Micro Focus
Fortify Software Security Center

Software Version: 23.1.0

User Guide

Document Release Date: Revision 1: June 2023
Software Release Date: May 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

This document was produced on June 09, 2023. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support/documentation

Contents

Preface

Contacting Fortify Customer Support

Visit the Support website to:

- Manage licenses and entitlements
- Create and manage technical assistance requests
- Browse documentation and knowledge articles
- Download software
- Explore the Community

https://www.microfocus.com/support

For More Information

For more information about Fortify software products:

https://www.microfocus.com/cyberres/application-security

About the Documentation Set

The Fortify Software documentation set contains installation, user, and deployment guides for all Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following Micro Focus Product Documentation website:

https://www.microfocus.com/support/documentation

To be notified of documentation updates between releases, subscribe to Fortify Product Announcements on the Micro Focus Community:

https://community.microfocus.com/cyberres/fortify/w/fortify-product-announcements

Fortify Product Feature Videos

You can find videos that highlight Fortify products and features on the Fortify Unplugged YouTube channel:

https://www.youtube.com/c/FortifyUnplugged

Change Log

The following table lists changes made to this document.

A document revision is published only if the changes made affect product functionality.

Software Release / Document Revision	Changes
23.1.0 Revision 1: June 2023	**Updated:** • In "Configuring Fortify Software Security Center for the First Time" on page 72, step 12 d was reformatted and a cautionary note was added. • The upgrade paths were corrected in"Upgrading Fortify Software Security Center" on page 195. • The address for the Fortify documentation team was corrected in the "Send Documentation Feedback" section.
23.1.0	Most references to Micro Focus were removed to reflect changed corporate ownership. **Added:** • "Adding a Fortify Insight Link to the Dashboard" on page 165 • "Setting the Required Password Strength for Fortify Software Security Center Login" on page 168 **Updated:** • Information about using secure cipher suites was added to "Securing Tomcat Server" on page 38. • The URL for a how-to video was changed in "Downloading Fortify Software Security Center Files" on page 50. • A cautionary note was added to "About Seeding the Fortify Software Security Center Database" on page 70. • An informational note was added to "Configuring Fortify Software Security Center for the First Time" on page 72.

Software Release / Document Revision	Changes
	• A note about cached LDAP user data was modified in "Configuring LDAP Servers" on page 111. • A description of the newly introduced flexible job execution strategy was added to "Configuring Job Scheduler Settings" on page 135. • A note indicating that logout responses and logout requests sent by IdP must be signed and a new step were added to "Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single Sign-On" on page 150. • Information about the ability to search the Subject Alternative Name (SAN) extension was added to "Configuring Fortify Software Security Center to Use X.509 Certification-based SSO" on page 159. • The procedure for changing the support contact link in the About box was modified in "Changing the Support Contact Link in the About Fortify Software Security Center Box" on page 166. • Troubleshooting information for handling failed LDAP user logins was added to "Handling Failed LDAP User Logins" on page 183. • The procedure for enabling Fortify Static Code Analyzer and Fortify Apps and Tools upgrades from Fortify Software Security Center was modified in "Enabling Fortify Static Code Analyzer and Fortify Apps and Tools Upgrades from Audit Workbench" on page 201 to reflect the separation of installation files with this release. • Descriptions of global events and application version events were added to "Creating Webhooks" on page 292. • Obsolete search query examples were removed from "Search Query Examples" on page 339. • A new section, "Viewing Priority Override Information in Issue Reports," was added to "Overriding Assigned Issue Priority" on page 353 to show how priority overrides are now represented in reports. The "Limitations" section was

Software Release / Document Revision	Changes
	removed from this topic. **Removed:** What's New in Micro Focus Fortify Software Security Center 22.2.0 Configuring an Eclipse Plugin Update Site
22.2.0	**Added:** • What's New in Micro Focus Fortify Software Security Center 22.2.0 • "Setting the Required Password Strength for Fortify Software Security Center Login" on page 168 • "Deploying Fortify Software Security Center to a Kubernetes Cluster" on page 52 contains the new section "Customizing the Apache Tomcat Access Logs" on page 56. The deployment procedure was also modified. • "Enabling Persistence of the LDAP Cache" on page 126 • "Changing the Support Contact Link in the About Fortify Software Security Center Box" on page 166 • "Customizing Fortify Software Security Center Logging " on page 167 • "Preparing Fortify Software Security Center to Display Debricked Results" on page 177 • "Overriding Assigned Issue Priority" on page 353 • "Viewing Open Source Data" on page 367 • "Prioritizing a ScanCentral SAST Scan Request" on page 385 • "Moving ScanCentral SAST Sensors Between Pools" on page 394 **Updated:** • Changed the URL for file downloads in"About Integrating

Software Release / Document Revision	Changes
	Components with Fortify Software Security Center" on page 45. • Some descriptions of the <*fortify.home*> directory content were modified in "About the <fortify.home> Directory" on page 59. • An important note regarding non-GUI Linux operating systems was added to "Configuring Security for BIRT Reporting" on page 96. • The topic title "Updating the Distinguished Name for LDAP Entities" was changed to "Handling LDAP Entries Marked "Invalid"" on page 125. • The procedure for configuring Fortify Software Security Center to work with SSO that uses SAML 2.0 was extensively revised in "Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single Sign-On" on page 150. • Added an important note regarding the personal access token required for Azure DevOps to "About Bug Tracker Integration" on page 169. • Edited the procedure and changed the URL for file downloads in "Preparing Fortify Software Security Center to Display Sonatype Results" on page 175. • Updated the version numbers for upgrades in "Upgrading Fortify Software Security Center" on page 195. • An important note regarding Microsoft SQL databases was added to "Fortify Software Security Center Database Upgrade Tasks" on page 196. • "Accessing the Fortify Software Security Center API Documentation" on page 219 was revised to reflect changes in the About Fortify Software Security Center *<version>* box. • The heading "Editing Velocity Templates for Bug Tracker Plugins" was changed to "Customizing Velocity Templates for Bug Tracker Plugins" on page 258.

Software Release / Document Revision	Changes
	• A note about column sorting was added to "Viewing Information About Issues to Audit" on page 328. • Information on how to search issues for date-type custom tags was added to"Searching Issues" on page 335. • The `[fortify priority order]` modifier description was changed in, and the `[engine priority]` modifier was added to the table of modifiers in "Search Modifiers" on page 336. • The "Auditing Fortify Scan Results" heading was changed to "Auditing Scan Results" on page 340. • The URL for file downloads in "About Susceptibility Analysis of Web Applications" on page 370 was changed. • The topic "Exporting Sonatype Data" was changed to "Exporting Open Source Data" on page 372. • An important note regarding generating reports from a non-GUI Linux operating system was added to "BIRT Libraries" on page 398 and to "Importing Report Libraries" on page 399. • "Acquiring the BIRT Report Designer" on page 402 includes a corrected URL for the Eclipse Downloads page and the URL for instructions on how to install the Eclipse BIRT Report Designer. • A misstatement about extending the life of a token was corrected in "Generating Authentication Tokens" on page 406. **Removed:** • What's New in Micro Focus Fortify Software Security Center 22.1.0 • Configuring SAML 2.0 Single Sign-On for SCIM / Azure AD Integration
22.1.0	**Added:** • What's New In Micro Focus Fortify Software Security Center

Software Release / Document Revision	Changes
	22.1.0 • "Monitoring Disk I/O" on page 63 • "Recurring Cleanup Jobs" on page 143 • "Pausing and Resuming Job Execution" on page 188 **Updated:** • The command for installing a self-signed or locally-signed certificate into the keystore that Fortify Software Security Center and Fortify Static Code Analyzer tools can use was modified in "About Using HTTPS and SSL Communications" on page 39. • Information about how to change the default `fortify.home` directory location was added to "About the <fortify.home> Directory" on page 59. • In "Configuring a MySQL Database" on page 65, the table that lists the settings to configure in the [mysqld] section of the MySQL options file was revised for MySQL 8.0. • "Configuring Fortify Software Security Center for the First Time" on page 72 includes changes to notes regarding the JDBC URL. • A note to indicate that the core configuration setting **Login attempts before lockout** does not apply to LDAP users was added to "Configuring Core Settings" on page 99. • "Configuring Job Scheduler Settings" on page 135 now includes descriptions of the new **Pause job execution** and **Days to preserve** settings. • "Customizing the Fortify Banner for Your Organization" on page 163 now includes a note to advise users that the banner must be re-created after a Fortify Software Security Center upgrade. • "Placing Fortify Software Security Center in Maintenance Mode" on page 185 was modified to reflect the change from

Software Release / Document Revision	Changes
	the **Configuration** > **Maintenance mode** selection to **Configuration** > **Maintenance**. • The version upgrade paths were updated in "Upgrading Fortify Software Security Center" on page 195. • An important note about restricted characters was added to "Creating Custom Roles" on page 223, "Creating Local User Accounts" on page 225, and "Editing Local User Accounts" on page 227. • A note regarding characters restricted for certain fields was added to "Creating the First Version of a New Application" on page 246 and "Adding a New Version to an Application" on page 249. • "Setting Analysis Results Processing Rules for Application Versions" on page 266 was modified to reflect the rule name change from **Ignore SCA scans performed in Quick Scan mode** to **Ignore SCA quick scan results and SCA speed dial results performed with a setting of less than four**. That topic also includes the new section "About Processing Rules that Affect Instance ID Migration" on page 271. • "Adding Custom Tags to the System" on page 274 now includes descriptions for two additional optional tag features and the new section "Adding Custom Tags to the System" on page 274. • Notes regarding the restrictions on deleting custom tags were added to "Deleting Custom Tags" on page 280. • Information about the criteria for purging scan artifacts was added to "Purging Scan Artifacts" on page 323. • A note about restrictions on artifact deletion was added to "Deleting Artifacts" on page 324. • "Viewing Information About Issues to Audit" on page 328 was modified to reflect changes to the AUDIT page. • The topic title "Viewing Issues Based on Fortify Priority" was changed to "Viewing Issues Based on Folders" on page 330" to reflect changes in terminology.

