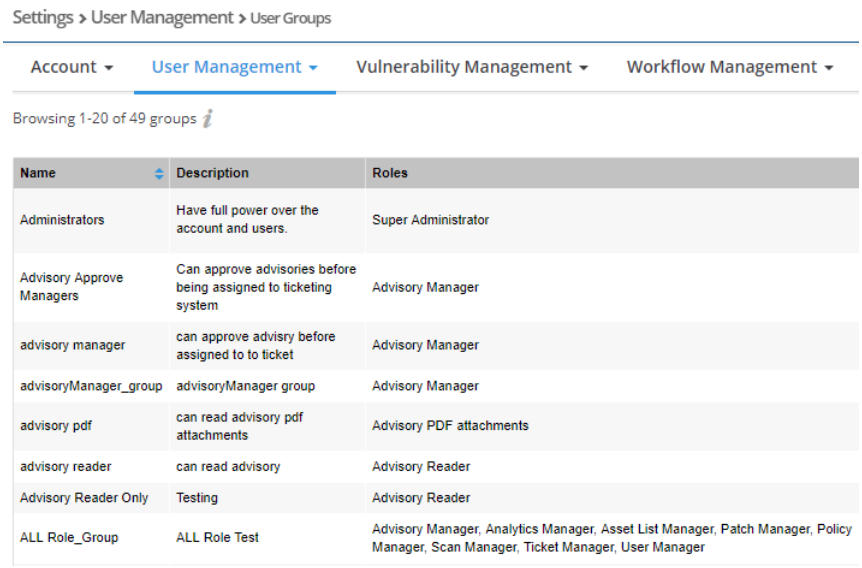
1. Locate the list of user account details in **Settings > User Management > Users**. In the **Blocked** column, **Yes** will be marked for the respective users.
2. Select the user details and click **Unblock** button.
3. Now in the **Blocked** column, **Yes** will be changed to **No**.



Note • *Only an **Admin** user can unblock the blocked users*

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.



Name	Description	Roles
Administrators	Have full power over the account and users.	Super Administrator
Advisory Approve Managers	Can approve advisories before being assigned to ticketing system	Advisory Manager
advisory manager	can approve advisry before assigned to to ticket	Advisory Manager
advisoryManager_group	advisoryManager group	Advisory Manager
advisory pdf	can read advisory pdf attachments	Advisory PDF attachments
advisory reader	can read advisory	Advisory Reader
Advisory Reader Only	Testing	Advisory Reader
ALL Role_Group	ALL Role Test	Advisory Manager, Analytics Manager, Asset List Manager, Patch Manager, Policy Manager, Scan Manager, Ticket Manager, User Manager

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.

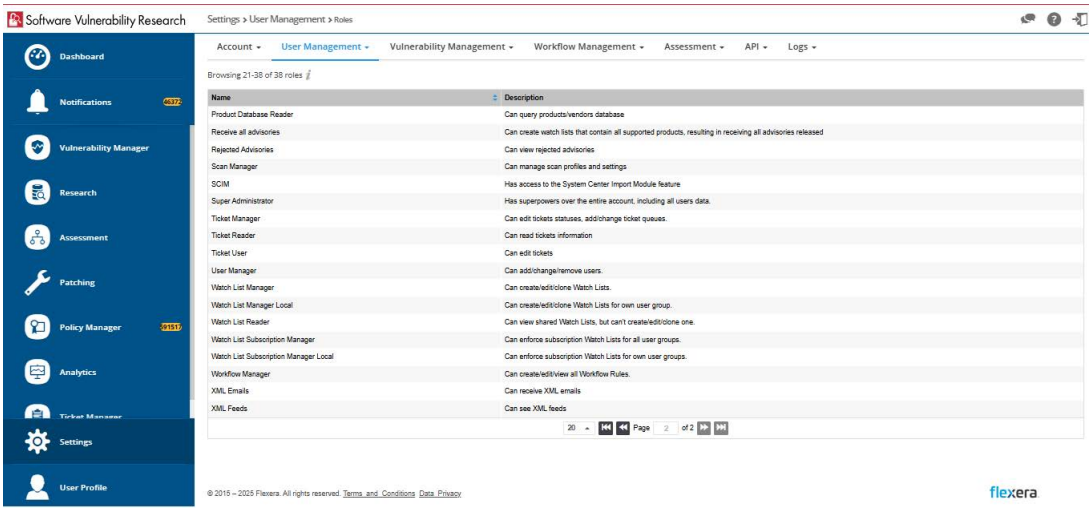
User groups can be linked to one or several predefined User profiles for access control.

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 11-1 • SSO Settings / IDP Configuration Instructions

Setting	Description
Single Sign On URL	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.
Account Key	Set this field in your Identity Provider (IdP) as a SAML attribute named accountKey.
Generate and Show Key	Click to generate and display the Account Key. ***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 Metadata URL	Lists the Service Provider Metadata URL.

Service Provider Configuration

Under **SSO Settings** on the **Settings > User Management** tab, you can specify the following **Service Provider Configuration** settings.

Table 11-2 • SSO Settings / Service Provider Configuration

Setting	Description
SSO Enabled	Select this option to enable Single Sign-On.
Disable standard login	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.*
Upload IDP Metadata XML file	Select this option if you want to upload the IDP metadata XML file.
Provide IDP Metadata URL	Select this option if you want to enter the identity provider metadata URL into the **IDP Metadata URL** field.

Table 11-2 • SSO Settings / Service Provider Configuration

Setting	Description
Automatically create new users	Select this option to automatically create new users.
Default groups for new users	Specify the default group for new users.

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.

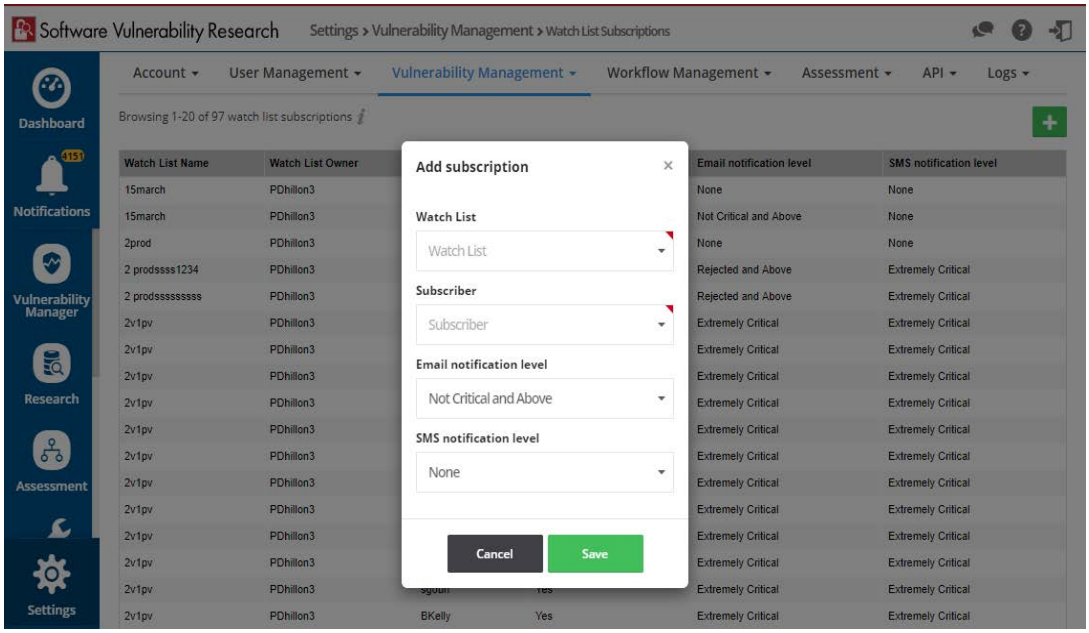
Watch List Subscriptions

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***

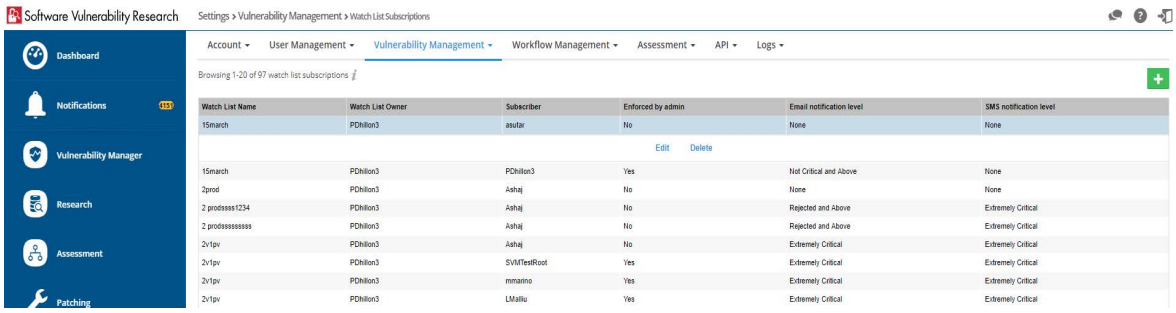
1. Open the **Settings > Vulnerability Management > Watch List Subscriptions** page.
2. To add a new subscription, Click . The **Add subscription** tab opens.



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
   - 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.

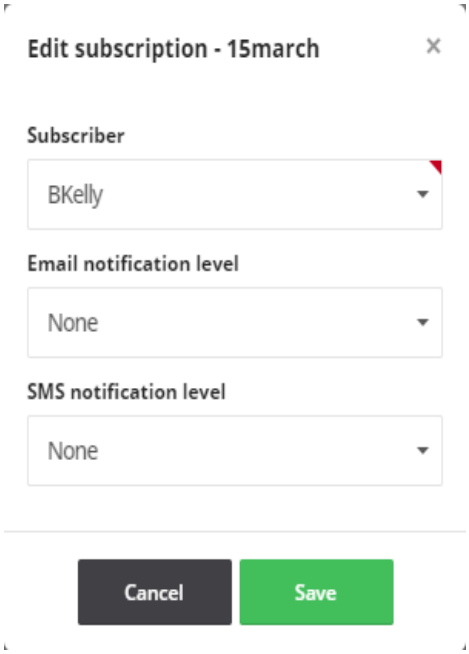
8. List of added subscriptions will appear in the **Settings > Vulnerability Management > Watch List Subscriptions,** Admin user can edit or delete any existing subscription from the list.

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.



Note • *You can subscribe a user only once to the* ***Watch List***

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.

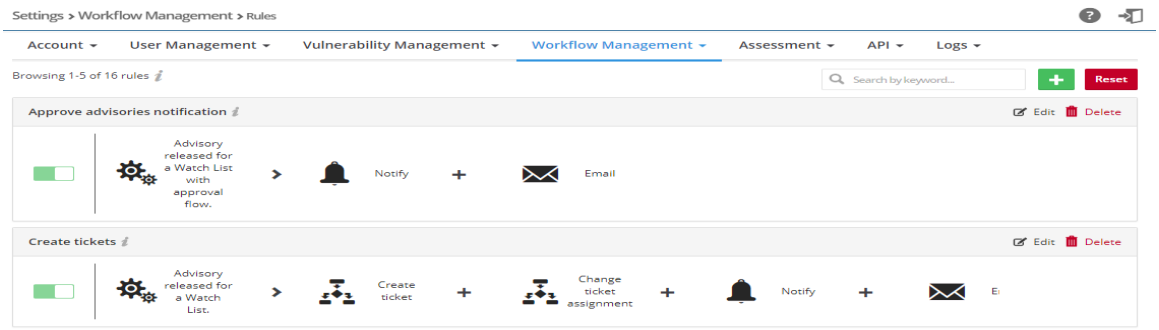
Use the Workflow Management pages to create and edit Rules, Ticket Queues, Ticket Status and Ticket Priorities.

- 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 a minimum 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 11-3 • Rule Channels, Triggers, and Actions

Channel	Trigger	Action

Advisory	• Advisory for Watch List approved
	  • Any Watch List or select a Watch List from the drop-down list
	  • Any Watch List Group or select a Watch List Group from the drop-down list
	  • Select Advisory Condition or select a Advisory Condition from the drop down list
	• Advisory for Watch List changed
	  • Any Watch List or select a Watch List from the drop-down list
	  • Any Watch List Group or select a Watch List Group from the drop-down list
	  • Select Advisory Condition or select a Advisory Condition from the drop down list
	• Advisory released for a Watch List with approval flow
	  • Any Watch List or select a Watch List from the drop-down list
	  • Any Watch List Group or select a Watch List Group from the drop-down list
	  • Select Advisory Condition or select a Advisory Condition from the drop down list
	• Advisory released for a Watch List
	  • Any Watch List or select a Watch List from the drop-down list
	  • Any Watch List Group or select a Watch List Group from the drop-down list
	  • Select Advisory Condition or select a Advisory Condition from the drop down list
	• Product version end-of-life
	  • Notify for all, default only for my tracked product versions (select Yes or No from the drop-down list)
		• Email
		• SMS
		• Notify
		• Create Advisory for Watch List
		• Create ticket
		• Change ticket assignment
		• Change ticket queue
		• Change ticket status
		
		Note • *Threat Score details are added in the Email notification for users with the Threat Intelligence Module*

Table 11-3 • Rule Channels, Triggers, and Actions (cont.)

Channel	Trigger	Action

Advisory
(continued)
	• Advisory Threat for Watch List changed
	  • Any Watch List or select a Watch List from the drop-down list
	  • Any Watch List Group or select a Watch List Group from the drop-down list
	  • Select Advisory Condition or select a Advisory Condition from the drop down list
	  • Skip trigger if score decreases (Select Yes or No from the drop down list)
	
	Note *• This add-on requires purchase of the Software Vulnerability Research Threat intelligence Module*	

Analytics	• PDF Report Generated	• Email PDF report • Email • SMS • Notify
Policy	• Policy Breached	• Email • SMS • Notify
Release Notes	• New Release arrived	• Email
Ticketing	• Ticket assigned to me • Ticket changed • Changed by me (select Yes or No from the drop-down list) • Ticket created • Ticket priority changed • Ticket queue changed • Ticket status changed	• Email • SMS • Notify • Create ticket • Change ticket status • Change ticket queue • Change ticket assignment

Table 11-3 • Rule Channels, Triggers, and Actions (cont.)