Software Release / Document Revision	Changes
	• "Filtering Issues for Display on the OVERVIEW and AUDIT Pages" on page 332 was modified to reflect the addition of the **CLEAR ALL** control and the new section Viewing Correlated Issues on the AUDIT Page. • New information about correlated issues was added to "Auditing Scan Results" on page 340. • "Viewing ScanCentral SAST Sensor Information" on page 386 was changed to reflect the addition of the **Shutdown scheduled** option to the **Filter by** list. • "Auditing Scan Results" on page 340 now includes the new section "Auditing Correlated Issues" on page 348. • The sections "Viewing Suppressed Issues", "Viewing Removed Issues," and "Viewing Hidden Issues" were added to "Setting Issue Viewing Preferences" on page 350. • Viewing Sonatype Data was changed to reflect the addition of the **Shutdown scheduled** item to the **Filter by** list. • YAML-formatted content to add to the *<app_context>*.autoconfig file was changed in "Automating Fortify Software Security Center Configuration" on page 435. **Removed:** • What's New in Micro Focus Fortify Software Security Center 21.2.0
21.2.0	**Added:** • What's New in Micro Focus Fortify Software Security Center 21.2.0 • "About Integrating Components with Fortify Software Security Center" on page 45 • "Deploying Fortify Software Security Center to a Kubernetes Cluster" on page 52 • "Setting Preferences: System-Wide and Across Application Versions" on page 212

Software Release / Document Revision	Changes
	• "Handling LDAP Entries Marked "Invalid"" on page 125 • "Viewing Scan Artifact Details" on page 313 • "Auditing a Batch of Issues" on page 358 • "Placing the ScanCentral SAST Controller in Maintenance Mode" on page 389 • "Safely Shutting Down Sensors" on page 389 **Updated:** • " Deployment Overview" on page 44 includes modified Information on how to request access to the Fortify Software Security Center Docker image. • An updated illustration of the various components of the Fortify Software Security Center environment was added to "The Fortify Software Security Center Installation Environment" on page 48. • Information about the `fortify.home` directory structure was added to "About the <fortify.home> Directory" on page 59. • The table of tables and views was changed in "Configuring Security for BIRT Reporting" on page 96. • "About Fortify Software Security Center User Authentication" on page 108 was changed to include information about SCIM. • Information about the requirements for using multiple LDAP servers was added to "Preparing to Configure LDAP Authentication" on page 108. • "Configuring LDAP Servers" on page 111 was changed to reflect the addition of new fields to the CREATE NEW LDAP CONFIGURATION dialog box. • The description of the conservative job execution strategy was changed in "Configuring Job Scheduler Settings" on page 135. • Steps were changed in the procedure described in "Setting

Software Release / Document Revision	Changes
	up Kerberos Authentication with Fortify Software Security Center" on page 157. • An important note relating to Azure DevOps Server was added to "About Bug Tracker Integration" on page 169. • The procedure described in "Updating Rulepacks from theFortify Update Server" on page 190 was modified. • In "Exporting Rulepacks" on page 190, what occurs with Rulepack exportation was clarified. • In "Deleting Rulepacks" on page 191, what occurs with Rulepack deletion was clarified. • Steps were added to the topic "Creating Custom Roles" on page 223 to reflect the addition of the **ADD MISSING PERMISSIONS** button. • Information about how a hash-based message authentication code (HMAC) is calculated was corrected in"Creating Webhooks" on page 292. • "Uploading Scan Artifacts" on page 311 was updated to reflect the removal of the **3rd party results** check box. • "Downloading Scan Artifacts" on page 315 was modified to reflect changes to the user interface. • "Viewing Information About Issues to Audit" on page 328 now includes a table that lists the columns in the issues table and a description of each. • "Viewing Hidden Issues," "Viewing Removed Issues,"and "Viewing Removed Issues" were all moved to "Setting Issue Viewing Preferences" on page 350. • A note was added to "Search Modifiers" on page 336 to recommend against using the `audience` search modifier. • "Auditing Scan Results" on page 340 was modified to reflect changes in user assignment. • "Automating Fortify Software Security Center Configuration" on page 435 includes new detail.

Software Release / Document Revision	Changes
	Removed: • What's New in Micro Focus Fortify Software Security Center 21.1.1 • Disabling Keyboard Shortcuts (Hotkeys) - That information is now available in "Setting Preferences: System-Wide and Across Application Versions" on page 212. • Enabling and Disabling Receipt of Email Alerts - That information is now available in "Setting Preferences: System-Wide and Across Application Versions" on page 212. • Accessing the Configuration Settings in the ADMINISTRATION View • Exporting Data for All Application Versions to a CSV File

Chapter 1: Introduction

Fortify Software Security Center is a browser-based product that provides a set of capabilities across the software development life cycle to automate detection of security vulnerabilities in applications. It helps your security and development teams work together to resolve security flaws quickly and accurately by making correlated data from Fortify Static Code Analyzer, Fortify ScanCentral SAST, ScanCentral DAST, and Sonatype available through its collaborative online environment.

Intended Audience

This content is written for users who are responsible for deploying and maintaining Fortify Software Security Center. It provides all of the information needed to acquire, install, and configure Fortify Software Security Center.

The information presented here is intended for users who are at least moderately knowledgeable about enterprise application development and skilled in enterprise system and database administration. It is written for:

- System and instance administrators
- Database administrators

For information about how to access the Software Security Center API Documentation, see "Accessing the Fortify Software Security Center API Documentation" on page 219.

Document Structure

This document is divided into two main parts. Part I ("Deploying Fortify Software Security Center" on page 37) includes chapters that describe the deployment environment and provide instructions for installing and configuring Fortify Software Security Center. Part II ("Using Micro Focus Fortify Software Security Center" on page 205) includes chapters that describe how to use Fortify Software Security Center.

Related Documents

This topic describes documents that provide information about Micro Focus Fortify software products.

Note: You can find the Fortify Product Documentation at https://www.microfocus.com/support/documentation. Most guides are available in both PDF and HTML formats. Product help is available within the Fortify LIM product and the Fortify WebInspect products.

All Products

The following documents provide general information for all products. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website.

Document / File Name	Description
About Fortify Product Software Documentation About_Fortify_Docs_<*version*>.pdf	This paper provides information about how to access Fortify product documentation. **Note:** This document is included only with the product download.
Fortify License and Infrastructure Manager Installation and Usage Guide LIM_Guide_<*version*>.pdf	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.
Fortify Software System Requirements Fortify_Sys_Reqs_<*version*>.pdf	This document provides the details about the environments and products supported for this version of Fortify Software.
Fortify Software Release Notes FortifySW_RN_<*version*>.pdf	This document provides an overview of the changes made to Fortify Software for this release and important information not included elsewhere in the product documentation.
What's New in Fortify Software <version> Fortify_Whats_New_<*version*>.pdf	This document describes the new features in Fortify Software products.

Fortify ScanCentral DAST

The following document provides information about Fortify ScanCentral DAST. Unless otherwise noted, this document is available on the Micro Focus Product Documentation website at https://www.microfocus.com/documentation/fortify-ScanCentral-DAST.

Document / File Name	Description
Fortify ScanCentral DAST Configuration and Usage Guide SC_DAST_Guide_ *<version>*.pdf	This document provides information about how to configure and use Fortify ScanCentral DAST to conduct dynamic scans of Web applications.

Fortify ScanCentral SAST

The following document provides information about Fortify ScanCentral SAST. Unless otherwise noted, this document is available on the Micro Focus Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center.

Document / File Name	Description
Fortify ScanCentral SAST Installation, Configuration, and Usage Guide SC_SAST_Guide_ *<version>*.pdf	This document provides information about how to install, configure, and use Fortify ScanCentral SAST to streamline the static code analysis process. It is written for anyone who intends to install, configure, or use Fortify ScanCentral SAST to offload the resource-intensive translation and scanning phases of their Fortify Static Code Analyzer process.

Fortify Static Code Analyzer

The following documents provide information about Fortify Static Code Analyzer. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at https://www.microfocus.com/documentation/fortify-static-code.

Document / File Name	Description
Fortify Static Code Analyzer User Guide SCA_Guide_<*version*>.pdf	This document describes how to install and use Fortify Static Code Analyzer to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding.
Fortify Static Code Analyzer Applications and Tools Guide SCA_Apps_Tools_<*version*>.pdf	This document describes how to install Fortify Static Code Analyzer applications and tools. It provides an overview of the applications and command-line tools that enable you to scan your code with Fortify Static Code Analyzer, review analysis results, work with analysis results files, and more.
Fortify Static Code Analyzer Custom Rules Guide SCA_Cust_Rules_Guide_<*version*>.zip	This document provides the information that you need to create custom rules for Fortify Static Code Analyzer. This guide includes examples that apply rule-writing concepts to real-world security issues. **Note:** This document is included only with the product download.
Fortify Audit Workbench User Guide AWB_Guide_<*version*>.pdf	This document describes how to use Fortify Audit Workbench to scan software projects and audit analysis results. This guide also includes how to integrate with bug trackers, produce reports, and perform collaborative auditing.
Fortify Plugin for Eclipse User Guide Eclipse_Plugin_Guide_<*version*>.pdf	This document provides information about how to install and use the Fortify Complete Plugin for Eclipse.

Document / File Name	Description
Fortify Analysis Plugin for IntelliJ IDEA and Android Studio User Guide IntelliJ_AnalysisPlugin_Guide_<*version*>.pdf	This document describes how to install and use Fortify Analysis Plugin for IntelliJ IDEA and Android Studio.
Fortify Extension for Visual Studio User Guide VS_Ext_Guide_<*version*>.pdf	This document provides information about how to install and use the Fortify extension for Visual Studio to analyze, audit, and remediate your code to resolve security-related issues in solutions and projects.
Fortify Static Code Analyzer Applications and Tools Properties Reference Guide SCA_Tools_Props_Ref_<*version*>.pdf	This document describes the properties used by Fortify Static Code Analyzer applications and command-line tools.

Fortify WebInspect

The following documents provide information about Fortify WebInspect. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at https://www.microfocus.com/documentation/fortify-webinspect.

Document / File Name	Description
Fortify WebInspect Installation Guide WI_Install_<*version*>.pdf	This document provides an overview of Fortify WebInspect and instructions for installing Fortify WebInspect and activating the product license.
Fortify WebInspect User Guide WI_Guide_<*version*>.pdf	This document describes how to configure and use Fortify WebInspect to scan and analyze Web applications and Web services. **Note:** This document is a PDF version of the Fortify WebInspect help. This PDF

Document / File Name	Description
	file is provided so you can easily print multiple topics from the help information or read the help in PDF format. Because this content was originally created to be viewed as help in a web browser, some topics may not be formatted properly. Additionally, some interactive topics and linked content may not be present in this PDF version.
Fortify WebInspect and OAST on Docker User Guide WI_Docker_Guide_<*version*>.pdf	This document describes how to download, configure, and use Fortify WebInspect and Fortify OAST that are available as container images on the Docker platform. The Fortify WebInspect image is intended to be used in automated processes as a headless sensor configured by way of the command line interface (CLI) or the application programming interface (API). It can also be run as a Fortify ScanCentral DAST sensor and used in conjunction with Fortify Software Security Center. Fortify OAST is an out-of-band application security testing (OAST) server that provides DNS service for the detection of OAST vulnerabilities.
Fortify WebInspect Tools Guide WI_Tools_Guide_<*version*>.pdf	This document describes how to use the Fortify WebInspect diagnostic and penetration testing tools and configuration utilities packaged with Fortify WebInspect and Fortify WebInspect Enterprise.
Fortify WebInspect Agent Installation Guide WI_Agent_Install_<*version*>.pdf	This document describes how to install the Fortify WebInspect Agent for applications running under a supported Java Runtime Environment (JRE) on a supported application server or service and applications running under a supported .NET Framework on a supported version of

Document / File Name	Description
	IIS.
Fortify WebInspect Agent Rulepack Kit Guide WI_Agent_Rulepack_Guide_<*version*>.pdf	This document describes the detection capabilities of Fortify WebInspect Agent Rulepack Kit. Fortify WebInspect Agent Rulepack Kit runs atop the Fortify WebInspect Agent, allowing it to monitor your code for software security vulnerabilities as it runs. Fortify WebInspect Agent Rulepack Kit provides the runtime technology to help connect your dynamic results to your static ones.

Fortify WebInspect Enterprise

The following documents provide information about Fortify WebInspect Enterprise. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at https://www.microfocus.com/documentation/fortify-webinspect-enterprise.

Document / File Name	Description
Fortify WebInspect Enterprise Installation and Implementation Guide WIE_Install_<*version*>.pdf	This document provides an overview of Fortify WebInspect Enterprise and instructions for installing Fortify WebInspect Enterprise, integrating it with Fortify Software Security Center and Fortify WebInspect, and troubleshooting the installation. It also describes how to configure the components of the Fortify WebInspect Enterprise system, which include the Fortify WebInspect Enterprise application, database, sensors, and users.
Fortify WebInspect Enterprise User Guide WIE_Guide_<*version*>.pdf	This document describes how to use Fortify WebInspect Enterprise to manage a distributed network of Fortify WebInspect sensors to scan and analyze Web applications and Web services. **Note:** This document is a PDF version of the

Document / File Name	Description
	Fortify WebInspect Enterprise help. This PDF file is provided so you can easily print multiple topics from the help information or read the help in PDF format. Because this content was originally created to be viewed as help in a web browser, some topics may not be formatted properly. Additionally, some interactive topics and linked content may not be present in this PDF version.
Fortify WebInspect Tools Guide WI_Tools_Guide_ *<version>*.pdf	This document describes how to use the Fortify WebInspect diagnostic and penetration testing tools and configuration utilities packaged with Fortify WebInspect and Fortify WebInspect Enterprise.

Part I: Deploying Fortify Software Security Center

The following chapters describe the Fortify Software Security Center deployment environment and provide instructions for installing and configuring Fortify Software Security Center.

Chapter 2: Providing for Secure Deployment

Just as you apply security precautions to analyzed source code, you must also secure access to the Fortify Software Security Center analysis products that access the source code. Moreover, the concentrated summarization of security vulnerabilities that the Fortify Software Security Center family of products provides might mandate an even higher level of secure deployment.

The topics in this section summarize some of the ways to securely deploy Fortify Software Security Center.

Securing Access to Facilities

Fortify Software Security Center stores and renders the source code of applications it has analyzed and any issues discovered in those applications as HTML. Because program source code and any detected vulnerabilities it contains offer various opportunities for mishandling or abuse, Fortify recommends that administrators deploy Fortify Software Security Center in a secure operations facility. You must also secure the underlying Fortify Software Security Center file system and restrict access to the Fortify Software Security Center installation directory.

Securing Tomcat Server

You must ensure the operational security of the application server that runs Fortify Software Security Center. At a minimum, configure Tomcat Server to use HTTPS in conjunction with an SSL certificate issued by a trusted certificate authority. Also, take any additional steps necessary to secure Tomcat Server in your operating environment.

Using More Secure Cipher Suites

Fortify recommends that you disable weak SSL/TLS cipher suites in Tomcat in favor of more secure suites.

APR-based SSL Connections

If you use an APR-based SSL connection, use the SSLCipherSuite directive. For detailed information, see https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslciphersuite and Cipher Suites and Enforcing Strong Security (https://httpd.apache.org/docs/current/ssl/ssl_howto.html).

JSSE-based SSL Connections

If you use a JSSE-based SSL connection, use the `ciphers` and the `honorCipherOrder` attributes. For details, see Apache Tomcat 9 Configuration Reference - The HTTP Connector.

Because of trade-offs between improved security and improved interoperability, better performance, and so on, there is no correct cipher suite choice. However, Apache provides information that can help you make your choice (see https://cwiki.apache.org/confluence/display/TOMCAT/Ciphers).

Setting Tomcat Server Attributes to Protect Sensitive Data in Cookies

Some Tomcat Server settings might make the sensitive information in some cookies vulnerable to unnecessary disclosure.

To protect sensitive data, Fortify recommends that you add the following attributes (flags) for cookies on the Tomcat application server:

- `Secure:` The `Secure` attribute prevents the cookie from being transmitted on requests that are not protected with SSL or TLS. Use this option to prevent cookies that could disclose sensitive information (for example, session identifiers) from leaking information over insecure channels (such as HTTP).
- `HttpOnly:` The `HttpOnly` attribute prevents the cookie value from being accessed through client-side scripting routines. Fortify recommends that you keep this attribute enabled unless the cookie is being read by client-side JavaScript routines.

For information about how to set the `Secure` and `HttpOnly` attributes, see the Apache Tomcat configuration reference documentation.

About Using HTTPS and SSL Communications

Fortify strongly recommends that you configure Fortify Software Security Center and Fortify client products (including Audit Workbench, fortifyclient, the Eclipse Complete plugin, and the Visual Studio extension) to use HTTPS and Secure Sockets Layer (SSL) for all communications.

Configuring Fortify Static Code Analyzer Applications to Communicate with Fortify Software Security Center Using HTTPS

If you are using a third-party certificate purchased from and signed by a trusted root CA such as VeriSign, Entrust, or Thawte, you do not need to do anything on the client side to use https to communicate with Fortify Software Security Center. The

certificate is trusted because these root CA certificates are in the keystore that Fortify client products use.

However, by default, Fortify Software Security Center, Audit Workbench, fortifyclient, the Eclipse Complete plugin, and the Visual Studio extension do not trust self-signed certificates or certificates signed by an internal or local signing authority. In this case, to use https to communicate with Fortify Software Security Center, you must import the self- or locally-signed certificate into the Java Runtime certificate store.

Important! If you used a third-party Certification Authority to issue a locally-signed certificate, make sure that you import the CA certificate chain you used to issue the certificate.

To install a self-signed or locally-signed certificate into the keystore that Fortify Software Security Center and Fortify Static Code Analyzer tools use, do the following on every machine on which any of these products is installed:

Open a command prompt, and then run the following:

```
cd "<sca_install_dir>\jre\bin"
keytool -importcert -alias SSC -keystore ..\lib\security\cacerts -file
"YourCertFile.cer" -trustcacerts
```

where `YourCertFile.cer` is the same certificate file that you imported on Tomcat Server.

If, for some reason, the certificate file is not available, you can export it from the keystore used by Tomcat Server, as follows:

```
cd <java_home>\jre\bin
keytool -exportcert -alias SSC -keystore <keystore_used_by_tomcat> -
file
YourCertFile.cer
```

Note that you can use any name you want for the alias. These examples use `SSC`.

Additional Information

When you create a self-signed certificate interactively with the java keytool, you are prompted to provide your first and last names. Provide the fully-qualified domain name of the server that hosts Fortify Software Security Center. Do not simply use the short hostname or "localhost."

When you create a connector in the `server.xml` file for HTTPS, make sure that you include the attribute `keyAlias`, using the name of the alias for the certificate in your keystore. Otherwise, if the keystore contains multiple certificates, it uses the first certificate it finds.

About Securing Passwords and User Roles

Fortify recommends that, after you deploy Fortify Software Security Center and log in for the first time, you immediately create one or more new local administrator accounts and delete the default administrator account. For information about how to log in to Fortify Software Security Center, see "Logging in to Fortify Software Security Center" on page 78.

Fortify Software Security Center account security features include:

- The ability for administrators to suspend accounts that have become temporarily inactive
- The automatic lock-out of accounts on the basis of failed log-on attempts

For more information about Fortify Software Security Center account management, see "Managing User Accounts" on page 221.

If you are using LDAP to authenticate Fortify Software Security Center users, configure your LDAP server to use secure LDAP communications. For information about how to configure Fortify Software Security Center to use LDAP authentication, see "LDAP User Authentication" on page 108.

Managing Computer Services and Accounts

When you install Fortify Software Security Center, configure it as a service running under a least-privileged user account. Also, because Fortify Software Security Center temporarily stores files that are uploaded from a user account to the computer's file system, always install and run updated anti-virus software on the machine that hosts Fortify Software Security Center.

Chapter 3: Preparing for Fortify Software Security Center Deployment

This section describes how to prepare to deploy Fortify Software Security Center for the first time.

High-Level Deployment Tasks

The following table lists the high-level tasks you need to perform to prepare for Fortify Software Security Center deployment. It also provides links to the topics that describe these tasks.

Note: If you are upgrading Fortify Software Security Center, see "Upgrading Fortify Software Security Center" on page 195.