Channel	Trigger	Action

User	• Password changed
	  • User (select from the drop-down list)
	• User Logged in
	  • User (select from the drop-down list)
		• Email
		• SMS
		• Notify

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:

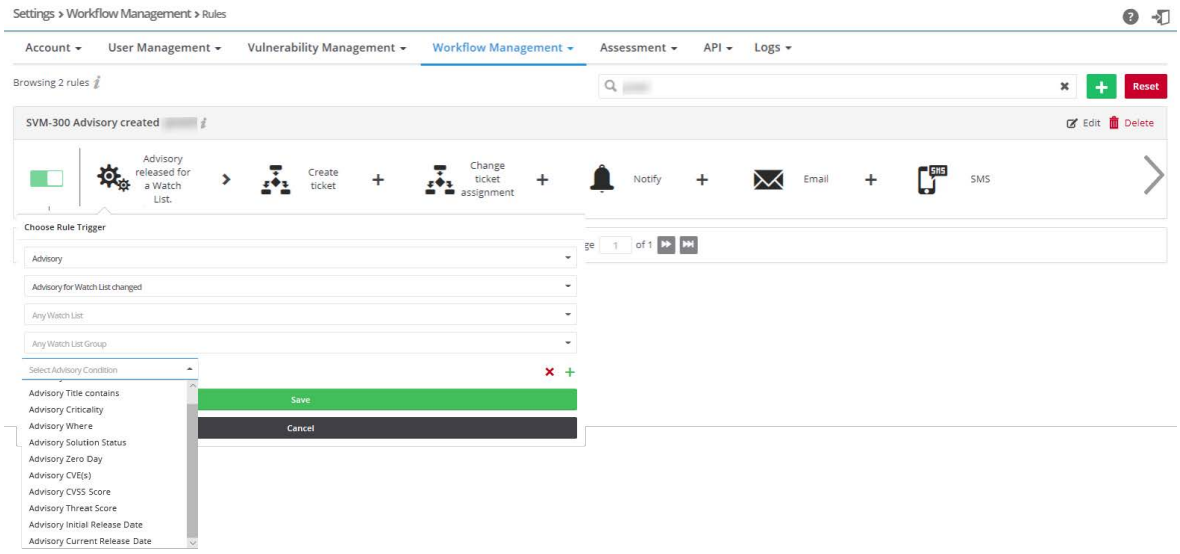
- Create a Workflow Rule to Send an Advisory and Ticket Information After Approval
- Create a Workflow Rule to Create a Patching Ticket
- Create a Workflow Rule to Send a New Release Notes Notification to Non-Administrators

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
   - 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.



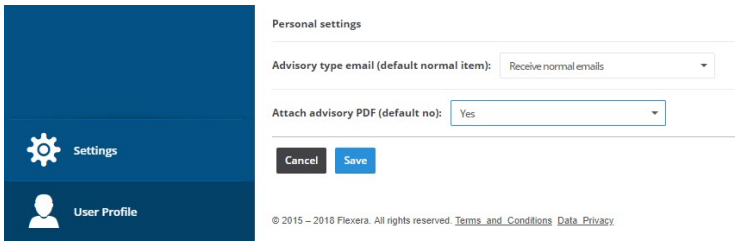
Note • *Customized workflow rules for Watch Lists take precedence over non-customized workflow rules using the following hierarchy from most important to least important:*

- *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.

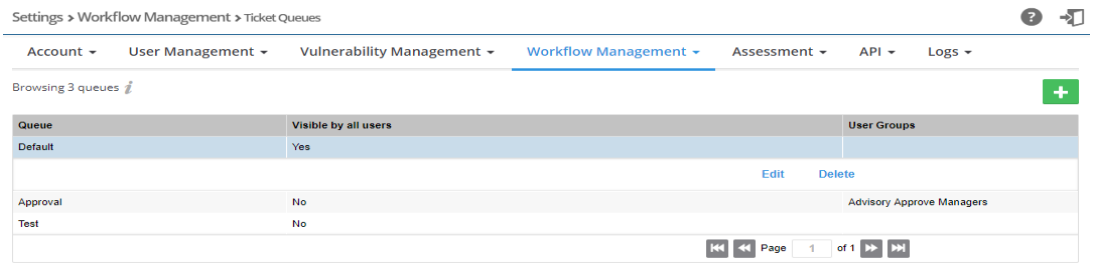
Note • *All administrator accounts are configured to receive release note notification emails in the Notifications module.*

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.

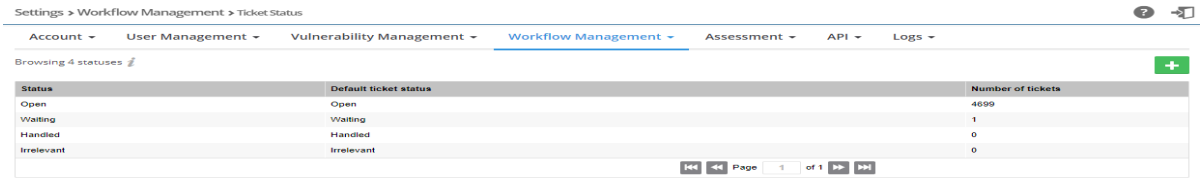


Ticket Queues can be used for sharing and limiting access to tickets for users. You can create ticket queues that are relevant to a limited subset of your users (for instance only for Linux administrators or for Windows administrators) and use Rules to create tickets from special Watch Lists directly 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.



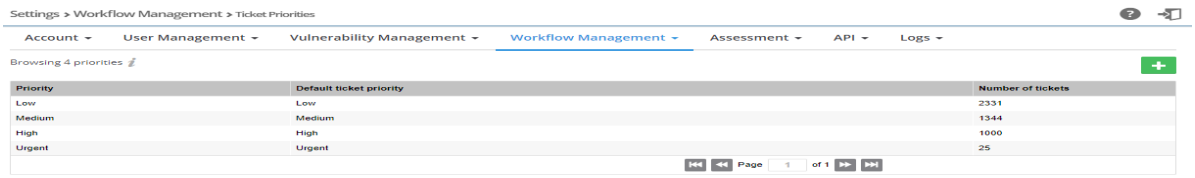
Click + to add a ticket status. The default values are:

- 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
- Medium
- High
- Urgent

You can click any Ticket Priority that you have added to edit or delete priorities that do not have tickets assigned.

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:

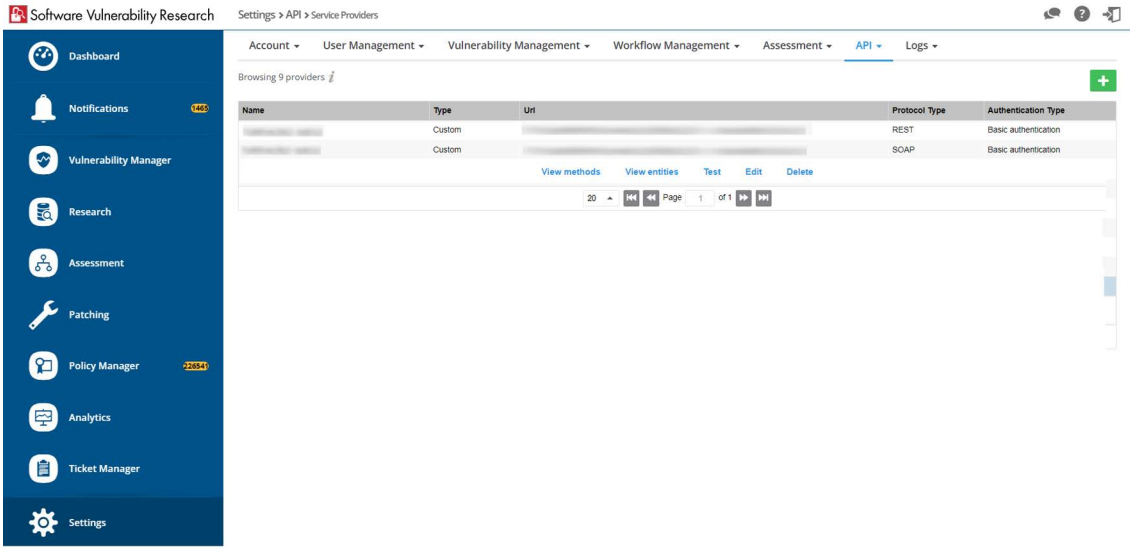
https://docs.flexera.com/svr/api/Default.htm

Note • *Access to the SVR API documentation portal is available through the same Single Sign-On (SSO) credentials and authentication method used by the SVR platform. The only way SSO users can log in to API documentation portal is to log in to the web application and then come back to the API documentation portal.*

Service Providers shows the details of the service providers. For more information, see Service Providers.

Service Providers

Use this page to view, Add, configure and edit the ServiceNow and BMC Remedy for the Service Provider.



This section includes the following topics:

- Configure ServiceNow Instance for Service Provider
- Create Service Method for Service Providers

Configure ServiceNow Instance for Service Provider

Use this page to configure ServiceNow instance for the Service Providers.

Task ***To Configure ServiceNow instance:***

1. In the **Settings** menu, select the **API** tab, then choose **Service Providers** from the drop-down menu. A list of available service providers will appear on the screen.
2. Click + and select **Add recipe for ServiceNow** from the drop down list. A new ServiceNow entry is added to the Service Provider list.
3. Click on the ServiceNow and select **Edit** option. The Edit Provider dialog box will appear.

4. The Edit Provider dialog box includes the following properties:

Property	Description
Type	Choose the required Type from the drop down list. By default ServiceNow will be selected. • Custom • ServiceNow • BMC Remedy
Name	Enter the required name for the selected type. By default, ServiceNow will be selected name.
Url	Enter a valid ServiceNow instance URL.
Protocol Type	Choose the required Protocol type from the drop down list. • REST • SOAP
Authentication type	Choose one of the following Authentication type: • **None—**If no authentication, then leave this property as none. • **Basic authentication—** Enter the appropriate Username and Password.

5. After modifying the above details as needed, click the **Save** button.
6. Upon saving, the modified details will be updated.

Create Service Method for Service Providers

Use this page to create a new Service Method for the Service Providers.

Task ***To create a new Service Method:***

1. In the **Settings** menu, select the **API** tab, then choose **Service Providers** from the drop-down menu. A list of available service providers will appear on the screen.
2. Click on the desired Service Provider and select **View methods** option.
3. In the **Service Methods** page, click the icon. The **Add service method** dialog box will appear.
4. The Add service method dialog box includes the following properties:

Property	Description
Service Provider	ServiceNow will be selected by default as the Service Provider. This property is non-editable.
Name	Enter the valid name.
Url	Enter the valid ServiceNow URL.

Property	Description
Method	Choose the one of the following Method: • GET • POST • PUT • PATCH • DELETE • HEAD • OPTIONS • TRACE
Content	Enter the valid content. Example: {"u_id": #$advisory.id#$, "u_advisory_identifier": #$advisory.advisory_identifier#$}

5. After entering the above details, click the **Save** button.
6. Upon saving, the new Service Method will be added.

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

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.

12

User Profile

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.

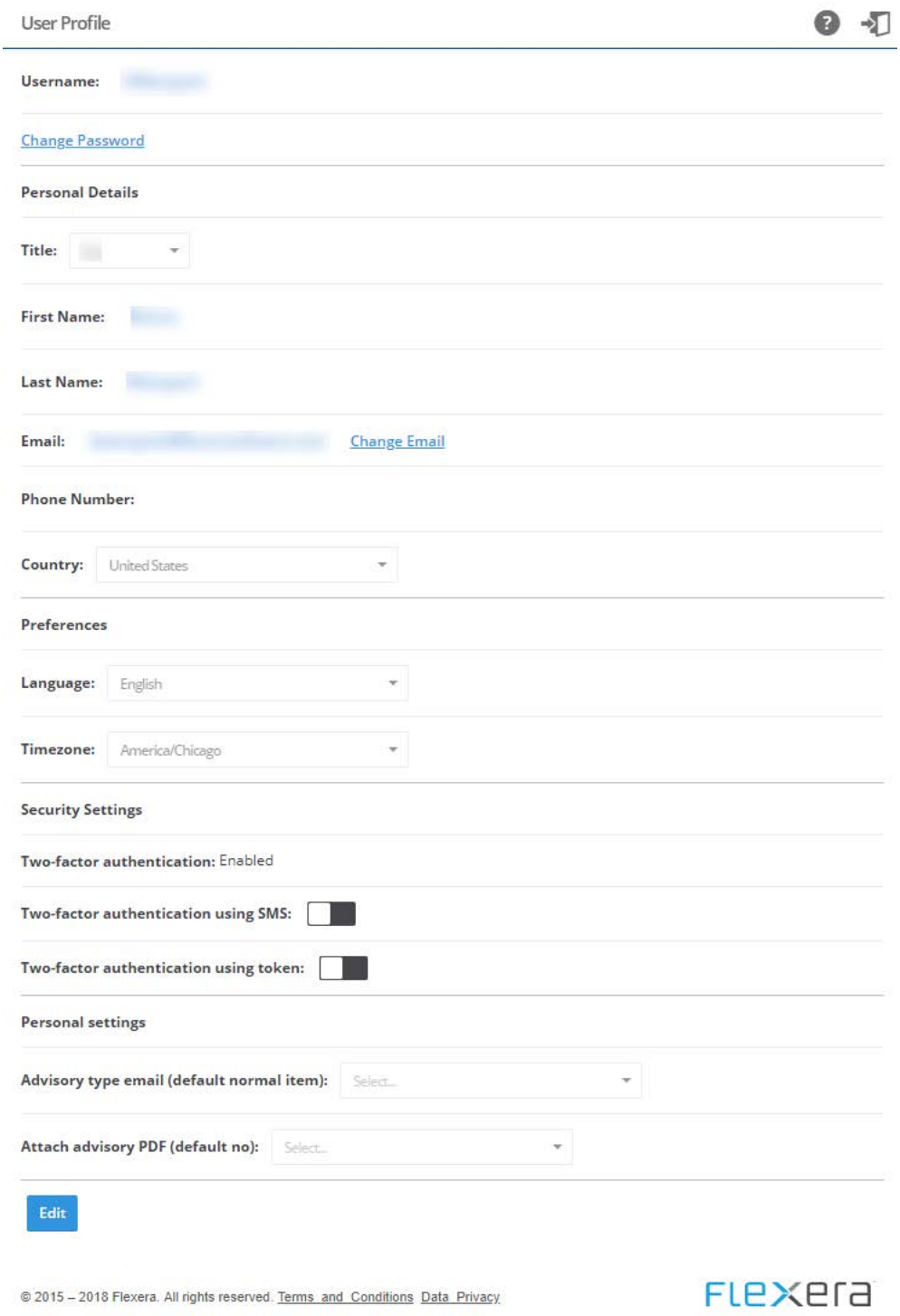


Figure 12-1: User Profile Page

13

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

- CVSSv4 Score
- 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.

CVSSv4 Score

SVR will now support entering all new CVSS scores using the v4 standard. After a CVSS v4 score is entered, the score appears in the User Interface (UI), API, XML, email notifications, and PDF reports.

In the User Interface

The CVSS v4 score is noted with a blue v4 after the score.

In the API

API calls returning CVSS data return another set of values for CVSS v4, so that you can programmatically differentiate between CVSSv2, CVSSv3, and CVSSv4 scores.

`/api/advisories/`

`/api/vulnerabilities/`

In the XML

A change to the schema is necessary to add specific values for CVSSv4 scores. As with the json API values above, a second cvss4 labeled value was added to distinguish v4 scores.

In Email Notifications

Emails contain CVSSv4 labels. The Advisory will show latest CVSS version.