Task	Description	Information and Instructions
1	Download the Fortify Software Security Center software files and the `fortify.license` file.	"Downloading Fortify Software Security Center Files" on page 50
2	Unpack and deploy the installation bundle. Then deploy Fortify Software Security Center in Tomcat Server.	"Unpacking and Deploying Fortify Software Security Center Software" on page 50
3	Install and configure the software for the database server you plan to use for the Fortify Software Security Center database.	"About the Fortify Software Security Center Database" on page 62
4	Start Tomcat server, and then log in to Fortify Software Security Center. (See "Logging in to Fortify Software Security Center" on page 78.)	"Logging in to Fortify Software Security Center" on page 78
5	Use the Fortify Software Security Center Setup wizard to perform initial configuration. (Locate your Fortify license, create the Fortify Software Security Center	"Configuring Fortify Software Security Center for the First Time" on page 72

Task	Description	Information and Instructions
	database tables and initialize the database schema, seed the database, and so on.) **Tip:** *Advanced users only*: You can automate configuration *before* you deploy Fortify Software Security Center. After you do, the Setup wizard retrieves your configuration settings at server startup and automates the entire installation. For details, see "Automating Fortify Software Security Center Configuration" on page 435.	
6	Restart the Fortify Software Security Center server.	
7	Complete the Fortify Software Security Center configuration settings in the ADMINISTRATION view. (For the list of the options to configure in the ADMINISTRATION view, see "Configuration Options Available in the ADMINISTRATION View" on page 85.)	"Additional Fortify Software Security Center Configuration" on page 82
8	Perform additional tasks such as configuring an Eclipse plugin update site, setting up bug tracker integration, configuring single sign-on, administering users, registering LDAP entities, managing LDAP user roles, and creating custom attributes that users can assign to their applications.	"Additional Installation-Related Tasks" on page 169

If you plan to remove Fortify Software Security Center and no longer need the Fortify Software Security Center database, you can find instructions on how to permanently delete it in "Permanently Deleting a Fortify Software Security Center Database" on page 71.

Deployment Overview

Fortify Software Security Center provides a centralized management and analysis facility for application data gathered and processed using Fortify analysis products and tools (Fortify Static Code Analyzer, Fortify WebInspect Agent, Fortify ScanCentral, and Audit Workbench) across the complete Secure Development Lifecycle (SDL).

Fortify Software Security Center is packaged as a Web Archive (WAR) file. It runs under Tomcat Server and requires a supported third-party database.

After initial deployment, you use the Fortify Software Security Center Setup wizard to complete preliminary configuration. This enables Fortify Software Security Center to work with required entities such as the third-party database.

Tip: For advanced users only. You can automate configuration before you deploy Fortify Software Security Center.

After you finish the initial Fortify Software Security Center configuration, complete the configuration of the core parameters and configure additional settings from the ADMINISTRATION view. For instructions, see "Additional Fortify Software Security Center Configuration" on page 82.

Important! Fortify only supports the deployment of a single Fortify Software Security Center instance. Furthermore, that instance must not be behind a load balancer.

For system requirements information, see the *Micro Focus Fortify Software System Requirements* document.

To provide centralized management, Fortify Software Security Center inter-operates with the following external components:

- Required components
  - Apache Tomcat Server
  - Third-party database
  - Fortify Security Content Server
- Optional components
  - Third-party LDAP authentication server
  - Defect-tracking system
  - Parser plugin
  - SMTP email server

- One or more Fortify analysis agents and tools
- Kubernetes

About Integrating Components with Fortify Software Security Center

You can integrate the following components with Fortify Software Security Center:

Components	Integration Instructions
System for Cross-domain Identity Management (SCIM)	"Enabling SCIM for Provisioning of Externally Managed Users and Groups" on page 132 "Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single Sign-On" on page 150
Fortify Audit Assistant	"Configuring Audit Assistant" on page 90
Java Message Service (JMS)	"Configuring Java Message Service Settings" on page 107
LDAP servers	"Configuring LDAP Servers" on page 111
Single-sign on (SSO) providers:	
• Central Authentication Server (CAS)	"Configuring Fortify Software Security Center to Work with a Central Authorization Server" on page 149
• SPNEGO/Kerberos	"Setting up Kerberos Authentication with Fortify Software Security Center" on page 157
• SAML	"Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single Sign-On" on page 150
• HTTP	"Configuring Fortify Software Security Center to Work with Single Sign-On and Single Logout Solutions that use HTTP Headers" on page 155
• x509	"Configuring Fortify Software Security Center to Use X.509 Certification-based SSO" on page 159
Fortify ScanCentral SAST	"Configuring ScanCentral SAST Monitoring in Fortify Software Security Center" on page 134
Fortify ScanCentral	"Enabling the Running and Management of

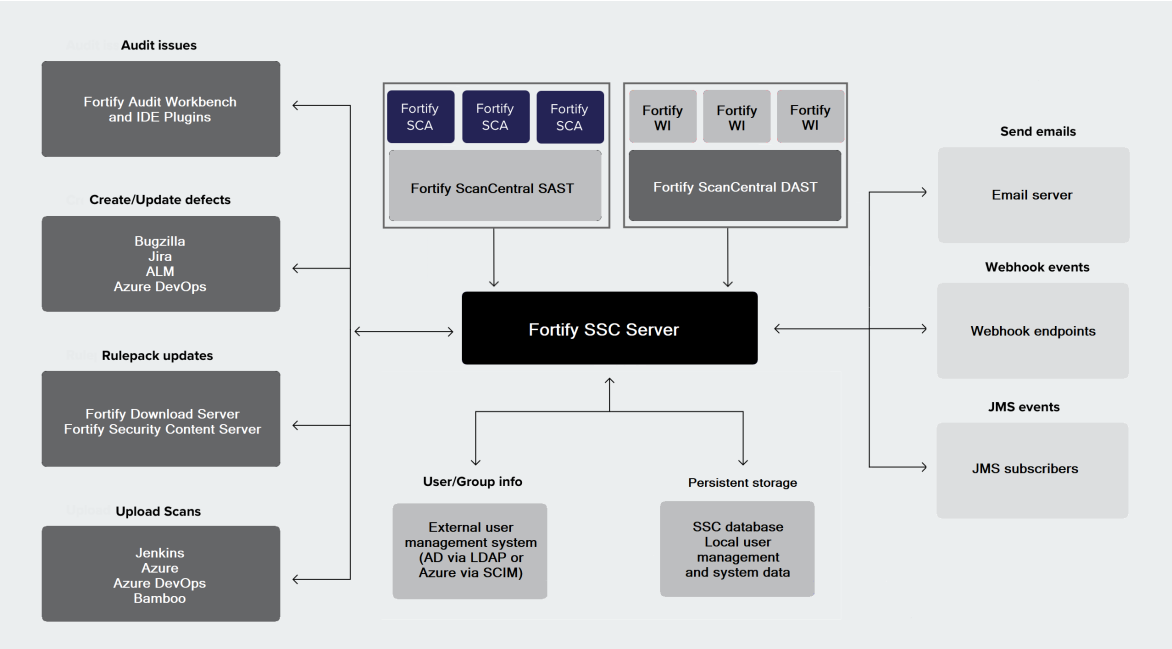
Components	Integration Instructions
DAST	ScanCentral DAST Scans from Fortify Software Security Center" on page 135
Fortify Static Code Analyzer Applications and Tools:	
• Fortify Audit Workbench	*Fortify Audit Workbench User Guide* https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools
• Fortify Jenkins plugin	*Fortify Jenkins Plugin User Guide* https://www.microfocus.com/documentation/fortify-jenkins-plugin
• Fortify Eclipse plugin	*Fortify Plugin for Eclipse User Guide* https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools
• Fortify Extension for Visual Studio	*Fortify Extension for Visual Studio User Guide* https://www.microfocus.com/documentation/fortify-visual-studio-code
• Fortify Extension for Visual Studio Code	Fortify Visual Studio Code Documentation https://www.microfocus.com/documentation/fortify-visual-studio-code
• Fortify Plugin for Bamboo	Fortify Plugin for Bamboo User Guide https://www.microfocus.com/documentation/fortify-plugin-for-bamboo
• Fortify Analysis Plugin for IntelliJ IDEA and Android Studio	*Fortify Analysis Plugin for IntelliJ IDEA and Android Studio User Guide* https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools
• Fortify Remediation Plugin for Eclipse	*Fortify Remediation Plugin for Eclipse User Guide*
• Fortify Remediation Plugin for IntelliJ	*Fortify Remediation Plugin for IntelliJ IDEA and Android Studio User Guide*

Components	Integration Instructions
IDEA and Android Studio	
• Fortify SourceAndLibScanner	Download Fortify SourceAndLibScanner from the Fortify Marketplace at https://marketplace.microfocus.com/cyberres/category/fortify. The software package comes with documentation.
Fortify Azure DevOps Extension	https://www.microfocus.com/documentation/fortify-azure-devops-extension
Security training vendors	"Configuring Application Security Training" on page 88

Important! When you integrate Fortify Software Security Center with other Fortify products (for example, ScanCentral DAST, Audit Workbench, and so on) make sure that you minimize clock skew between communicating machines. Fortify recommends that you synchronize computer clock times using, for example, Network Time Protocol (NTP). If that is not possible, Fortify suggests that you maintain a clock skew of less than five minutes, compared on a UTC basis. Otherwise, requests to Fortify Software Security Center can fail.

The Fortify Software Security Center Installation Environment

The following figure illustrates the relationship of Fortify Software Security Center to the required and optional components listed in " Deployment Overview" on page 44.



The following table provides descriptions of the required and optional Fortify Software Security Center installation components in the illustration.

Component	Description
Fortify SSC Server	Fortify Software Security Center is delivered as a Web Archive (WAR) file run by Tomcat Server or as a Helm chart for Kubernetes deployment.
SSC database	Third-party database that Fortify Software Security Center requires to store user and artifact data. Before you put Fortify Software Security Center into production, you must install a supported third-party database.
Third-party LDAP authentication server	(Optional) You can configure Fortify Software Security Center to use LDAP authentication.

Component	Description
Defect-tracking server	(Optional) You can configure Fortify Software Security Center to enable bug submission directly to Bugzilla, Jira, ALM, Azure DevOps Server, or a customized bug-tracking system. For information about how to create a customized bug-tracking system, see "Authoring Bug Tracker Plugins" on page 423.
Third-party email server	(Optional) You can configure Fortify Software Security Center to use an external SMTP email server to send alerts to application collaborators.
Fortify Static Code Analyzer analysis agent	(Optional) Fortify Static Code Analyzer scans source code and identifies issues.
Audit Workbench and IDE plugins	Audit Workbench and Fortify IDE plugins can be used as alternative source-code auditing tools.
Jenkins Azure DevOps Bamboo	Use these plugins to scan source code (using Fortify Static Code Analyzer) and upload scan results.
Fortify ScanCentral SAST	(Optional) Fortify Static Code Analyzer users can use ScanCentral SAST to offload processor-intensive code analysis tasks from their build machines to a group of machines (sensors) provided for this purpose.
Fortify ScanCentral DAST	(Optional) A dynamic application security testing tool that you can use to configure and run dynamic scans of your web applications from Fortify Software Security Center.
Fortify WebInspect	(Optional) Analysis agent that connects with Fortify WebInspect agents to retrieve potential dynamic issues.
Fortify Security Content update server	Used to acquire and update Security Content.