Note • *Email notifications will include CVSS overall score.*

In a PDF Report

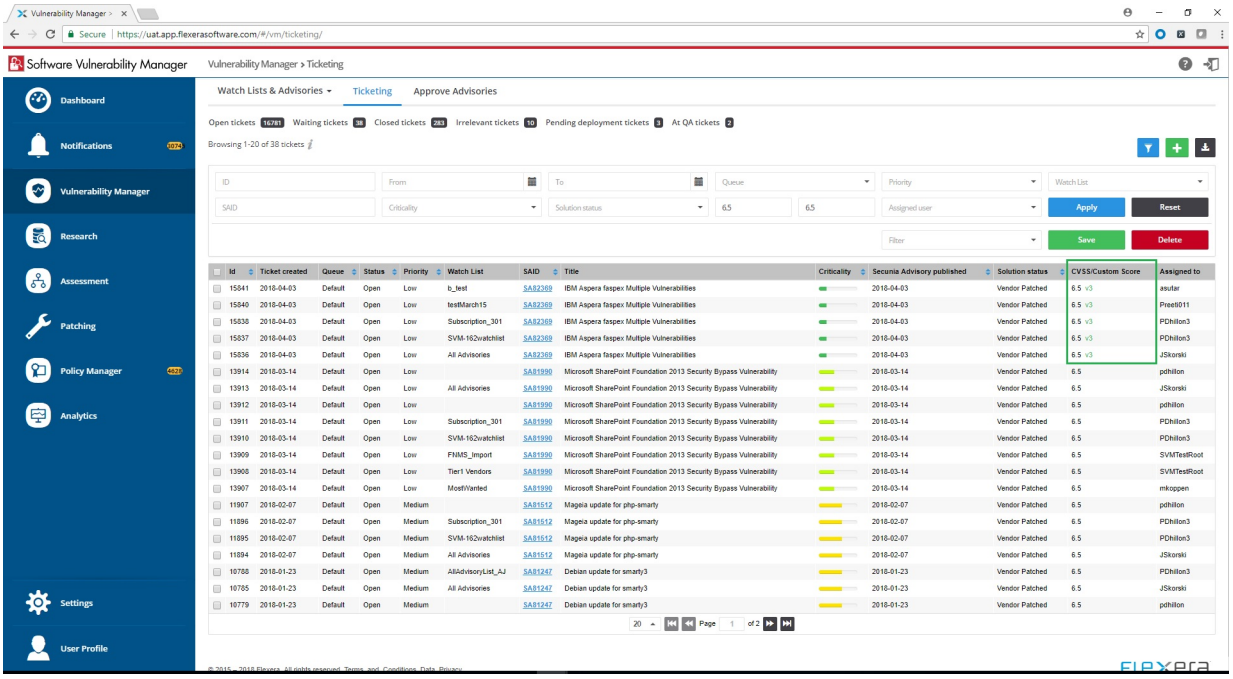
PDF reports containing CVSS values will show CVSS v3 or CVSS v4 as appropriate.

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 programmatically 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).

```
"cvss_info": {
    "cvss_vector": "",
    "cvss_base_score": 0,
    "cvss_overall_score": 0
},
"cvss_score": "0.0",
"cvss_vector": "",
"cvss3_info": {
    "cvss_vector": "CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C",
    "cvss_base_score": 7.8,
    "cvss_overall_score": 6.8
},
"cvss3_score": "7.8",
"cvss3_vector": "CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C",
"cvss_score_ui": "7.8",
```

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.**

```
<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>
<cvss3_vector>CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</cvss3_vector>
<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.

Criticality	Not critical
Release Date	03/11/2022
Last Update	03/11/2022
Solution Status	Vendor Patched
SAID	SA112006
CVSS	0.0 (E:U/RL:OF/RC:C)
CVSS3	Base: 4.7, Overall: 4.1 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N/E:U/RL:O/RC:C
Impact	Spoofing
Where	From remote
Threat Score	0

Note • *Email notifications will include CVSS overall score.*

In a PDF Report

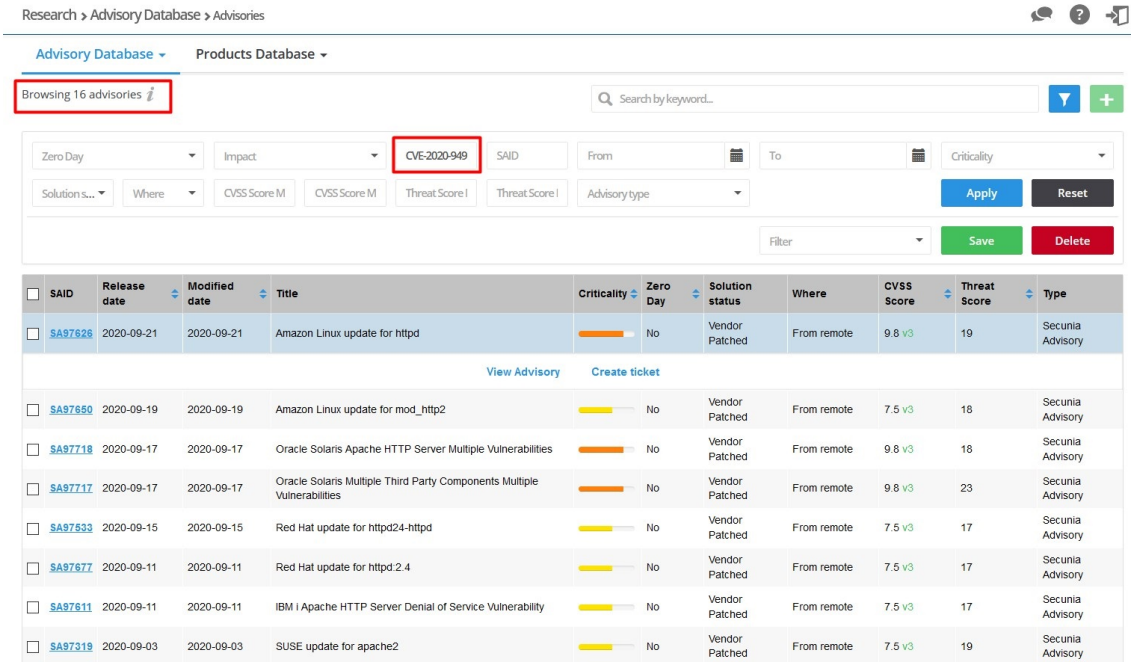
PDF reports containing CVSS values will show CVSSv2 (displayed as CVSS) or CVSSv3 (displayed as CVSS3) as appropriate.

Criticality	- Moderately critical
Impact	System access
Where	From remote
Solution Status	Vendor Patched
Secunia CVSS Scores	CVSS3 Base: 7.8 , Overall: 6.8 CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

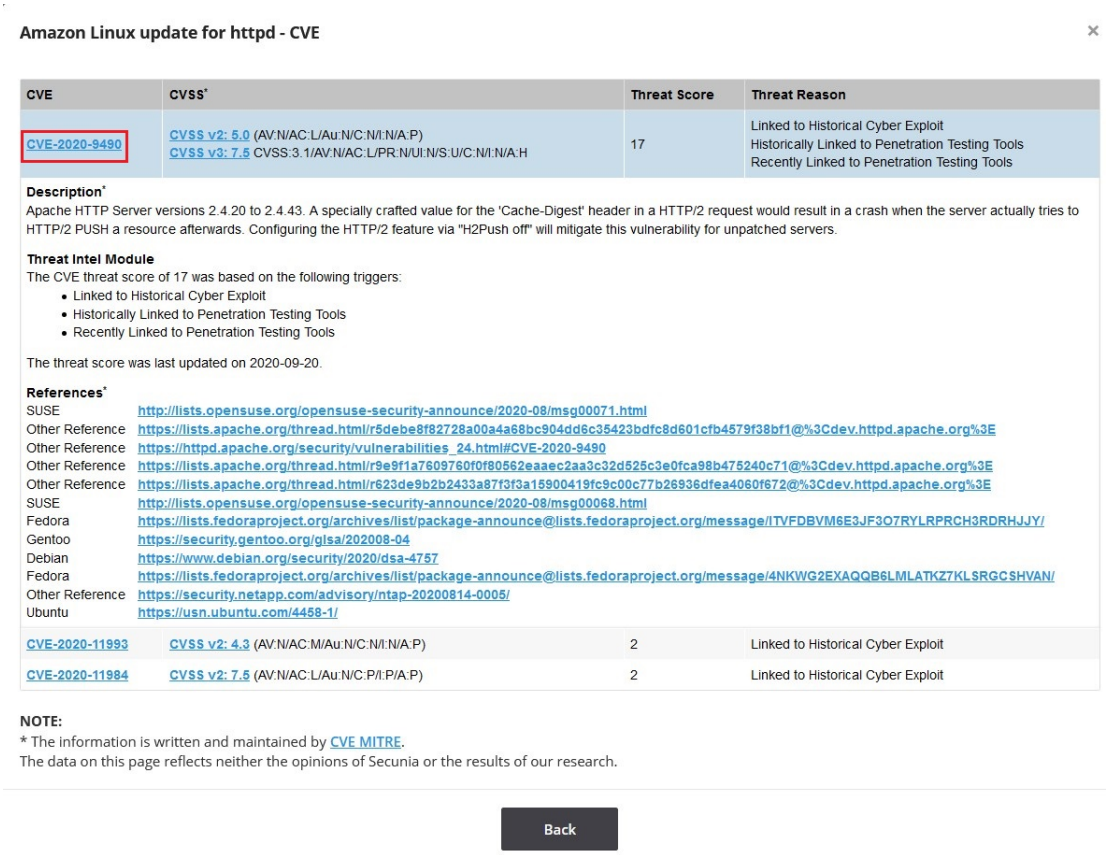
CVE References

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.



Amazon Linux update for httpd - CVE

CVE	CVSS*	Threat Score	Threat Reason
CVE-2020-9490	CVSS v2: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P) CVSS v3: 7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	17	Linked to Historical Cyber Exploit Historically Linked to Penetration Testing Tools Recently Linked to Penetration Testing Tools

Description*
Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

Threat Intel Module
The CVE threat score of 17 was based on the following triggers:
- Linked to Historical Cyber Exploit
- Historically Linked to Penetration Testing Tools
- Recently Linked to Penetration Testing Tools

The threat score was last updated on 2020-09-20.

References*

SUSE	http://lists.opensuse.org/opensuse-security-announce/2020-08/msg00071.html
Other Reference	https://lists.apache.org/thread.html/r5debe8f82728a00a4a68bc904dd6c35423bdfc8d601cfb4579f38bf1@%3Cdev.httpd.apache.org%3E
Other Reference	https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2020-9490
Other Reference	https://lists.apache.org/thread.html/r9e9f1a7609760f0f80562eaaec2aa3c32d525c3e0fca98b475240c71@%3Cdev.httpd.apache.org%3E
Other Reference	https://lists.apache.org/thread.html/r623de9b2b2433a87f3f3a15900419fc9c00c77b26936dfea4060f672@%3Cdev.httpd.apache.org%3E
SUSE	http://lists.opensuse.org/opensuse-security-announce/2020-08/msg00068.html
Fedora	https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/ITVFDBVM6E3JF3O7RYLRPRCH3RDRHJJY/
Gentoo	https://security.gentoo.org/glsa/202008-04
Debian	https://www.debian.org/security/2020/dsa-4757
Fedora	https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/4NKWG2EXAQQB6LMLATKZ7KLSRGCSHVAN/
Other Reference	https://security.netapp.com/advisory/ntap-20200814-0005/
Ubuntu	https://usn.ubuntu.com/4458-1/

CVE-2020-11993	CVSS v2: 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)	2	Linked to Historical Cyber Exploit
CVE-2020-11984	CVSS v2: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)	2	Linked to Historical Cyber Exploit

NOTE:
* The information is written and maintained by CVE MITRE.
The data on this page reflects neither the opinions of Secunia or the results of our research.

Back

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 40,000 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*

- *For more details about the Threat Intelligence Modules, see our datasheet: https://www.flexera.com/media/pdfs/datasheet-svm-threat-intelligence-module.pdf*

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

Rule	Severity	Value
Recently Linked to Remote Access Trojan	Medium	+2
Historically Linked to Remote Access Trojan	Low	+1
Recently Linked to Ransomware	Medium	+2
Historically Linked to Ransomware	Low	+1
Recently Linked to Penetration Testing Tools	Medium	+2
Historically Linked to Penetration Testing Tools	Low	+1
Recently Linked to Malware	Medium	+2
Historically Linked to Malware	Low	+1
Recently Linked to Exploit Kit	Medium	+2

Table A-1 • Rules, Severity and Value

Rule	Severity	Value
Historically Linked to Exploit Kit	Low	+1
Linked to Recent Cyber Exploit	Low	+1
Linked to Historical Cyber Exploit	Low	+1
Recently exploited in the wild	Very Critical	+5
Exploited in the wild in the past year	Critical	+4
Historically exploited in the wild	High	+3
Recent remote code execution POC verified	Critical	+4
Recent POC verified	High	+3
Historical remote code execution POC verified	Medium	+2
Recent possible POC	Medium	+2
Historical POC verified	Low	+1
Tools to exploit the vulnerability developed recently	Medium	+2
Tools to exploit the vulnerability developed historically	Low	+1
Recently verified intelligence	High	+3
Historically Verified intelligence	Low	+1

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

Criticality	From	To
Very Critical	71	99
Critical	45	70
High	24	44
Medium	13	23
Low	1	12

Table A-2 • Criticality - Ranges

Criticality	From	To
None	0	0

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.

Item	Value
Base Score	+45
Recent remote code execution POC verified	+4
Linked to Recent Cyber Exploit	+1
Historically Linked to Remote Access Trojan	+1
Threat Score (Sum of above values)	**51**

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 medium. This sets the score's maximum and minimum range as between 13 and 23.

Item	Value
Base Score	+13
Recently Linked to Malware	+2 * 7 CVE = +14
Threat Score (Sum of above values)	**27** ***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.

Item	Value
Base Score	+24

Item	Value
Historically exploited in the wild	+3
Threat Score (Sum of above values)	**27**

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 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

Software Vulnerability Manager	Software Vulnerability Research
• Offers a Threat Score at the Advisory level	• Offers a Threat Score at the Advisory level • Offers a Threat Score at the vulnerability level, within the advisory • Offers a list of which rules were triggered to arrive at the Threat Score displayed

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

B

Appendix B - Assessment & Patching

Important • *The Assessment & Patching module is not available for Software Vulnerability Research.*

This appendix explains where software vulnerabilities are installed across your organization by device and product. A list of advisories is also provided to address software vulnerabilities. The following topics are discussed in this section:

- Assessment Scenarios
- Assessment Reports
- Patching

Assessment Scenarios

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 macOS
- 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.

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

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

Requirement	Description
Permissions	Administrative privileges to download and install Software Vulnerability Research's Vulnerable Software Discovery Tool files `SVMScanInstall.msi` and `SVMScan.exe` from: https://app.flexerasoftware.com/
Access	Access to: https://agent.app.flexerasoftware.com
Operating systems	• Microsoft Windows Server 2012 R2 or Later • Microsoft Windows Operating System: Windows 10, Windows 11
Internet Connection	SSL 443/TCP to https://app.flexerasoftware.com/
Update agent	Windows Update Agent 2.0 or later
Port	Port 443 (standard HTTPS) to access the cloud

Agent-Based Scan – Requirements for macOS

The following requirements should be met before installing the Software Vulnerability Research's Vulnerable Software Discovery Tool for Mac on an Intel-based macOS machine:

Table B-2 •

Requirement	Description
Operating System	Supported operating systems: ● 10.8 Mountain Lion ● 10.9 Mavericks ● 10.10 Yosemite ● 10.11 El Capitan ● 10.12 Sierra ● 10.13 High Sierra ● 10.14 Mojave ● 10.15 Catalina ● 11 Big Sur ● 12 macOS Monterey ● 13 macOS Ventura ● 14 macOS Sonoma ● 15 macOS Sequoia
Permissions	● Administrator at minimum ("root" privileges required for the installation) ● The user installing the Agent must have 'execute' permissions on the file (chmod +x)
Internet Connection	SSL 443/TCP to https://app.flexerasoftware.com/.

To scan Apple macOS 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 macOS 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 macOS, see:

- Prepare Your Mac
- Install the Vulnerable Software Discovery Tool for Mac

Prepare Your Mac

Installation of daemons (services) on macOS 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.

```
bash-3.2$ su root
Password:
```

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 macOS 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 3048
-rw-r--r--@ 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.

```
chmod +x svmscan_macos
```

```
sh-3.2# chmod +x svmscan_macos
sh-3.2# ls -l
total 3048
-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:

Task ***To install the Vulnerable Software Discovery Tool for Mac:***

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

   ```
   sh-3.2# ./svmscan_macos -i
   [10/25 12:37:27.421] Initializing Flexera Software Vulnerable Software Discovery
    Tool 8.0.0.344
   [10/25 12:37:27.453] GUID : 41713AB6-9437-4B8D-A1E6-5CA8D9883AC1
   [10/25 12:37:27.493] 'Flexera SVM Scanner' service started
   [10/25 12:37:27.493] 'Vulnerable Software Discovery Tool' successfully installed
   [10/25 12:37:27.493] Vulnerable Software Discovery Tool 8.0.0.344 shutting down
   ```

   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:

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.

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.

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 "`dnsdomainname`" 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.

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 to Run as <user> with <password>
- Install But Without Writing Anything to the Registry

Install as Current 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 B-3 • Agent Configuration Options

Category	Configuration Option	Description
Program Options	`-A/--network-appliance`	Run in Network Appliance mode.

	`-c/--cli`	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`

	`-d <path>  --debug <path>`	Write diagnostic information to the specified file.
	`--getfileinfo <path>`	Directory for output file
	`-h/--help`	Display this message and exit.
	`-n/--checkin-interval <interval>`	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
	`-o/--outdir <path>`	Directory for output file
	`-oc/--output-csv <file>`	Output inspection results to a CSV file.
	`-ox/--output-xml <file>`	Output inspection results to an XML file.
	`-si/--scantime_interval <minutes>`	Set a random range to delay running software inspection. 0 means no random range, or 1-60 minutes.
	`--skip-wait/--skipwait`	Skip the initial 10 minute wait before the first check in.
	`-v  --verbose`	Display or log additional diagnostic information.
	`-V/--version`	Display program version information and exit. Use this option when you want to check the version of the agent.

Table B-3 • Agent Configuration Options (cont.)

Category	Configuration Option	Description
Customer Area Option	`-g/--group <group>`	Create host as a member of <group> in your Software Vulnerability Research Account (defaults to domain or langroup if unspecified).
Mac Agent Option	`--delete-all-settings`	Deletes all information, including Globally Unique Identifiers (GUID), from the system to ensure it is clean to accommodate a new installation.

Table B-3 • Agent Configuration Options (cont.)

Category	Configuration Option	Description
Network Settings	`-D --direct-connection`	Bypass proxy, use direct connection.
	`--forcehttps`	Force HTTPS, regardless of port. When this option is not specified, we default HTTPS on port 443 and HTTP on other ports. This option is for debugging purposes.
	`--ignore-ca`	Ignore unknown certificate authority.
	`--ignore-cn`	Ignore invalid Common Name in cert.
	`--ignore-crl`	Ignore Certificate Revocation list.
	`--pac-url <url>`	Proxy Autoconfig url
	`--request-timeout <minutes>`	Sets a timeout on network connections. Set for 1-10 minutes or use 0 for no timeout. 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.
	`-U <user:pass> --proxy-user <user:pass>`	Set proxy credentials (saved in encrypted form).
	`--use-network-winhttp`	Enable WinHttp network stack. 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.
	`--use-network-wininet`	Enable WinInet network stack (default). 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.
	`-x <proxy:port> --proxy <proxy:port>`	Set proxy.

Table B-3 • Agent Configuration Options (cont.)

Category	Configuration Option	Description
Proxy Options	`-D/--direct-connection`	Force direct connection, overriding default internet proxy settings.
	`--pac-url <URL>`	Specify the URL of the Proxy Auto Configuration file (.pac/.dat).
	`-U/--proxy-user <user[:pass]>`	Specify Proxy authentication.
	`-x/--proxy <host[:port]>`	Use HTTP proxy on given port.
Scan Options	`--check-wmi`	Use WMI to get Windows updates. Use this option to query Windows updates on SCCM using WMI in addition to a query using Windows Update Agent. This option could be used to see if the SCCM client on the device/host can be used for reporting missing KBs.
	`-t/--type`	Software scan type: • **Minimal Scan**—Scan Type 1: Inspect applications in default locations only. • **Optimal Scan**—Scan Type 2: Inspect applications in non-default locations. • **Full Scan**—Scan Type 3: Inspect all .dll, .exe, and .ocx files. For details, see Scan Types.
	`-w/--no-os-update/--no-win-update`	Do not connect to Windows Update.
	`--wua-proxy <0,1 or host[:port]>`	Configure proxy settings for Windows Update. • 0: Use the default setting. • 1: Use the proxy configured with `-x/--proxy`. • `<host[:port]>` Manually set the proxy host and port.

Table B-3 • Agent Configuration Options (cont.)

Category	Configuration Option	Description
Scan Settings that Server Can Override	`-g <group> --group <group>`	Group name for association
	`-n <minutes>M --checkin-interval <minutes>M` `-n <hours>H --checkin-interval <hours>H`	Set Check-in interval.
	`-w --no-win-update --no-os-update`	Disable windows update check.
Security Options	`--ignore-ca`	Ignore Unknown SSL Certificate Authority (CA).
	`--ignore-crl`	Ignore SSL Certificate Revocation Check.
	`--ignore-cn`	Ignore Invalid SSL Certificate Common Name (CN).
Server Options	`--userid <userid>`	Set the Software Vulnerability Research access user ID.
	`--token <token>`	Set the Software Vulnerability Research access token.
	`--host <hostname>`	Set the Server hostname.
	`--port <port>`	Set the Server port.

Table B-3 • Agent Configuration Options (cont.)

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

Table B-3 • Agent Configuration Options (cont.)

Category	Configuration Option	Description
Service Recovery Settings:	`--service-failure-actions <actions>`	Failure actions and their delay time (in milliseconds), separated by / (forward slash) – e.g., run/5000/reboot/800. Valid actions are <run|restart|reboot>. (Must be used in conjunction with the --service-failure-reset option)
	`--service-failure-command <command line>`	Command line to be run on failure.
	`--service-failure-flag`	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.
	`--service-failure-reboot <message>`	Message broadcast before rebooting on failure.
	`--service-failure-reset <period>`	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)

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.

Scan Types

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

Table B-4 • Scan Types

Scan Type	Folders Searched	File Name Match	Applications Detected
Minimal Scan - Scan Type 1	Default folders only Example: Program Files	File names are matched first; then metadata is matched. Example: `c:\Program Files\Mozilla Firefox\Firefox.exe`	Known applications in predefined locations on a device
Optimal Scan - Scan Type 2	All files and folders	File names are matched first; then metadata is matched. Example: `c:\Custom Mozilla Firefox Folder\Firefox.exe`	Known applications in any location (“portable applications”) on a device
Full Scan - Scan Type 3	All files and folders	Metadata only Example: `c:\Custom Mozilla Firefox Folder\myFirefox.exe`	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

Assessment Reports

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

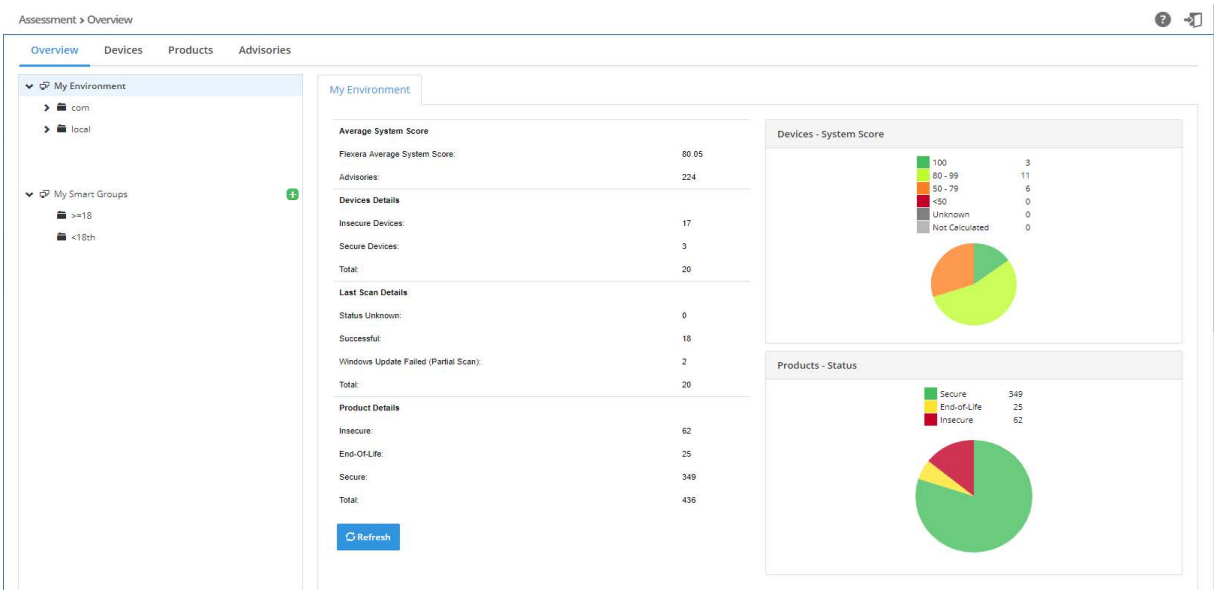
Overview

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.*



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

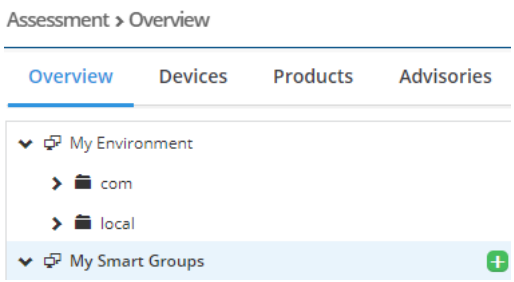
- **All types of conditions**—Select the devices; then select devices with the product conditions and eliminate devices or products that do not have the advisory conditions. This selection order ensures that a group with the conditions "Windows platform, Python product installed, Highly and extremely 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.
- **Product secure type**—Is context dependent on the list of devices; a product can be insecure on one device and secure on other devices (Example: Windows may be insecure depending on the KBs installed on the device). For example, if you create a Smart Group "Devices from AD group "NorthAmerica" and insecure products", you might not get "Windows 8" as insecure in your Smart Group list, although you see it as insecure in the full product list, since Windows 8 is secure on all devices in your Active Directory (AD).

Create a Smart Group

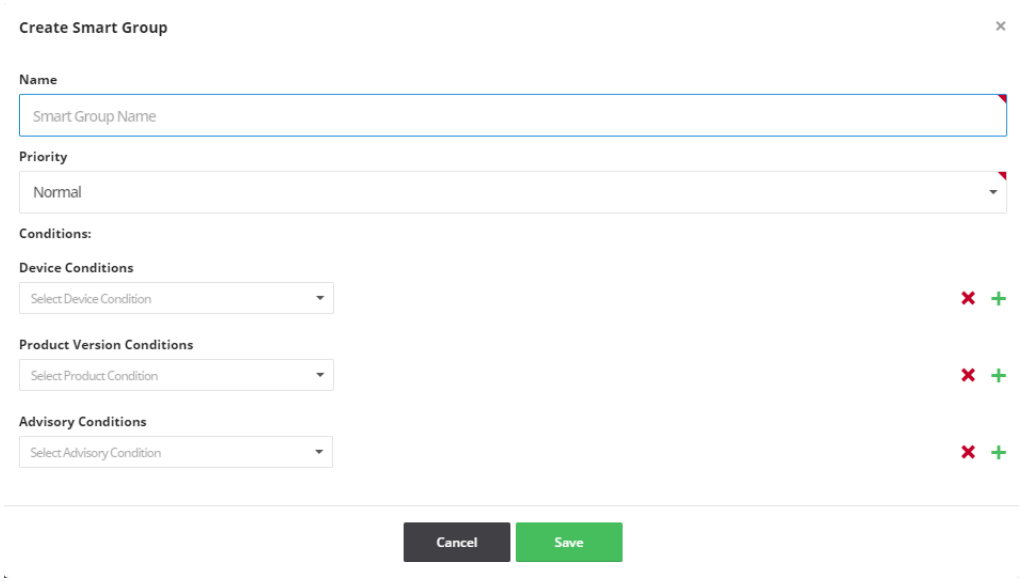
To create a Smart Group, perform the following steps.

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.

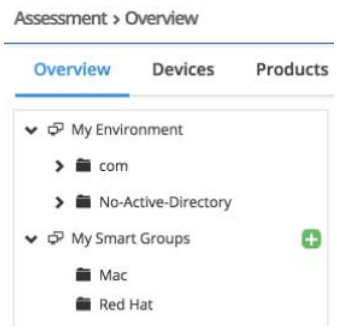
Note • *Device Platform is limited to Windows, macOS, and RedHat Enterprise Linux. If you want to select a particular operating system (Example: Windows 8), Select Windows as the Device Platform, add Device Condition "Operating System In", click "Select Operating System(s)", enter Windows 8 in the search 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 CVSS4 value if the advisory has CVSS4 data. Otherwise, the condition is applied to the CVSS3 or CVSS2 score respectively.*

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.

Task ***To create a Smart Groups report under Analytics > Reports:***

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

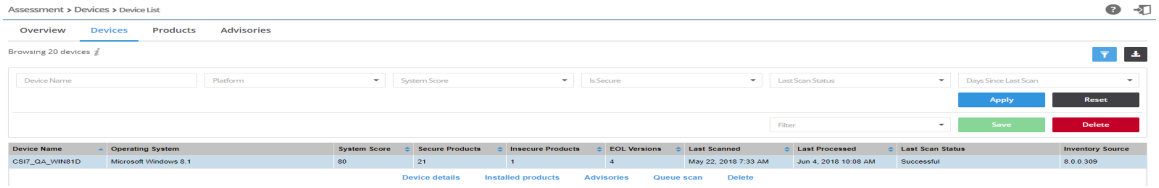
***Note** • For recurring reports based on a Smart Group, the Smart Group contents are recalculated, based on the conditions before the report is sent out, to reflect the latest data for your selection.*

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.