Important! Fortify does not support load balancing across multiple Fortify Software Security Center servers.

Downloading Fortify Software Security Center Files

Fortify software is only available for download from the Software Licenses and Downloads (SLD) portal (https://sld.microfocus.com). For descriptions of the Fortify software installation packages available there, see the*Fortify Software System Requirements* document.

Download the installation files and the `fortify.license` file following the instructions in the *Fortify Software System Requirements* document. A helpful how-to video at https://www.youtube.com/playlist?list=PL8yfmcqTN8GE9XCGVgxMQDFFZy9_-R-e3 also provides instructions on how to download Fortify software.

See Next

"Unpacking and Deploying Fortify Software Security Center Software" below

Unpacking and Deploying Fortify Software Security Center Software

To unpack and deploy the Fortify Software Security Center installation files:

1. Extract the contents of the installation file into a temporary directory in a secure location. (The installation file is the file you downloaded using the instructions in "Downloading Fortify Software Security Center Files" above.)
2. Locate the distribution file (`Fortify_<version>_Server_WAR_Tomcat.zip`) and extract all of the contents into a directory in a secure location. This creates the `Fortify-Server-WAR` directory, which contains the resources and tools you need for tasks such as configuring Fortify Software Security Center and migrating applications from previous versions.

   Note: The directory into which you extract the distribution file content is referred to in all topics as the `<ssc_install_dir>` directory.

3. Copy the seed bundle files from the `srg_content` folder in the temporary directory to the `<ssc_install_dir>` directory. *Do not* unzip the seed bundle files.

   Note: Although you are not required to copy the resource files to the `<ssc_install_dir>` directory, the procedures in this document are based on the assumption that you saved the files to that location.

   The seed bundles are described in the following table.

File Name	Description
`Fortify_`	Process template seed bundle used to seed database

File Name	Description
`Process_Seed_Bundle-2023_Q1_<build>.zip`	tables. It provides a default admin user account and issue template data.
`Fortify_Report_Seed_Bundle-2023_Q1_<build>.zip`	Report seed bundle used to seed database tables. It provides the default set of Fortify Software Security Center reports.
`Fortify_PCI_Basic_Seed_Bundle-2023_Q1_<build>.zip`	(Optional) The PCI Basic seed bundle adds a Payment Card Industry (PCI) Data Security Standard (DSS) process template and its associated report to the default set of issue templates and reports. PCI DSS will remain open for assessment of previously-started, and newly-started assessments initiated before June 2021, until October 2022. After October 2022, the new PCI Software Security Framework (SSF) will be the set of standards for evaluation. Please use the PCI SSF Basic seed bundle (`Fortify_PCI_SSF_Basic_Seed_Bundle-2023_Q1_<build>.zip`) to begin to understand how software security issues can affect evaluation under these new PCI SSF standards.
`Fortify_PCI_SSF_Basic_Seed_Bundle-2023_Q1_<build>.zip`	(Optional) The PCI SSF Basic seed bundle adds a Payment Card Industry (PCI) Software Security Framework (SSF) process template and its associated report to the default set of issue templates and reports. PCI SSF was introduced in June 2019 as a set of new standards used to evaluate systems developed by payment software vendors. The existing PCI DSS will remain open for assessment of previously-started, and newly-started assessments initiated before June 2021, until October 2022. After October 2022, the new PCI Software Security Framework (SSF) will be the set of standards for evaluation. Please use the PCI Basic seed bundle (`Fortify_PCI_Basic_Seed_Bundle-2023_Q1_<build>.zip`) for evaluation under PCI DSS.

The process templates seed bundle and the reports seed bundle are required for Fortify Software Security Center deployment. The PCI Basic seed bundles are optional.

4. Copy the `fortify.license` file to the `<ssc_install_dir>` directory. (For information about how to obtain the `fortify.license` file, see the *Fortify Software System Requirements* document.)

Deploying Fortify Software Security Center to a Kubernetes Cluster

The following steps describe how to prepare for and perform a Fortify Software Security Center Kubernetes deployment. For information about supported versions of the required software, see the *Micro Focus Fortify Software System Requirements* document for this release.

The following are required in the Kubernetes and helm space:

- Persistent volume: For the configuration file and log files. Kubernetes persistent volume must support the PodSecurityContext `fsGroup` field. Fortify Software Security Center Helm chart deployment supports changing the default UID and GID using the "user" Helm chart values ("user.uid", "user.gid"). With `fsGroup` supported, you can change both the UID and GID without affecting Fortify Software Security Center functionality.

  If Fortify Software Security Center runs on Kubernetes with persistent volume *without* `fsGroup` support, or if the Fortify Software Security Center container image is used outside of Kubernetes, Fortify Software Security Center cannot start if run with a non-default GID. In this case, you must manually configure permission on Fortify Software Security Center volume directories and files before you can start it.
- Secrets file - Responsible for storing everything regarding licenses or connections to the database, for example, username / password, and such information, and this is important when it comes to SSL or HTTPS, because Fortify Software Security Center in Kubernetes only runs on HTTPS. So, you must have a TLS or SSL connection. All of this information (trust, keystore, license file) is stored in the secrets file. You must have your license and keystore available.
- `ssc-values.yaml` file - Used to store or set all parameters for your helm chart. The Helm chart needs data to set up SSC.

You want to store results in SSC, and for that you use the SSC database. And, the version of database in your Kubernetes space must be the same as the version used for the ssc db.

You also need to grant users access to ssc. For that you need some kind of service (load balancer, cluster IP, or node port) that are components of Kubernetes

To prepare for your Fortify Software Security Center Kubernetes deployment, do the following:

1. Install and set up kubectl. For instructions, see https://kubernetes.io/docs/tasks/tools/install-kubectl.
2. Install Helm. (To download the software, see https://github.com/helm/helm/releases. For installation instructions, see https://helm.sh/docs/intro/install. For upgrade instructions, see https://helm.sh/docs/helm/helm_upgrade/#helm.)
3. (Air-gapped installation only) Install Docker. For installation instructions, see https://docs.docker.com/get-docker.
4. Copy the contents of the helm directory from the Fortify Software Security Center distribution ZIP file to the *<ssc_helm_dir>* directory. Navigate to the *<ssc_helm_dir>* directory and copy the `ssc-values-example.yaml` file to `ssc-values.yaml`.

Fortify Software Security Center Kubernetes Deployment

You can deploy Fortify Software Security Center in an environment with Internet access, or in an air-gapped environment. If you plan to deploy the application in an environment with Internet access, you can pull the Fortify Software Security Center Docker image (fortifydocker/ssc-webapp) from the Docker Hub registry. If you must deploy the application in an air-gapped environment, you must use a private registry for the deployment and transfer the Fortify Software Security Center container image to it.

Deploying Fortify SSC to a Kubernetes Cluster

The procedure used to deploy Fortify Software Security Center in an environment that has Internet access is almost identical to the procedure used to deploy the product in an air-gapped environment. The only difference is that, for an air-gapped deployment, you must push the Fortify Software Security Center container image to a private registry that is accessible from your Kubernetes cluster.

To deploy Fortify Software Security Center to a Kubernetes cluster:

1. Create a Docker Hub account, and then supply your account name to Fortify Customer Support (https://www.microfocus.com/support).

   Note: Fortify Customer Support can give you access to the Fortify repository on the Docker Hub (fortifydocker organization).

2. To request access to the Fortify Software Security Center Docker image published in the Docker Hub registry, send an email with the following information to fortifydocker@microfocus.com:
   - First Name
   - Last Name
   - Company Name

- Docker ID
- Customer ID

3. (For an air-gapped installation, or if you want to use a private registry. A running Docker server and Docker client are assumed to be in place.) Transfer the Fortify Software Security Center container image to your private registry, as follows:
   a. Log in to the Docker Hub using `docker login`.
   b. Log in to your private registry using `docker login <priv_reg_host_and_port>`, where `<priv_reg_host_and_port>` represents the host and port of your private registry.
   c. Transfer the Fortify Software Security Center container image, as follows:
      i. `docker pull"fortifydocker/ssc-webapp:<tag>"`
      ii. `docker tag"fortifydocker/ssc-webapp:<tag>""<priv_reg_host_and_port>/<priv_reg_path>/ssc-webapp:<tag>"`
      iii. `docker push "<priv_reg_host_and_port>/<priv_reg_path>/ssc-webapp:<tag>"`

      Note: To determine the value to use for <*tag*>, go to the `<ssc_helm_dir>` directory and open the `ssc-<chart_version>+<ssc_version>.tgz` file. Use the `<ssc_version>` value (tag for the latest published image build) from the TGZ file name.

      There are also tags for exact image builds in the format `<ssc_version>.<imageBuildNumber>`

      You can list available image tags in the docker hub. If you use `<imageBuildNumber>`, you must specify it in the `image.buildNumber` Helm chart value.

      Important! The image name (`ssc-webapp`) and the tag (`<tag>`) value must stay the same.

   d. Enter the `<priv_reg_host_and_port>/<priv_reg_path>/` as the value for `image.repositoryPrefix` parameter in the `<ssc_helm_dir>/ssc-values.yaml` file. (The value you specify for the `image.repositoryPrefix` parameter must include a trailing forward slash (/).)
4. If you want to use the exact image build tag, enter the `<imageBuildNumber>` value as the value for the `image.buildNumber`. Otherwise, leave it empty.
5. Provision a Kubernetes secret for pulling images from the registry (Docker Hub or private registry). For instructions, see `https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry` and enter the secret name as the value for the `imagePullSecrets` parameter in the `<ssc_helm_dir>/ssc-values.yaml` file. If the secret is `regcred`, then the format is:

```
imagePullSecrets:
 - name: regcred
```

Note: The `imagePullSecrets` value is required for access to the Docker Hub registry. If you have a private registry that can be accessed without credentials, then there is no need to specify `imagePullSecrets`.