The **Last Processed** column refers to the last time LiveUpdate identified any new advisories that have come in since you last scanned your system.



Task ***To view devices:***

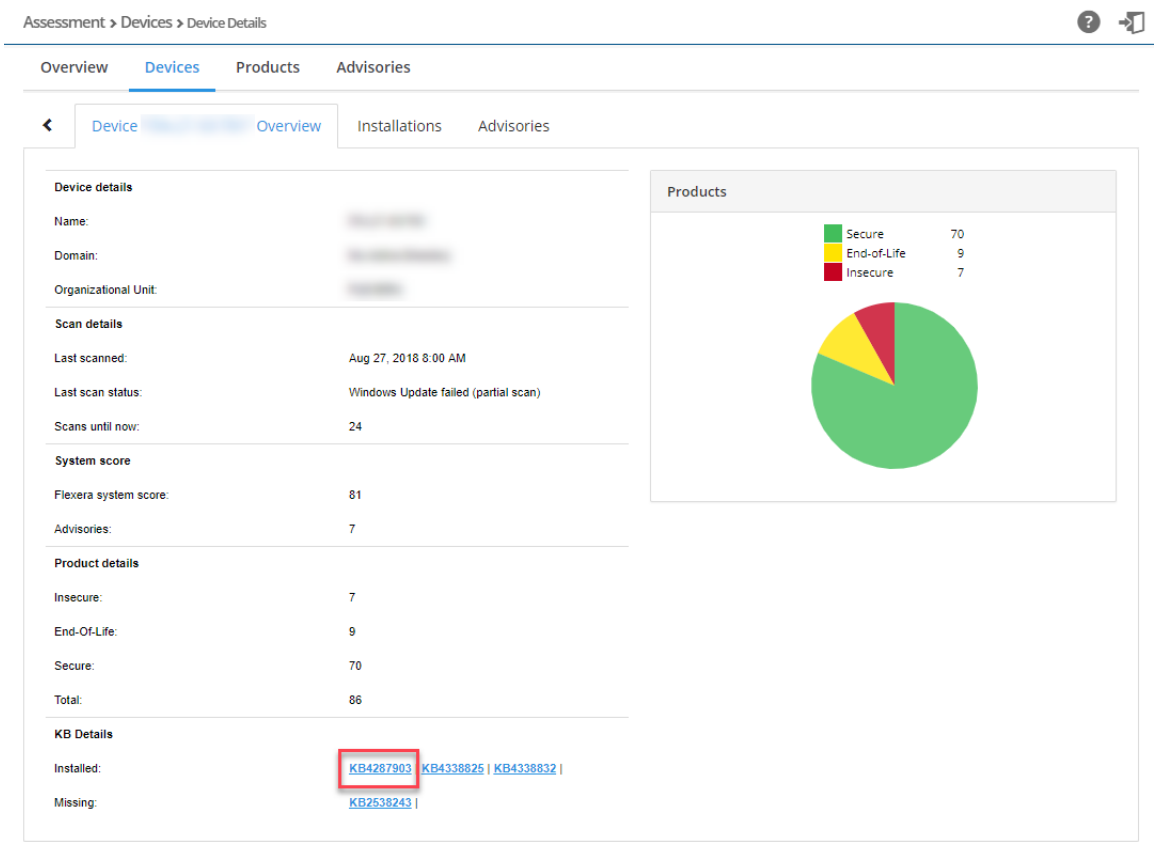
1. Open the **Assessment > Devices > Device List** page.
2. Click and select from the drop-down lists to filter the Devices by **Device Name**, **Platform** (Windows, macOS, or RedHat Enterprise Linux), **System score** (100, 80-89, 50-79, <50, Unknown, or Not Calculated), **Is secure** (Yes or No), 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.

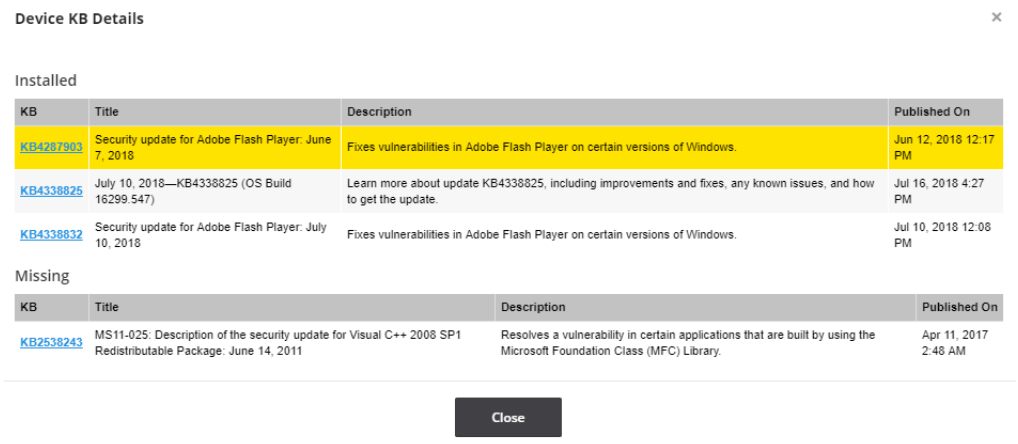
Device Details

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

Task ***To view device details:***

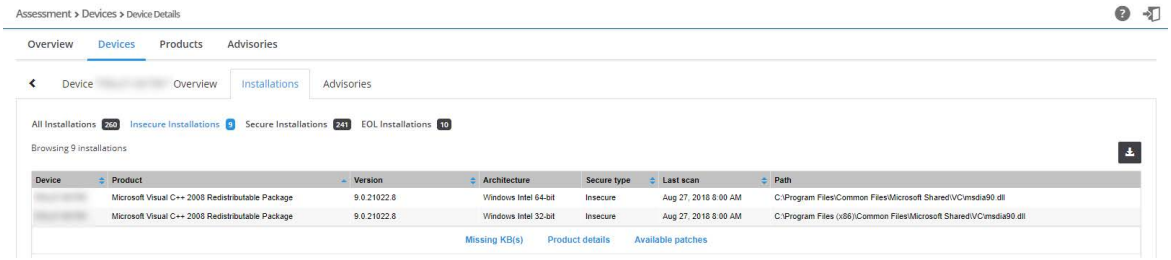
1. In the **Overview** tab, click an Installed or Missing **KB Details** link to view detailed KB information. The selected KB Details will be highlighted.



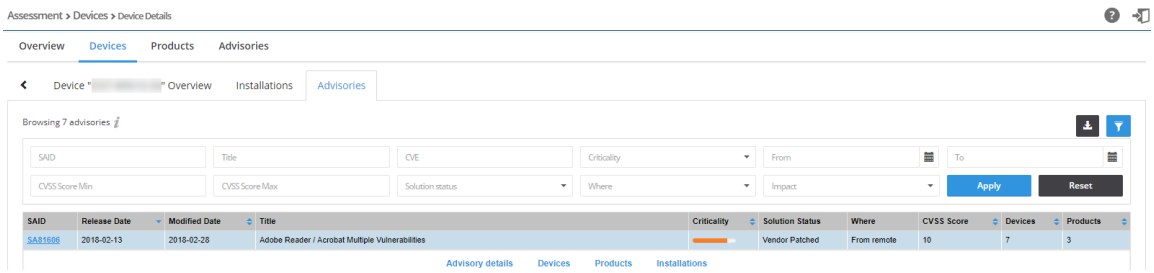


2. Click in the **Installations** and **Advisories** tabs to export the results to a CSV file.

3. In the **Installations** tab, click a Device in the grid to can find further information regarding the device's **Missing KB(s)** for insecure Microsoft products, **Product details**, and **Available Patches**.

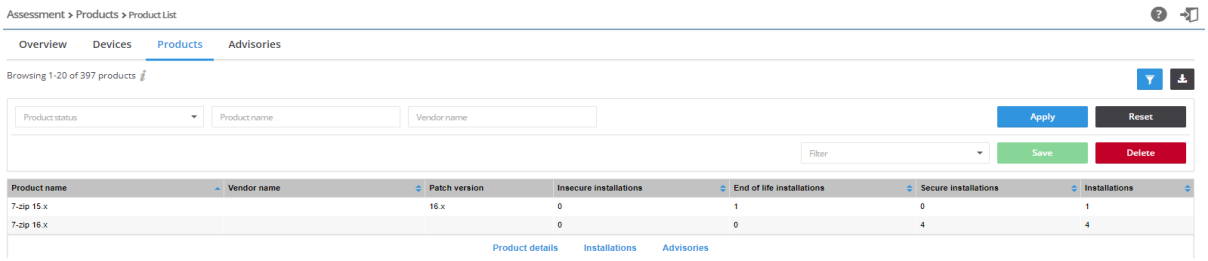


4. In the **Advisories** tab, click an SAID in the grid to view detailed information regarding the Advisory.



Products

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



Task ***To view products:***

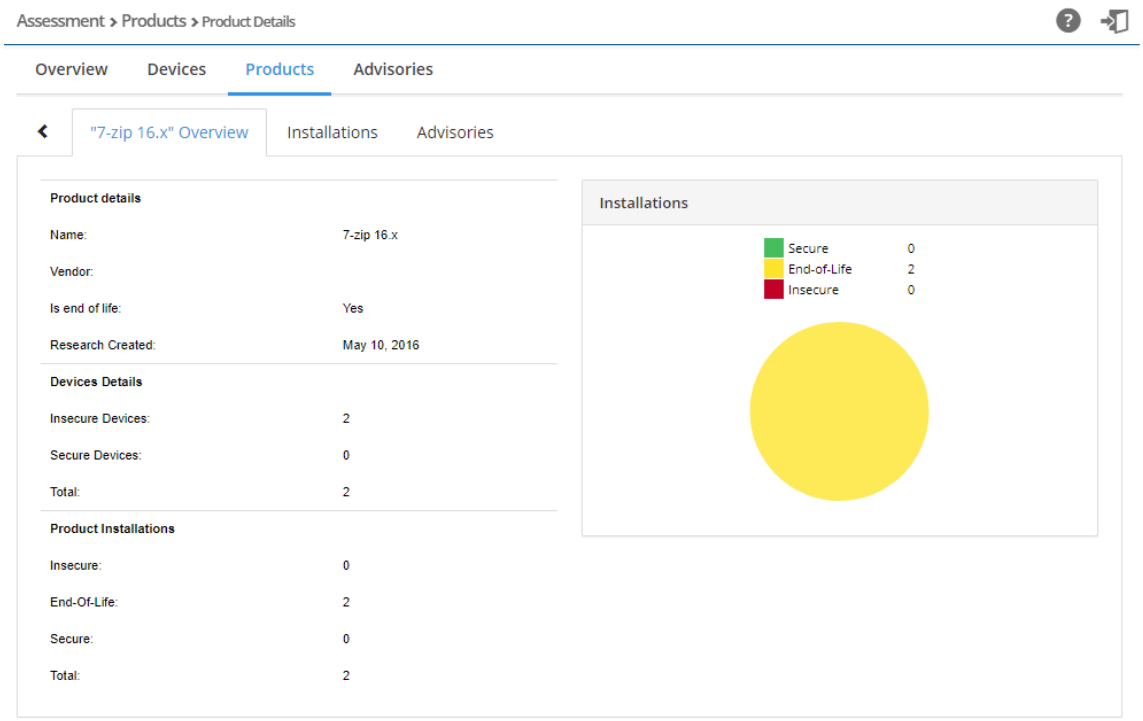
1. Open the **Assessment > Products > Product List** page.
2. Click and select from the drop-down lists to filter the Products by **Product Status** (Secure, Insecure, or EOL), Product name, and Vendor Name.
3. Click the **Apply** or **Reset** buttons to apply or reset the filters.
4. Click the **Save** 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.

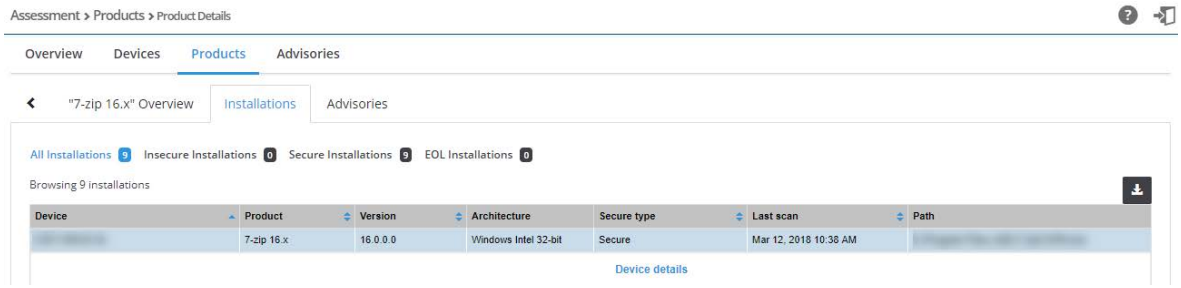
Product Details

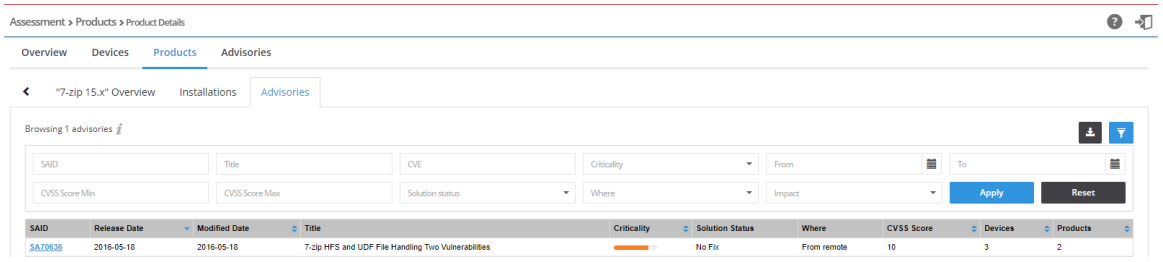
The **Product Details** page displays **Overview**, **Installations** and **Advisories** details for the selected Product.

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.





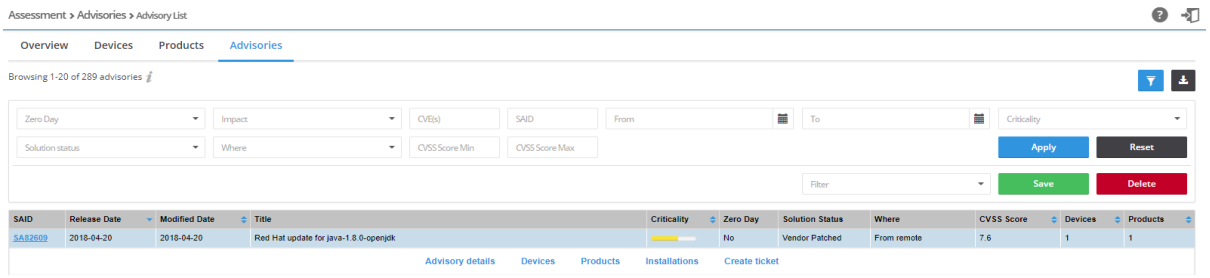


Advisories

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**.