6. Provision another Kubernetes secret that contains the data required for the deployment. Inspect the `secretRef.keys` file for the list of data accepted. The minimum required set includes `httpCertificateKeystoreFileEntry`, `httpCertificateKeystorePasswordEntry`, and `httpCertificateKeyPasswordEntry`.

   The following example shows how to create the secret manually:

   a. Create a *<ssc_secrets_dir>* directory.

   b. Create a file for each of the `secretRef.keys` required entries. You must have at least three files in the directory: a Java keystore file that contains the HTTPS certificate and its private key, a file with the password for the keystore, and a file that contains the password for the secret key of the HTTPS certificate.

   c. Create the secret using the `kubectl` command:

      ```
      kubectl create secret generic "<ssc_secret_name>" --from-file
      "<ssc_secrets_dir>"
      ```

   d. Enter the *<ssc_secret_name>* as the value for the `secretRef.name` parameter in the *<ssc_helm_dir>*`/ssc-values.yaml` file.

   e. For each file provided in *<ssc_secrets_dir>*, enter the file name as the value for the related the `secretRef.keys.*Entry` parameter in the *<ssc_helm_dir>*`/ssc-values.yaml` file.

   Note: Changes in the secret are not applied automatically by the deployment. To use a changed secret with an existing deployment, you must manually remove the Fortify Software Security Center Pod to trigger automatic re-creation.

7. Enter any other required parameters to the *<ssc_helm_dir>*`/ssc-values.yaml` file.

   - The `urlHost` must contain the fully-qualified DNS name intended for accessing Fortify Software Security Center. The address for accessing the Fortify Software Security Center installation is `<https://`*<urlHost>*`:`*<service.httpsPort>*`/`*<sscPathPrefix>*. For example, `https://ssc.example.com:443/ssc`. If the port is 443, you can omit it from the URL (`https://ssc.example.com/`).
   - For ease of use, Fortify recommends that you set the `service.type` parameter to `LoadBalancer`.

- To apply changes to the Fortify Software Security Center secret referenced by `secretRef.name`, you must manually remove the ssc-webapp Pod (it is later automatically re-created).

Note: If necessary, you can change most values you specify for parameters in the *<ssc_helm_dir>*`/ssc-values.yaml` file later, and then redeploy Fortify Software Security Center to implement the changes. Depending on the Kubernetes cluster, the exception might be parameters for a `persistentVolumeClaim`.

Deployment

To deploy Fortify Software Security Center for the first time, run the following:

```
helm install "<unique_deployment_name>" "<ssc_helm_dir>/ssc-<chart_version>+<ssc_version>.tgz" -f "<ssc_helm_dir>/ssc-values.yaml"
```

For subsequent deployments, run the following:

```
helm upgrade "<unique_deployment_name>" "<ssc_helm_dir>/ssc-<chart_version>+<ssc_version>.tgz" -f "<ssc_helm_dir>/ssc-values.yaml"
```

Next, use the default administrator account to log in to Fortify Software Security Center and perform post-installation configuration, just as you would after a standard installation. For details, see "Configuring Fortify Software Security Center for the First Time" on page 72.

Customizing the Apache Tomcat Access Logs

To change the default format for Tomcat access logs on the ssc-webapp container image, set the `HTTP_SERVER_ACCESS_LOG_PATTERN` environment variable to the Tomcat Access Log Valve pattern. For information about the patterns supported, see the Apache Tomcat 9 Configuration Reference website (`https://tomcat.apache.org/tomcat-9.0-doc/config/valve.html#Access_Log_Valve`).

You can use the environment Helm chart value, as shown in the following example:

```
environment:
-    name: HTTP_SERVER_ACCESS_LOG_PATTERN
     value: '%h %l %u %t "%r" %s %b'
```

Troubleshooting a Fortify Software Security Center Deployment to a Kubernetes Cluster

This section provides information about the error messages that can be encountered during an attempted deployment.

If you crash during the installation phase, run:

```
kubectl describe pod <pod_name>
```

To display logs after installation, run:

```
kubectl logs <pod_name> -f
```

To view the status of Pods running on your cluster (Pending, Running, Succeeded, Failed, or Unknown), run:

```
kubectl get pods
```

If no Pods are running, the interactive environment is still reloading its previous state. Wait for several seconds, and then run `kubectl get pods` again. Once you see the Pod running, continue.

To see a list of all services, the assigned IPs (cluster and external) and ports, run:

```
kubectl get services
```

To list those names, run:

```
helm list
```

To get values/configuration for a specific deployment installed by helm, run:

```
helm get values <installation name>
```

To see information about the volume being mounted or to see whether the image was pulled successfully or not (if, for example, the wrong credentials were provided), run:

```
 kubectl describe --help
```

If everything looks fine, but Fortify Software Security Center does not run as expected, and logs alone do not provide enough information, run the following to

inspect the container file system, check the state of the environment, and perform advanced debugging tasks:

```
kubectl exec -it <pod_name> bash
```

This enables you to interactively browse the container, print other internal logs (Tomcat or the Fortify Software Security Center itself, and run other commands.

Other Troubleshooting Resources

For a visual guide to troubleshooting your deployment, see "A visual guide on troubleshooting Kubernetes deployments" (https://learnk8s.io/troubleshooting-deployments). For guidance on debugging common containerized application issues, see "Troubleshooting Applications" (https://kubernetes.io/docs/tasks/debug/debug-application).

About the <fortify.home> Directory

The *<fortify.home>* directory is where the configuration file and other Fortify Software Security Center resources reside.

Default Directory Locations

After Fortify Software Security Center deployment, you can find `<fortify.home>` in the following locations:

- `%USERPROFILE%\.fortify` on a Windows system (applies to both a standard user and a Windows service user)

  Note: `%USERPROFILE%` represents the user running the Tomcat service, which is not necessarily the user who installed Tomcat.

  ```
  Named Account = C:\Users\<username>
  LocalSystem [Default] = %WinDir%\System32\config\systemprofile
  LocalService = %WinDir%\ServiceProfiles\LocalService
  NetworkService = %WinDir%\ServiceProfiles\NetworkService
  ```

- `$HOME/.fortify` on a Linux system

Changing the Default Locations

You can override the default <*fortify.home*> directory location by setting the `fortify.home` system property on the JVM used to start the Tomcat Server. For example, you can specify this system property using the `CATALINA_OPTS` environment variable. Alternatively, you can add the `fortify.home` property to the **Java Options** field in the Tomcat service definition on a Windows system. For detailed information on setting Java system properties, see the Tomcat documentation.

Example: `-Dfortify.home=/home/fortify`

Note: If you want to change the `<fortify.home>` directory location after Fortify Software Security Center has already been configured (see "Configuring Fortify Software Security Center for the First Time" on page 72), make sure that you copy or move the contents of the existing `<fortify.home>` directory to the new location before you restart the server with the updated `fortify.home` system property value.

Directory Contents

The *<fortify.home>* directory is structured as follows:

```
<fortify.home>/
    <app_context>/
         conf/
              app.properties
              datasource.properties
              log4j2.xml
              version.properties
              secret.key
         logs/
              ssc.log
              ...
         init.token

               ...

         plugin-framework/

               /logs

     fortify.license
```

where

<app_context>	represents the application server context in which Fortify Software Security Center is deployed. For details, see "Automating Fortify Software Security Center Configuration" on page 435.
log4j2.xml	is the default log configuration. Although you can change this configuration manually, Fortify strongly recommends that you use the log4j2 configuration override feature instead (see "Customizing Fortify Software Security Center Logging " on page 167).
init.token	represents a new security token that is generated each time the Setup wizard is loaded (start of server in configuration mode). The user who configures Fortify Software Security Center uses this token to access the Setup wizard at the *<host>*:*<port>*/init URL.
app.properties	is a file that contains the application properties that the customer can configure.

`datasource.properties`	is a file that contains the database connection properties.
`version.properties`	is a file that stores information about current and previous versions of Fortify Software Security Center for application upgrade purposes.
`secret.key`	is an encryption key file used to encrypt and decrypt sensitive configuration information in Fortify Software Security Center. (Fortify Software Security Center never overwrites this file. However, the file is generated if it is missing from the `<fortify.home>/<app_context>/conf` directory.) The `datasource.properties` file and some database fields contain encrypted entries that rely on the `secret.key` file. If you move your Fortify Software Security Center instance from one computer to another, you must also move the `secret.key` file (not just your database files).
`plugin-framework`	is the plugin framework configuration and temporary storage (internal). **Note:** If you encounter a problem with a plugin, you can usually find more detailed information about it in `plugin-framework/logs` than you can in main Fortify Software Security Center logs.
`fortify.license`	is the license file for Fortify Software Security Center.

Important! The `<fortify.home>/<app_context>/conf` directory must always contain the following files:
- `app.properties`
- `datasource.properties`
- `secret.key`
- `version.properties`

If any one of these files is missing, Fortify Software Security Center either runs auto-configuration, or starts the Setup wizard to re-create any missing files.

About the Fortify Software Security Center Database

If you are deploying a new instance of Fortify Software Security Center, you must first install and configure the third-party database server software.

Important! Fortify Software Security Center requires that all database schema collations be *case-sensitive*.

Important! If you are installing a SQL Server or MySQL database, your installation requires special attention. For more information, see "Using a Microsoft SQL Server Database" on page 64 or "Configuring a MySQL Database" on page 65.

Later, after you go on to Fortify Software Security Center for the first time, you will use the Fortify Software Security Center Setup wizard to configure connectivity to the database and then seed the database. (See "Configuring Fortify Software Security Center for the First Time" on page 72.)

Topics covered in this section:

About JDBC Drivers

The JDBC drivers for SQL Server, MySQL server, and Oracle are bundled with Fortify Software Security Center software.

The MariaDB JDBC driver is used to connect to the MySQL database server. JDBC URL parameters must use MariaDB driver syntax. Note that the MariaDB is not supported as the back end database for Fortify Software Security Center.

About Fortify Software Security Center Database Character Set Support

For a list of the supported character sets for each third-party database type that Fortify Software Security Center supports, see the *Micro Focus Fortify Software*

System Requirements document.

Installing and Configuring the Database Server Software

Install and configure the database server software following the instructions in the documentation for your database software.

For information about supported databases, see the *Micro Focus Fortify Software System Requirements* document.

Monitoring Disk I/O

Disk I/O encompasses the input/output operations on a physical disk. If you are reading data from a file on a disk, the processor must wait for the file to be read (the same applies to writing data to a file). Fortify Software Security Center performs I/O-intensive database operations, which affects performance. Make sure that your disk subsystem provides low read/write latency. Fortify recommends that you monitor disk I/O as the database grows.