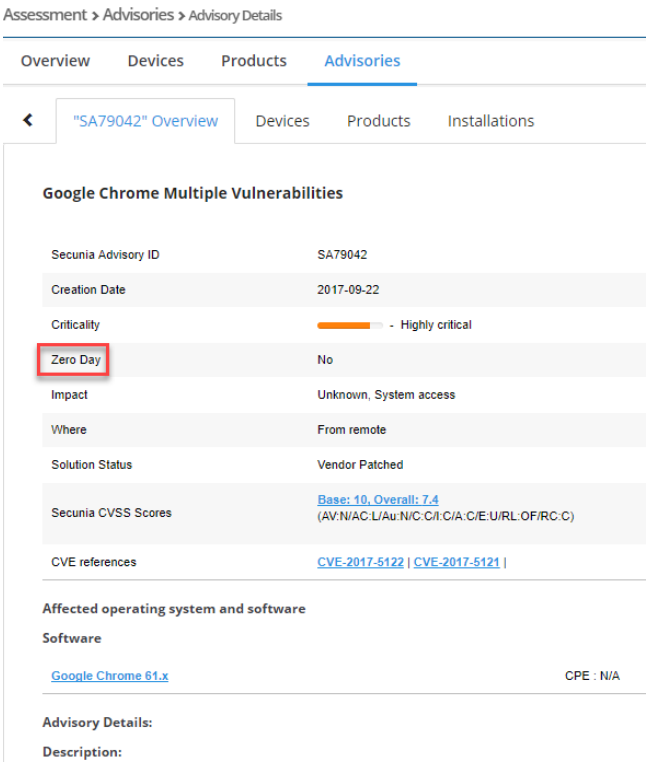
   Note • *To search for multiple advisories at the same time to determine which advisories apply to more than a single CVE for which you have interest, enter the CVEs in the **CVE(s)** filter and leave one space between entries (Example: CVE-2014-0224 CVE-2014-0160 CVE-2013-0169 CVE-2009-3555 CVE-2015-7575).*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

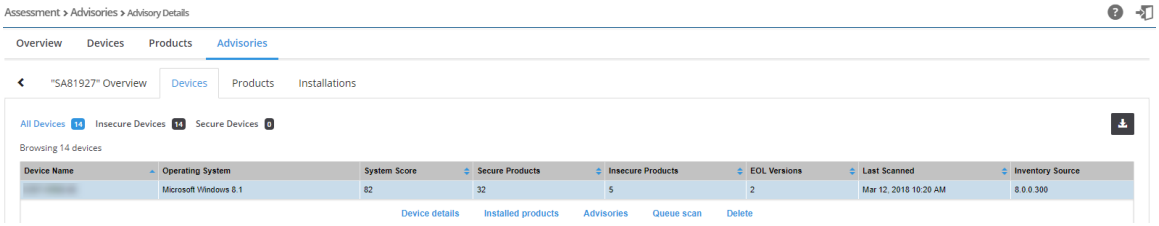
Advisory Details

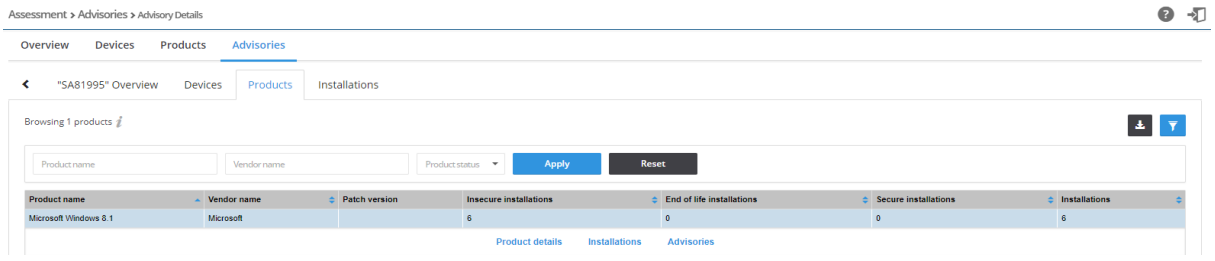
The **Advisory Details** page displays **Overview**, **Devices**, **Products** and **Installations** details for the selected Advisory.

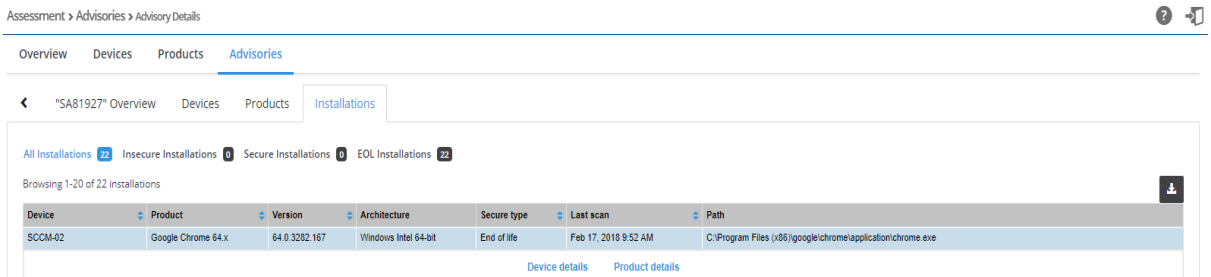
Click in the **Devices**, **Products** and **Installations** tabs to export the results to a CSV file.

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.


Assessment > Advisories > Advisory Details
Overview
Devices
Products
Advisories
"SA79042" Overview
Devices
Products
Installations
Google Chrome Multiple Vulnerabilities
Secunia Advisory ID
SA79042
Creation Date
2017-09-22
Criticality
- Highly critical
Zero Day
No
Impact
Unknown, System access
Where
From remote
Solution Status
Vendor Patched
Secunia CVSS Scores
Base: 10, Overall: 7.4
(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C)
CVE references
CVE-2017-5122 | CVE-2017-5121 |
Affected operating system and software
Software
Google Chrome 61.x
CPE : N/A
Advisory Details:
Description:


Assessment > Advisories > Advisory Details
Overview
Devices
Products
Advisories
"SA81927" Overview
Devices
Products
Installations
All Devices 14
Insecure Devices 14
Secure Devices 0
Browsing 14 devices
Device Name
Operating System
System Score
Secure Products
Insecure Products
EOL Versions
Last Scanned
Inventory Source
Microsoft Windows 8.1
82
32
5
2
Mar 12, 2018 10:20 AM
8.0.0.300
Device details
Installed products
Advisories
Queue scan
Delete


Assessment > Advisories > Advisory Details
Overview
Devices
Products
Advisories
"SA81995" Overview
Devices
Products
Installations
Browsing 1 products
Product name
Vendor name
Product status
Apply
Reset
Product name
Vendor name
Patch version
Insecure installations
End of life installations
Secure installations
Installations
Microsoft Windows 8.1
Microsoft
6
0
0
6
Product details
Installations
Advisories

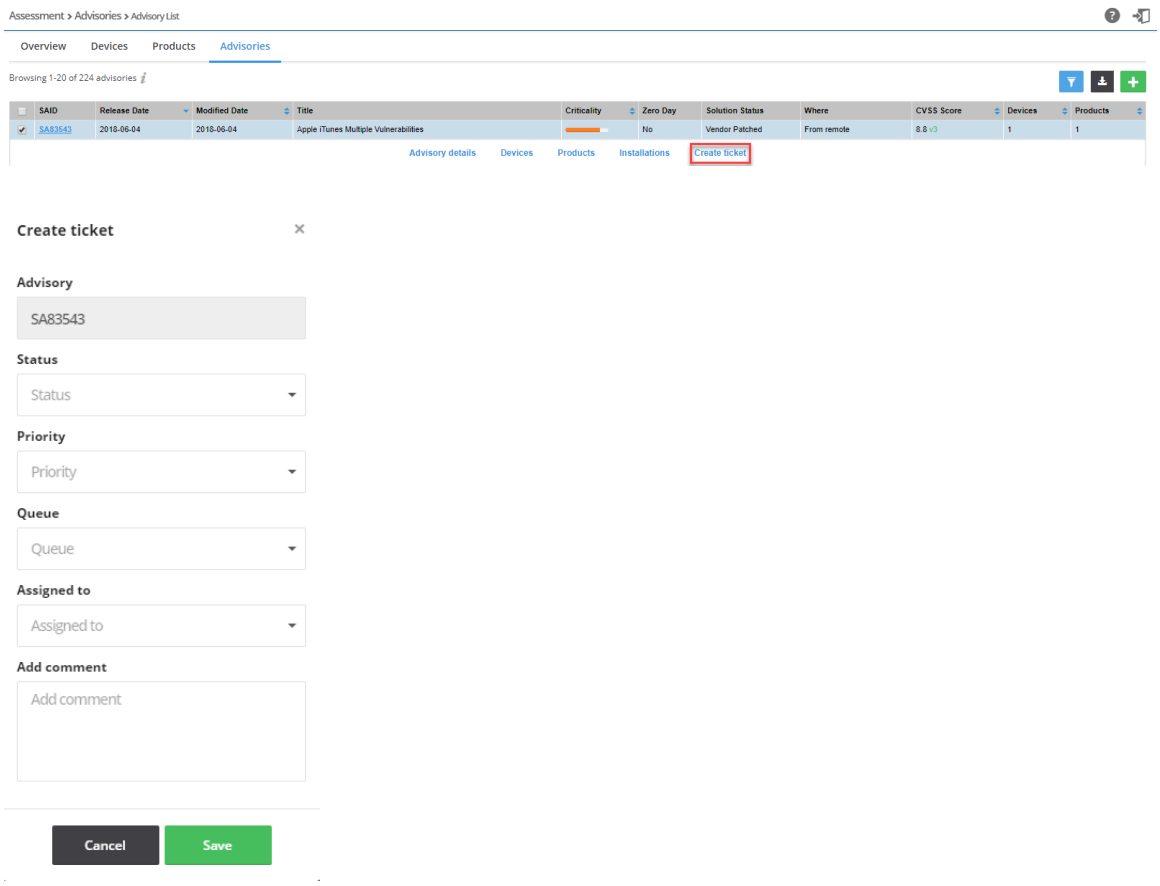

Assessment > Advisories > Advisory Details
Overview
Devices
Products
Advisories
"SA81927" Overview
Devices
Products
Installations
All Installations 22
Insecure Installations 0
Secure Installations 0
EOL Installations 22
Browsing 1-20 of 22 installations
Device
Product
Version
Architecture
Secure type
Last scan
Path
SCCM-02
Google Chrome 64.x
64.0.3282.167
Windows Intel 64-bit
End of life
Feb 17, 2018 9:52 AM
C:\Program Files (x86)\google\chrome\application\chrome.exe
Device details
Product details

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**.

Patching

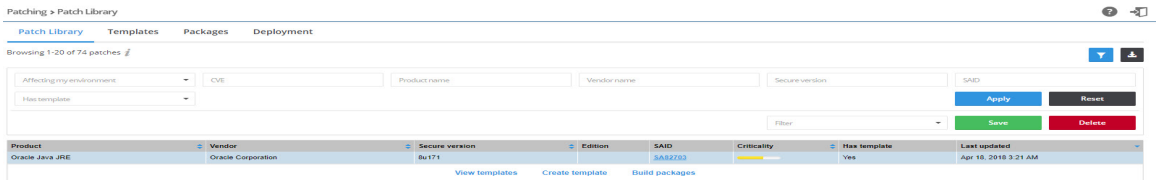
The patching feature in Software Vulnerability Research remediates software vulnerabilities in third-party applications. Software Vulnerability Research provides Patch and Grouped Patch Libraries that list all patches available for your environment, provides patch templates and build packages to deploy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

Patch Library

The **Patch Library** page displays details of all patches available for your environment.

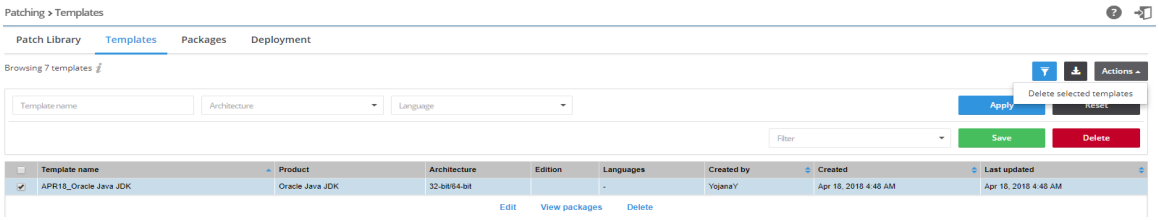


Task ***To view patches:***

1. Open the **Patching > Patch Library** page.
2. Click 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 to export the results to a CSV file.

Templates

The **T**emplates 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.

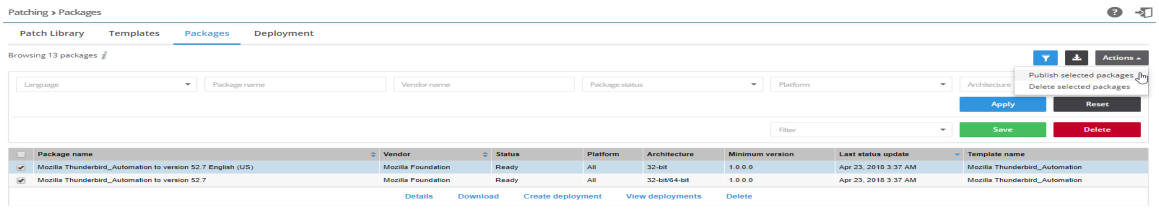


Task ***To view templates:***

1. Open the **Patching > Templates** page.
2. Click to filter the templates by Template Name, Architecture, or Language.
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 **Edit, View Packages,** or **Delete**.
6. To delete multiple templates, select the appropriate templates in the grid and click the **Actions** button.
7. Click 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:***

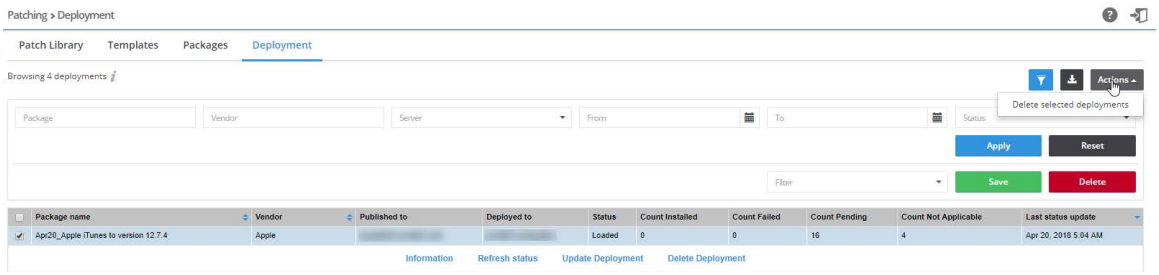
1. Open the **Patching > Packages** page.
2. Click to filter the packages by Language (select the required installation language or languages from the drop-down list), Package name, Vendor name, Package status (select Not ready, Building, Ready or Error building from the drop-down list), Platform (select 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 packages.*
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:***

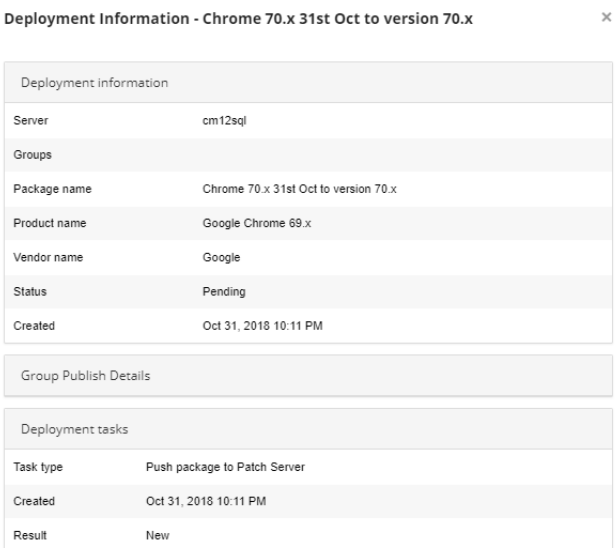
1. Open the **Patching > Deployment** page.
2. Click to filter the deployments by Package, Vendor, Server, From and To dates, and the **Status Options**:
   - Pending
   - Loaded
   - Completed

- 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.

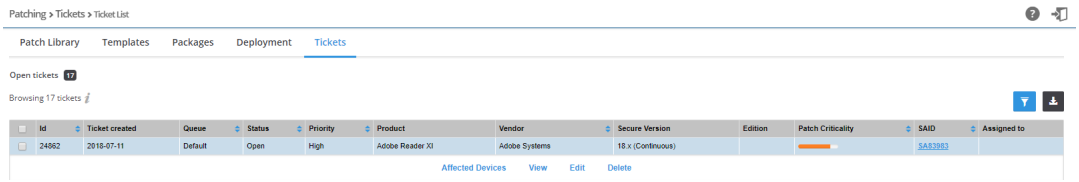


Update Deployment

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:***

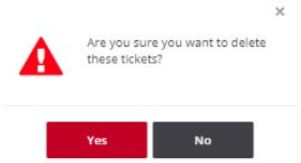
1. Open the **Patching > Tickets** page.
2. To filter the results by ticket status, select one of the bold ticket statuses in the upper-left-hand corner followed by a ticket count. The default ticket statuses are **Open**, **Waiting**, **Handled**, and **Irrelevant**. See Default Ticket Statuses in Ticket 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 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**.



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.

Task ***To enable manual signatures:***

1. Connect a daemon to your Software Vulnerability Research account by going to **Settings > Assessment > Update Servers & Daemon**.
2. Select a daemon.
3. Click the **More Info** action. In the pop-up, you will see a summary of the current state: the label **Digital signatures: Automatic** and the button **Sign packages manually**.
4. Toggle the **Sign packages manually** button to create the desired state: the label **Digital signatures: Manual** and the button **Sign packages automatically**.

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\SVM\SVMPD IO\Unsigned`
- Signed files (only useful if writable): `C:\ProgramData\Flexera Software\SVM\SVMPD IO\Signed`

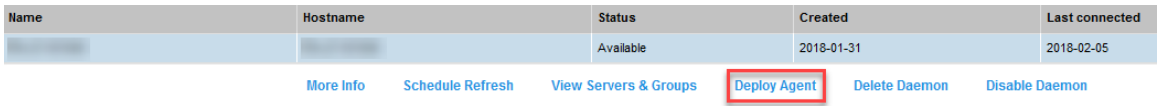
Note *• Altering or removing these shared folder names while a file is being signed will result in stale paths being shown in the Software Vulnerability Research user interface. Wait until no files are waiting for signatures before changing shared folder names.*

Deploy the Agent for a Manual Signature

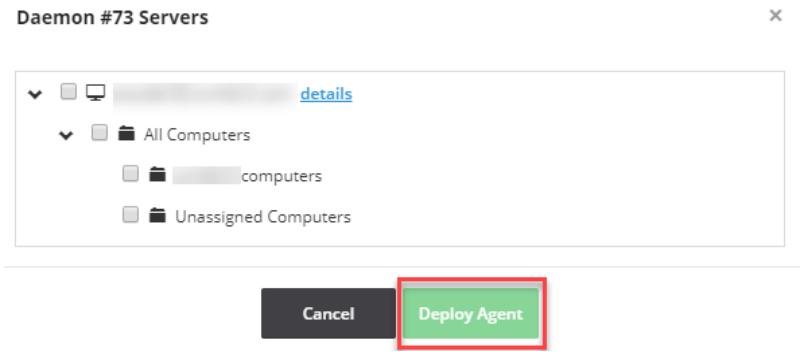
To deploy the Agent for a manual signature, perform the following steps.

Task ***To deploy the agent for a manual signature:***

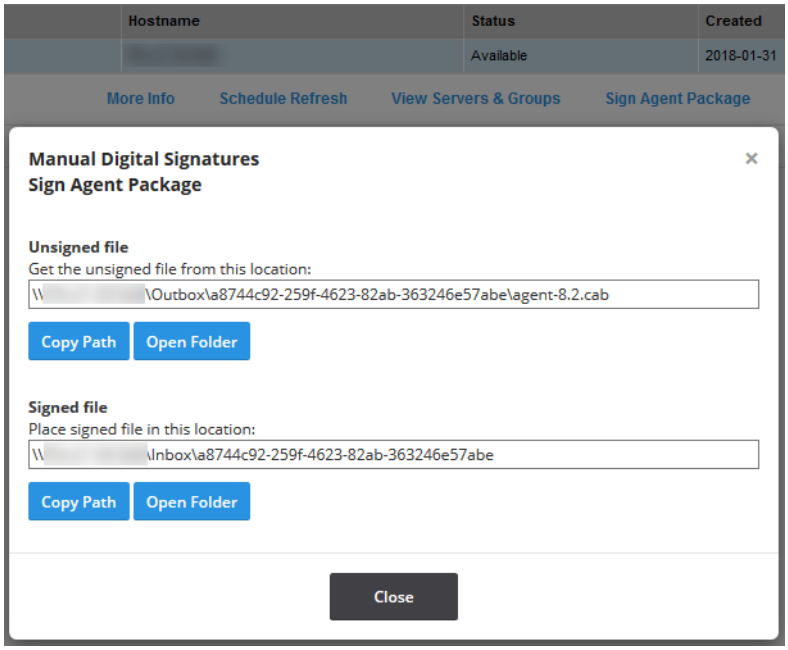
1. Click **Deploy Agent**.



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.



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.*

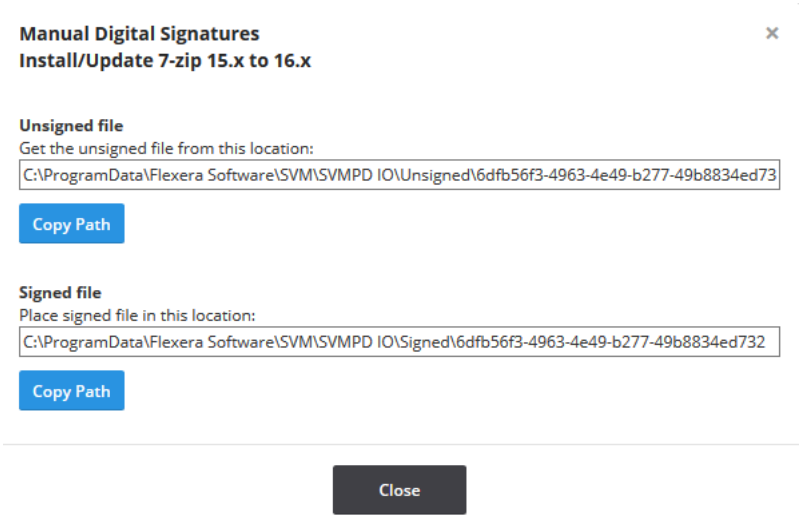
5. Copy the unsigned `.cab` file from the location mentioned under **Unsigned file** and invoke your organization's process for getting it signed. Once the `.cab` has been signed, copy the file into the folder mentioned under **Signed file.** The daemon will find the signed file, and, if the signature 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).



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.

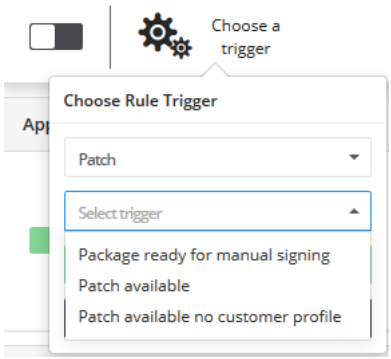
Note • *If multiple patch packages are all waiting for signature, it is safe to place signed* ***.cab*** *files in their respective signed paths in any order. The daemon will deploy the packages as they arrive.*

Manual Signature Notifications

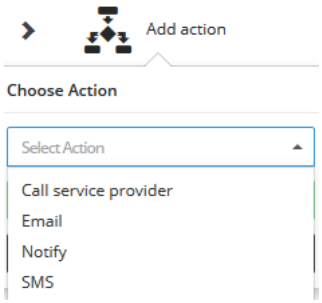
Typically, there is a pause between requesting to deploy an agent and the unsigned `.cab` file becoming available. To address this issue, you can notify the proper users that a `.cab` file is ready to be signed, where to get the `.cab` file and place it. To receive a notification, set up a rule in **Settings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

Appendix C - ThreatStream

This appendix explains step-by-step process to investigate vulnerabilities and associated threat models through advanced filtering and select capabilities:

- Analyzing Threat Models and Observables
- Viewing CVE Details and Associated Flexera Advisories

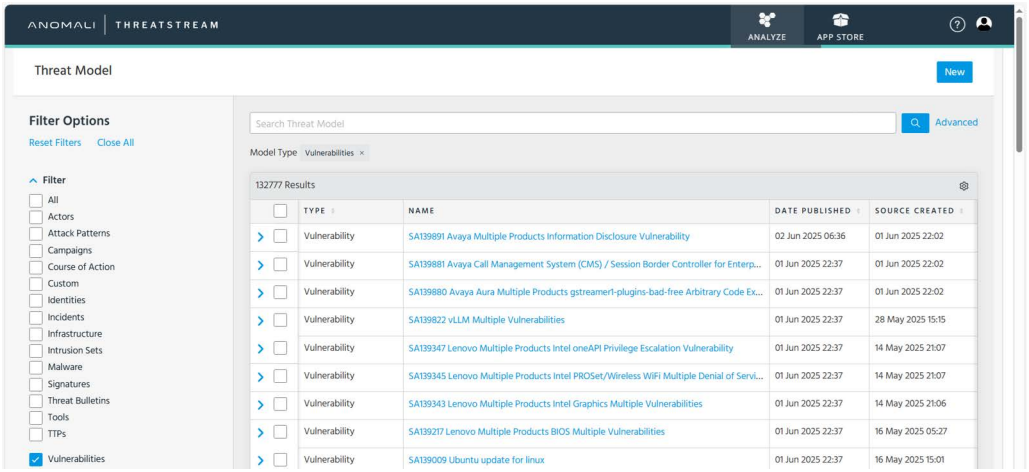
Analyzing Threat Models and Observables

This topic provides step-by-step process to investigate vulnerabilities and associated threat models through advanced filtering and select capabilities.

Task ***To search and analyze vulnerabilities using the Threat Model feature:***

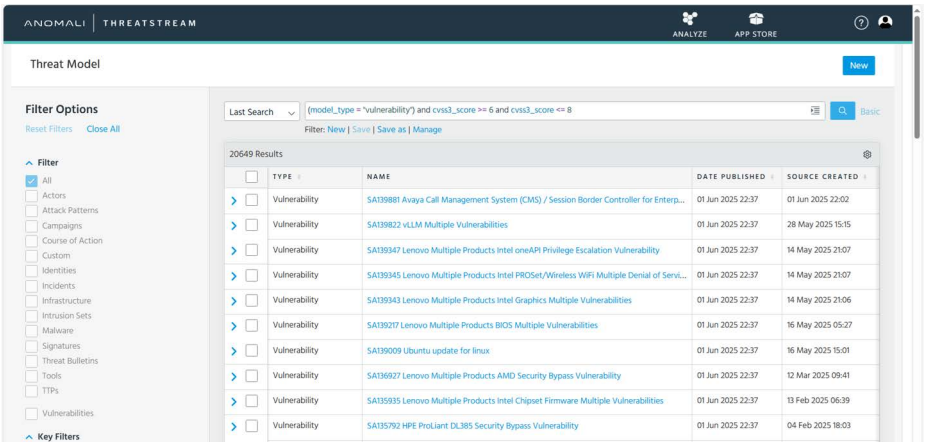
1. Login to **ThreatStream** using valid credentials.
2. On the home page, on top right click **Analyze > Threat Model**. The Threat Model page appears.

3. In the left navigation, under Filter Options, check the box for **Vulnerabilities**. Details of the selected Vulnerabilities will be appeared on the right pane.

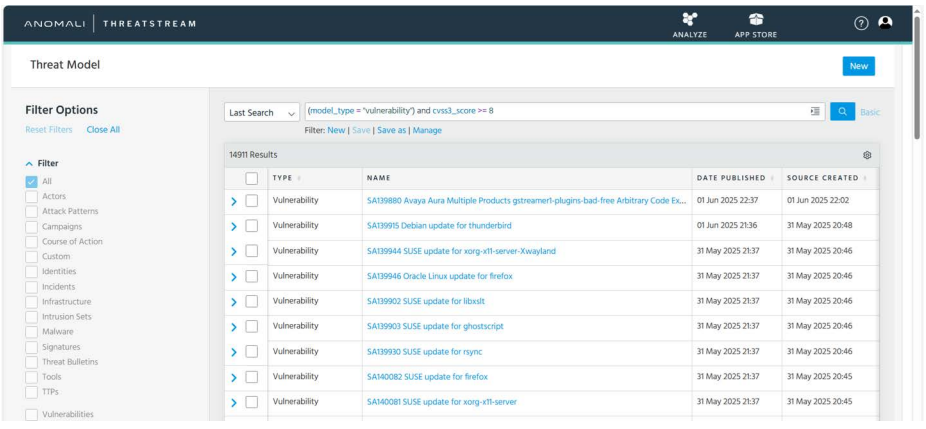


4. In the **Search Threat Model** search bar, search the query by:

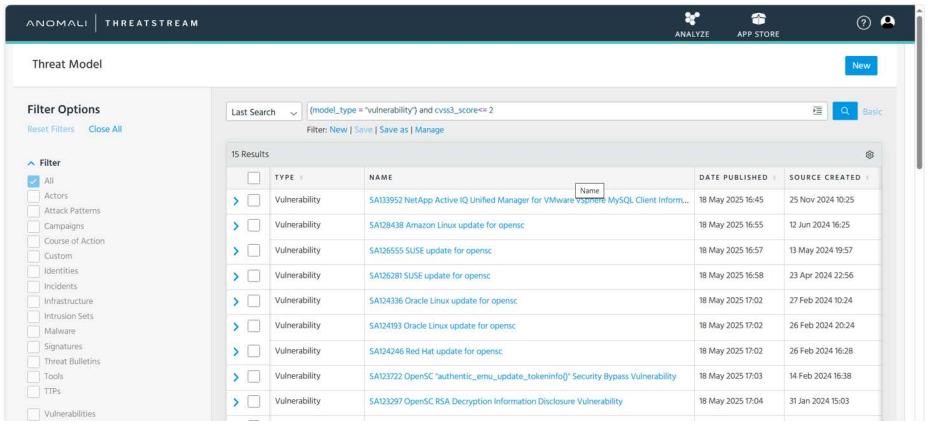
- Search by CVSS score between a value.