Database User Account Privileges

Fortify strongly recommends that you create accounts for users who perform the following tasks on the Fortify Software Security Center database:

- **Perform runtime tasks**

  A user who performs runtime tasks requires privileges to do the following:
  - Perform Data Manipulation Language (DML) operations to SELECT, UPDATE, INSERT, and DELETE data in all the database tables and views
  - Execute stored procedures.
- **Execute migration scripts**

  Important! Fortify strongly recommends that you create a separate user account to be used for executing migration scripts.

  A user who executes migration scripts requires privileges to do the following:
  - Perform Data Manipulation Language (DML) operations to SELECT, UPDATE, INSERT, and DELETE data in all the database tables and views
  - Execute stored procedures
  - Perform Data Definition Language (DDL) operations to CREATE, ALTER, and DROP database tables, views, and indexes.
  - For Oracle databases, permission to enable sequences.
- **Create and manage the database**

Important! Fortify strongly recommends that you create a separate user account to be used to create and manage the database.

A user who creates and manages the database requires privileges to do the following:

- Perform all the tasks for which the user who executes migration scripts has privileges.
- Create a Fortify Software Security Center database in a dedicated instance.
- Back up and then update the existing Fortify Software Security Center dedicated database instance.
- Bind a Fortify Software Security Center user account to the dedicated database instance.
- Assign a Fortify Software Security Center user account the read-write privileges required to create, initialize, and manage the Fortify Software Security Center database. At a minimum, this user must have a database account that enables the web application to connect to the database.

- **Create and generate reports**
  To add an extra measure of security to reporting, create a database user account with read-only access to the Fortify Software Security Center database, and then use the account credentials to configure enhanced security for your BIRT reports (see "Configuring Security for BIRT Reporting" on page 96).

Database-Specific Configuration Requirements

The following topics describe the configuration requirements for the Fortify Software Security Center-supported third-party databases and how to configure the databases to work with Fortify Software Security Center.

Using a Microsoft SQL Server Database

If you are using a SQL Server database as the Fortify Software Security Center database, perform the following checks:

- Enable the Auto Update Stats Asynchronously (`AUTO_UPDATE_STATISTICS_ASYNC`) option for the database. For instructions, see the Microsoft SQL documentation website (https://docs.microsoft.com/en-us/sql/?view=sql-server-ver15).
- Make sure that your SQL Server database schema collation is *case-sensitive*. The default installation of SQL Server is *case-insensitive*.

Caution! Fortify Software Security Center requires that all database schema collations be *case-sensitive*. If your database schema collation is *case-insensitive*, Fortify Software Security Center does not work correctly.

Important! Before you run the Fortify-provided SQL scripts, verify that there are no open connections to the database.

- Make sure that snapshot isolation is enabled (`ALLOW_SNAPSHOT_ISOLATION` and `READ_COMMITTED_SNAPSHOT` are set to `ON`) on the database schema used for the installation.
- During SQL script executions, check the client tool to make sure that its ANSI null default option is set to `ON`. To do this, you can either use a `SET` command (set `ANSI_NULL_DFLT_ON` to `ON`) or the Query Editor.

Windows Domain Authentication

For Windows domain authentication, you must perform the following additional steps before you deploy Fortify Software Security Center:

1. Make sure that you add `integratedSecurity=true` to the JDBC URL.
2. Obtain the `mssql-jdbc_auth-<version>-<arch>.dll` file. For more information, see https://docs.microsoft.com/en-us/sql/connect/jdbc/building-the-connection-url?view=sqlserver-ver15#Connectingintegrated.
3. Place the `mssql-jdbc_auth-<version>-<arch>.dll` file in the directory specified for the `-Djava.library.path` parameter of the `JDK_JAVA_OPTIONS` environment variable.
4. Place the `mssql-jdbc_auth-<version>-<arch>.dll`: file in a directory that is included in the `PATH` environment variable (for example, `C:\Windows\System32`).
5. Next, do one of the following:
   - Use the `ssc.autoconfig` file to configure Fortify Software Security Center.
   - Configure Fortify Software Security Center with SQL authentication, and then remove the `db.username` and `db.password` parameters from the `datasource.properties` file.
6. Check to make sure that Tomcat is running with the domain account you want to use to connect to the database.

Configuring a MySQL Database

If you are using MySQL as the Fortify Software Security Center database, you must configure the MySQL options file.

Caution! Fortify Software Security Center requires that all database schema collations be *case-sensitive*. If your installation is *case-insensitive*, Fortify Software Security Center cannot work correctly.

Note: For information about the supported versions of MySQL, see the *Fortify Software System Requirements* document.

Tip: If you use SSL to connect Fortify Software Security Center to MySQL, Fortify recommends that you increase the allowed number of concurrent client connections by increasing the value of the `max_connections` system variable (in the `my.cnf` file). This can prevent the `Too many connections` error from occurring.

To configure the MySQL 8.0 options file:

1. Stop MySQL server.
2. Navigate to the MySQL server installation directory.
3. Open the MySQL options file in a text editor.

   Tip: To locate the options files and the order in which they are read, run the following command from a terminal: `mysql --help`.

   - On Windows systems, the default options file is `my.ini`.

     Note: The default location for MySQL 8.0 is `c:\ProgramData\MySQL\MySQLServer 8.0`.

   - On Linux systems, the default options file is `my.cnf`.
4. In both the `[mysqld]` and `[mysqldump]` sections, set `max_allowed_packet` to `1G`. If the `[mysqldump]` section is not there, create it.
5. In the `[mysqld]` section, configure the settings in the following table. If a listed setting is not included in the file, add it.

Setting	Value
`default_storage_engine`	INNODB
`innodb_buffer_pool_size`	`512M` (Fortify recommends `10GB` or more) The best performance is achieved when all data and indexes fit. Together with per-connection memory, the `innodb_lock_wait_timeout` value must not exceed the total available memory on the server. You can roughly estimate the maximum memory usage as follows: `max_connections * max_allowed_packet + innodb_buffer_pool_size` An `innodb_buffer_pool_size` value of between 60 and 80 percent of available memory is appropriate. The larger the `innodb_buffer_pool_size` value, the less disk I/O

Setting	Value
	is needed to access data in tables. On a dedicated database server, you may set this to up to 80% of the machine physical memory size. However, be prepared to scale back this value if you see any of the following: • Competition for physical memory causes paging in the operating system. • InnoDB reserves additional memory for buffers and control structures, so that the total allocated space is approximately 10% greater than the specified size. • The address space must be contiguous, which can cause problems on Windows systems with DLLs that load at specific addresses. • The time to initialize the buffer pool is roughly proportional to its size. On large installations, this initialization time may be extensive. For example, on a modern Linux x86_64 server, initialization of a 10 GB buffer pool takes approximately 6 seconds. See the MySQL 8.0 Reference Manual (https://dev.mysql.com/doc/refman/8.0/en).
`innodb_lock_wait_timeout`	`300` (recommended) Expressed in seconds
innodb_log_file_size	512M
`max_allowed_packet`	1G
`sql-mode`	`"TRADITIONAL"`

6. Save the file, and then restart MySQL server.

Configuring an Oracle Database

This section provides information about how to configure an Oracle database to prevent database-related errors.

Preventing the "No more data to read from socket" Error

If you use Oracle as the Fortify Software Security Center database, you might see an exception of the type "No more data to read from socket."

One possible solution to this exception is to do the following:

1. Navigate to the `$ORACLE_HOME/network/admin/` directory.
2. Open the `tnsnames.ora` file in a text editor.
3. Set the value of `SERVER` to `DEDICATE`.
4. To apply the change, restart the active listener associated with the database.

Partitioning an Oracle Database for Improved Performance

The high input and output associated with large volumes of data in an Oracle database can prevent the database server from effectively operating on data. Database partitioning enhances database server performance, improving data manageability and availability. (The `partitioning.sql` script partitions ISSUE, SCAN_ISSUE, and ISSUECACHE tables using Oracle hash partitions.)

Preparing to Partition an Oracle Database

Before you run the `partitioning.sql` script, do the following:

1. Back up your database.
2. Create auxiliary tablespace. (To determine the auxiliary tablespace size required, you can run the `partitioning.sql` script.
3. Determine how many partitions best fit your data.

   Partitioning is based on application version ID. You want your records distributed evenly across hash partitions. Ideally, you would specify as many partitions as you have application versions. The number of partitions must also allow for the number of application versions to grow.

   Try to achieve record distribution that does not exceed a couple hundred thousand records per partition. Fortify recommends a record distribution of less than one million records per partition.
4. Schedule enough application downtime to partition data. In doing so, consider the time required to:
   - Partition the database

     Important! The maximum possible number of partitions supported is 700. If you request more than this, the Oracle partitioning script fails.

- Move your data to the auxiliary tablespace
- Move your data back to the original tablespace

Partitioning the Database

To use the partitioning script:

- Use Oracle SQL*Plus client to run the Oracle partitioning script (`partitioning.sql`), which is located in the `<ssc_distribution>/sql/oracle/extra` directory.

Note: Script execution time depends on the size of your database.

During script execution:

- Required parameters are obtained from standard input.
- Partitioned tables are created in auxiliary tablespace (with *_PART name).
- Data is moved from the original tablespace to the auxiliary tablespace and partitioned tables
- New partitioned indexes are created on partitioned tables (with *_PART name).
- The original tables and indexes are renamed (with *_NPART name).
- The original names of the partitioned tables and indexes are restored (*_PART name is removed).
- The original tables (*_NPART) are dropped.
- The partitioned tables are moved back to the original tablespace.

Increasing the Number of Job Execution Threads

After you partition your database, make sure that you increase the number of job execution threads, as follows:

1. Navigate to `<fortify_home>/<context>/conf`, and open the `app.properties` file in a text editor.
2. Increase the value of the `jobs.threadCount` property.

   Note: In testing, increasing the value of `jobs.threadCount` to 18 noticeably improved performance.

3. Save and close the `app.properties` file.

About the Fortify Software Security Center Database Tables and Schema

The Fortify Software Security Center installation directory contains an initialization script for each supported third-party database type. During initial configuration (see

"Configuring Fortify Software Security Center for the First Time" on page 72), run this script for your database type to create the database tables and initialize the database schema for Fortify Software Security Center.