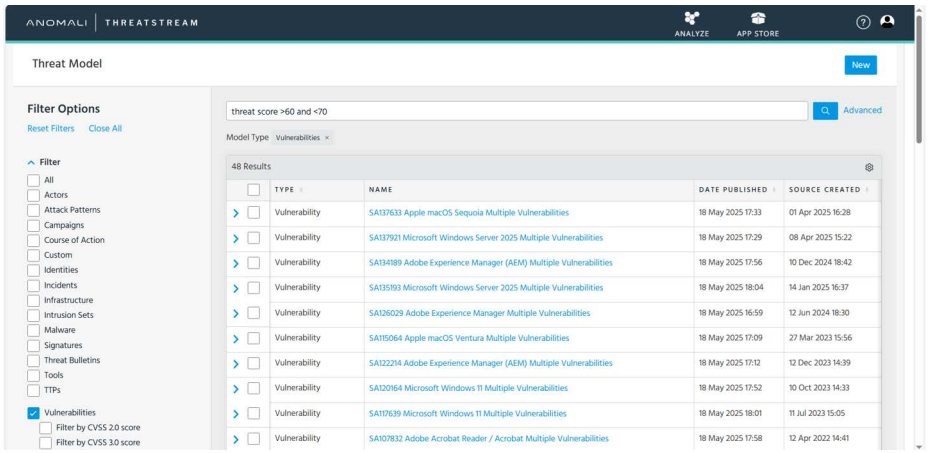
- Search by CVSS score greater than a value.



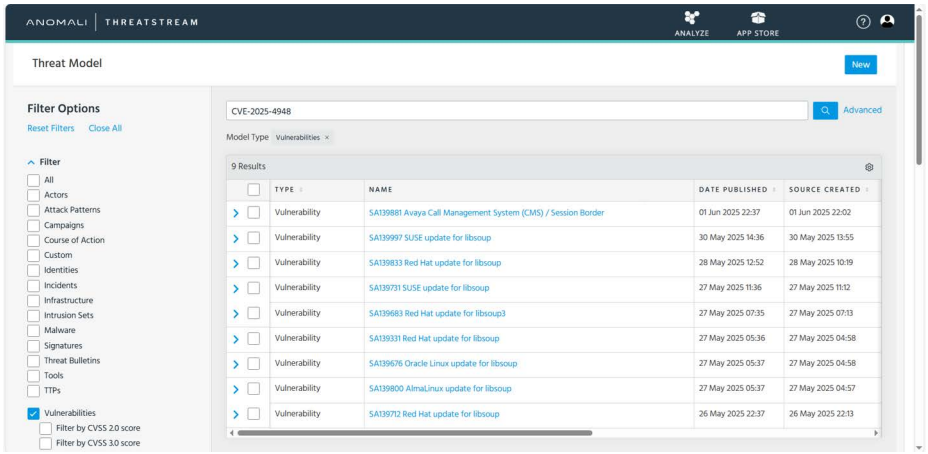
- Search by CVSS score less than a value.



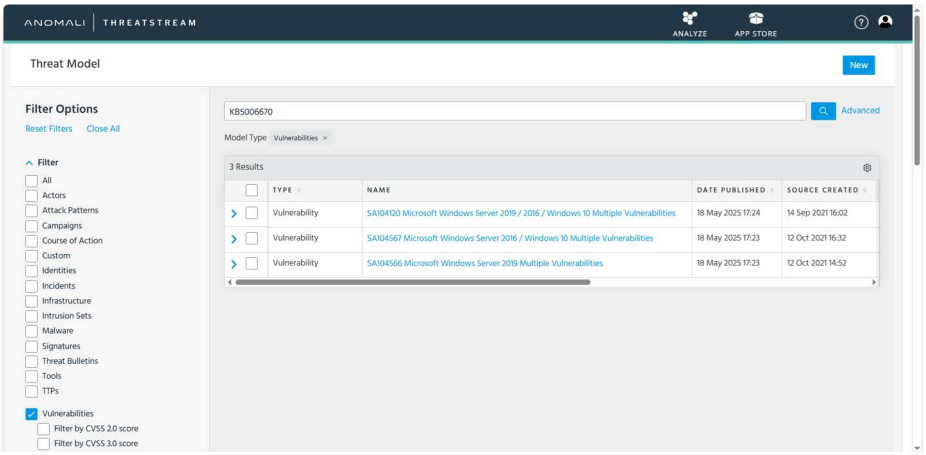
- Similar to above TI score - between, less, greater.



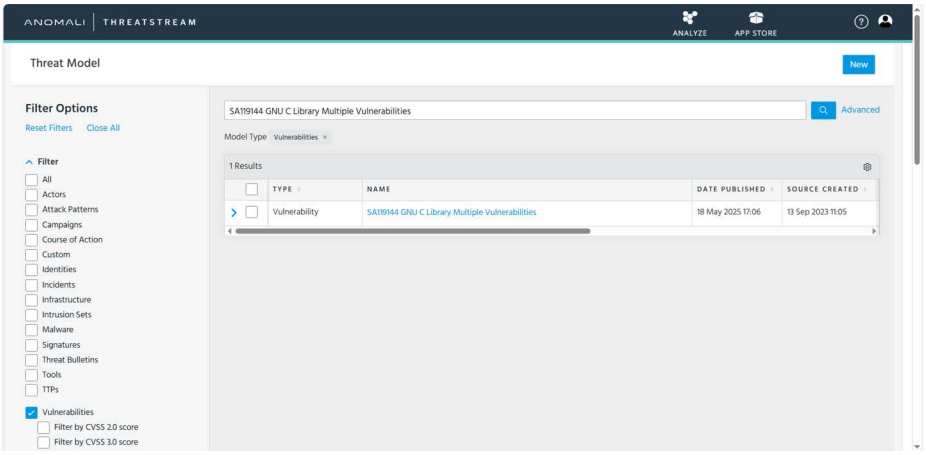
- Search by CVE.



- Search by KB Article.



- Search by any string.



Threat Model Search Queries Table:

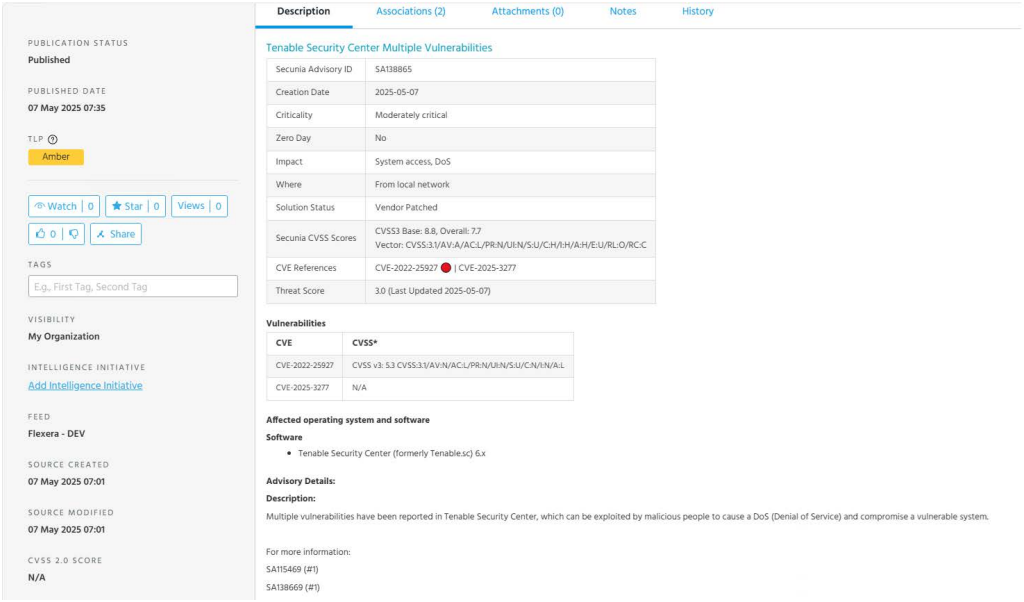
Search Type	Query Format
Search by CVSS score between a value	`(model_type=vulnerability) and cvss3_score >= 5 and cvss3_score <= 8`
Search by CVSS score greater than a value	`(model_type=vulnerability) and cvss3_score >= 8`
Search by CVSS score less than a value	`(model_type=vulnerability) and cvss3_score <= 2`

Search Type	Query Format

Similar to above TI score - between, less, greater	• TI Score Greater Than a Value
	`(body = threat) AND ( body = score) AND (body = >50) AND (model_type = "vulnerability")`
	• TI Score Less Than a Value
	`(body = threat) AND ( body = score) AND (body = <20) AND (model_type = "vulnerability")`
	• TI Score Between Two Values
	`(body = threat) AND ( body = score) AND (body = >50 ) AND (body = <70 ) AND (model_type = "vulnerability")`

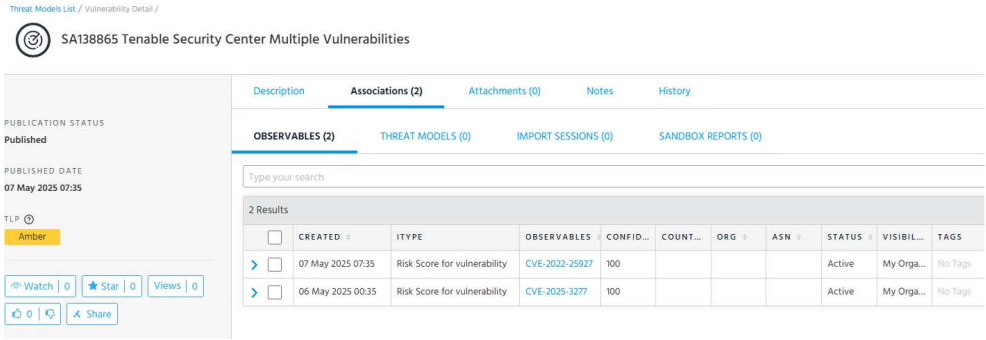
Search by CVE	`CVE-2025-4948`
Search by KB Article	`KB5006670`
Search by any string	`SA119144 GNU C Library Multiple Vulnerabilities`

5. Click on the desired listed vulnerability to open its detailed view. This provides information related to the selected vulnerability and associated Flexera Advisory.



6. To access more Details via SVR Application, Click the hyperlinked title within the detail view to open the SVR (Software Vulnerability Research) application for comprehensive data.

7. To see all associated observables (CVEs) linked to the selected Secunia advisory, click **Association > Observables**.

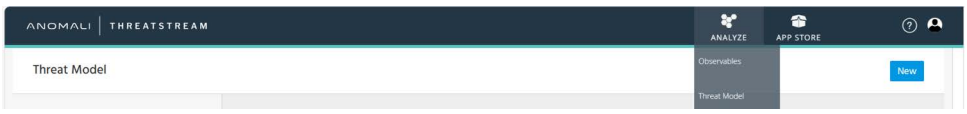


Viewing CVE Details and Associated Flexera Advisories

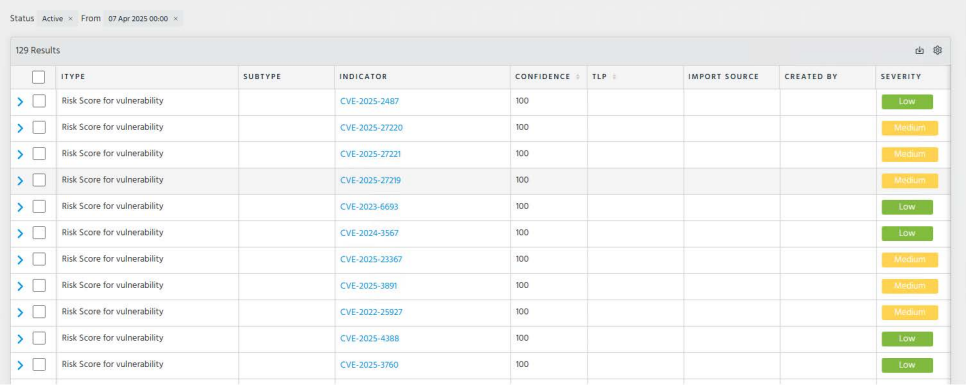
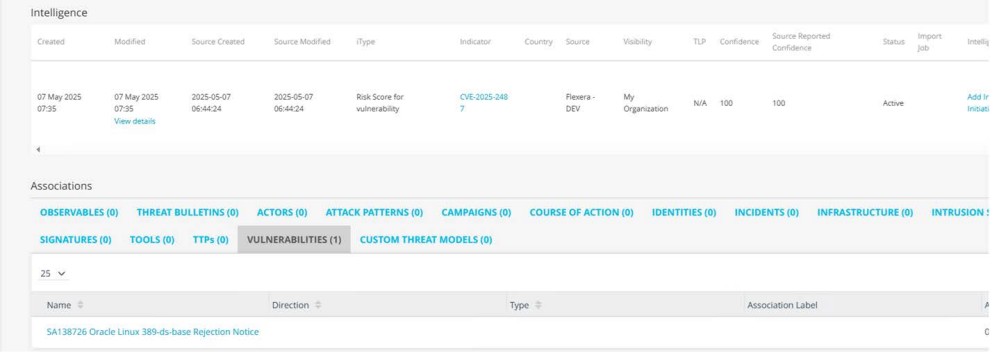
In this section you can view detailed information about CVEs and their associated Flexera advisories.

Task ***To view detailed information about CVEs and their associated Flexera advisories:***

1. Login to **ThreatStream** using valid credentials.
2. On the home page, on top right click **Analyze > Observables**. The Observables page appears.



3. You will see a list of CVEs displayed under Observables that are associated with Flexera advisories.



4. Click on any CVE to open its Details View. This view displays all associated Flexera Advisories related to the CVE, available under the **Vulnerabilities** tab.