Before you configure Fortify Software Security Center for the first time, make sure that you review the information contained in the following sections:

- "Database User Account Privileges" on page 63
- "Database-Specific Configuration Requirements" on page 64

About Seeding the Fortify Software Security Center Database

When you log in to Fortify Software Security Center for the first time, Fortify Software Security Center requires a minimum set of data to process your initial login credentials and to provide basic functionality. Seeding creates the minimum data set for a new database.

Seeding the Fortify Software Security Center database is necessary to maintain a consistent post-installation configuration. This includes the creation of the default administrator user account, as well as required entities such as issue templates, report definitions, and other default data required to make Fortify Software Security Center operational.

Fortify Software Security Center requires two of the downloaded seed bundles (see "Unpacking and Deploying Fortify Software Security Center Software" on page 50):

- The issue template seed bundle (`Fortify_Process_Seed_Bundle-2023_Q1_<build>.zip`) provides a default admin user account and issue template data.
- The report seed bundle (`Fortify_Report_Seed_Bundle-2023_Q1_<build>.zip`) provides the default set of Fortify Software Security Center reports.

You can also install the optional PCI Basic bundles `Fortify_PCI_Basic_Seed_Bundle-2023_Q1_<build>.zip` and `Fortify_PCI_SSF_Basic_Seed_Bundle-2023_Q1_<build>.zip`), which add Payment Card Industry process templates and associated reports to the default set of Fortify Software Security Center templates and reports.

The seed bundle files are included in the Fortify Software Security Center installation package. After your initial Fortify Software Security Center deployment, you can download off-cycle seed bundles from the Fortify Support Portal (https://support.fortify.com) under the **PREMIUM CONTENT** > **FORTIFY EXCHANGE**. (Quarterly security content releases can also include updated seed bundles.)

Caution! Only load the bundles shipped with a Fortify Software Security Center release into a Fortify Software Security Center instance of that same version (either a fresh install or an older instance upgraded to the current version).

After you finish seeding the database, you can modify any user-configurable data entities that were created in the seeding process from the Fortify Software Security

Center user interface. For more information, see "Additional Fortify Software Security Center Configuration" on page 82.

See Also

"Seeding the Database with Report Seed Bundles Delivered with Quarterly Security Content Releases" on page 204

Permanently Deleting a Fortify Software Security Center Database

If, at some point, you plan to remove Fortify Software Security Center altogether, you can remove the Fortify Software Security Center database. To permanently delete a Fortify Software Security Center database schema along with all the data in the database, you run the `drop-tables.sql` script.

Caution! Running the `drop-tables.sql` script permanently removes the Fortify Software Security Center database schema and all the data in the database. Make sure you have backed up any data you want to save before running this script.

To delete the Fortify Software Security Center database schema and all the data in the database:

1. Navigate to the `<ssc_install_dir>/sql` directory, and open the subdirectory for the third-party database you plan to use with Fortify Software Security Center:
   - `mysql`
   - `Oracle`
   - `sqlserver`
2. Copy the `drop-tables.sql` script from the subdirectory that matches your Fortify Software Security Center database type to the database server or other location where you will run the script.
3. In the database client program, log into the database account you created for use with Fortify Software Security Center.
4. Review the warning in the introduction to this topic.
5. Remove the Fortify Software Security Center database schema and all the data in the database by running the following script:

   ```
   drop-tables.sql
   ```

Chapter 4: Configuring Fortify Software Security Center for the First Time

After you deploy Fortify Software Security Center for the first time and then enter the Fortify Software Security Center URL in a browser window, the Fortify Software Security Center Setup wizard (Setup wizard) opens. Here, you can complete the steps for the initial server configuration. The Setup wizard is available to administrators only after you first deploy Fortify Software Security Center, after you upgrade it, or after you place Fortify Software Security Center in maintenance mode (see "Placing Fortify Software Security Center in Maintenance Mode" on page 185).

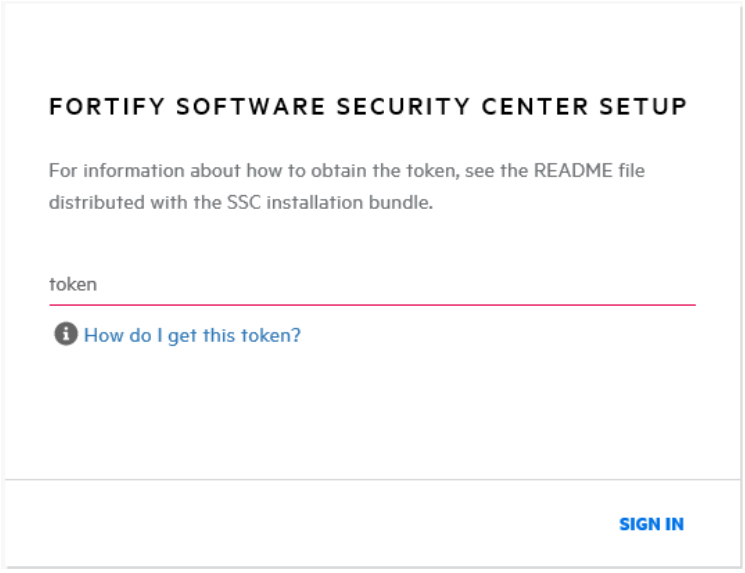
To configure Fortify Software Security Center for the first time:

1. After you deploy a new version of the Fortify Software Security Center WAR file in Tomcat Server, open a browser window and type your Fortify Software Security Center server URL (`https://<host_IP>:<port>/<app_context>/`).

   Note: For a normal deployment, the default Fortify Software Security Center URL is `<protocol>://<ssc_host>:<port>/ssc`. For a deployment to a Kubernetes cluster, the default URL is `<protocol>://<ssc_host>:<port>/` (without `ssc` at the end).

   If you deploy Fortify Software Security Center using a distributed WAR file without renaming the `ssc.war` file, `app_context` will be `ssc` unless it is overwritten by the Tomcat server configuration.

2. In the upper right corner of the web page, click **ADMINISTRATORS**.



3. Go to the `<fortify.home><app_context>` directory (see "About the <fortify.home> Directory" on page 59), and open the `init.token` file in a text editor. (If Tomcat is running as Windows service, then you can find the `init.token` file in `%SystemRoot%\System32\config\systemprofile\.fortify\ssc\init.token`).
4. Copy the contents of the `init.token` file to the clipboard.
5. On the web page, paste the string you copied from the `init.token` file into the text box, and then click **SIGN IN**.
6. Read the information on the **START** page of the Fortify Software Security Center Setup wizard, and then click **NEXT**.
7. On the **CONFIGURATION** step, under **UPLOAD FORTIFY LICENSE**, do the following:
   a. Click **UPLOAD**.
   b. Browse to and select your `fortify.license` file, and then click **UPLOAD**.

   If the license you entered is invalid or expired, Fortify Software Security Center displays a message to that effect.

   The right pane displays the default path of the configuration directory in which your configuration files (`app.properties`, `datasource.properties` and `version.properties`) are to reside.
8. Read the warning note about sensitive information in the configuration file directory. For information on how to change the location of this directory, see "About the <fortify.home> Directory" on page 59.
9. Select the **I have read and understood this warning** check box, and then click **NEXT**.

10. On the **CORE CONFIGURATION SETTINGS** step, do the following:
    a. In the **FORTIFY SOFTWARE SECURITY CENTER URL** box, type the URL for your Fortify Software Security Center server.
    b. In the center pane, select the **Enable HTTP host header validation** check box to ensure that the HTTP Host header value matches the value configured in the Fortify Software Security Center URL (`host.url` property). Both the host and port must match. This affects both browsers and direct REST APIs access. If validation is turned off, any HTTP Host header can access Fortify Software Security Center.
    c. To enable global searches in Fortify Software Security Center, in the GLOBAL SEARCH pane, select the **Enable global search** check box.
    d. The text box below the check box displays the default location for the search index files. If you prefer a different location, type a different directory path for your search index files. (Passwords are *not* indexed.)

    Note: The optimum disk size for the requisite indexing for global searches varies based on the characteristics of the data, but the Lucene indexes are much smaller than the data in the database. For example, the index size required for a database issue volume of 18 GB (with db indexes) is approximately 2 GB.

    Note: Because indexed data can include sensitive information (user names, email addresses, vulnerability categories, issue file names, and so on), make sure that you select a secure location to which only Tomcat Server user has read and write access.

    e. Read the warning in the GLOBAL SEARCH pane, and then select the **I have read and understood this warning** check box.
11. Click **NEXT**.
12. On the **DATABASE SETUP** step, do the following:
    a. In the **DATABASE TYPE** box, select the database type you are using with Fortify Software Security Center.
    b. In the **DATABASE USERNAME** box, type the username for your Fortify Software Security Center database. For more information, see "Database User Account Privileges" on page 63.
    c. In the **DATABASE PASSWORD** box, type the password for your Fortify Software Security Center database account.

    Note: Make sure that the database user credentials specified in the **DATABASE USERNAME** and **DATABASE PASSWORD** boxes are for a user account that has the privileges required to execute migration scripts. These privileges are described in "Database User Account Privileges" on page 63.

d. In the **JDBC URL** box, type the URL for the Fortify Software Security Center, keeping in mind the following:

   For MySQL databases -

   - If MySQL server is configured to use the `sha256_password` or the `caching_sha2_password` authentication plugin, you must provide the server RSA public key to the JDBC driver with the serverRsaPublicKeyFile option. Alternatively, you can use the less secure allowPublicKeyRetrieval option. For more detail, see the MariaDB Connector/J and MySQL server documentation (`https://mariadb.com/kb/en/mariadb-connector-j` and`https://dev.mysql.com/doc`).
   - If you are using a MySQL Server database, you must add the following to the end of the URL:
     - `rewriteBatchedStatements=true`
     - `sessionVariables=collation_connection=COLLATION`

     where `COLLATION` represents the collation type of your database

     Examples:

     ```
     jdbc:mysql://localhost:3306/ssc?sessionVariables=collation_connection=utf8_bin&rewriteBatchedStatements=true
     jdbc:mysql://localhost:3306/ssc?sessionVariables=collation_connection=latin1_general_cs&rewriteBatchedStatements=true
     ```

     MariaDB JDBC driver is used to connect to the MySQL database server. Any additional JDBC URL parameters must use MariaDB driver syntax.

   For MSSQL Server databases -

   - If you are using a MSSQL Server database, you must add the following property setting to the end of the URL:

     ```
     sendStringParametersAsUnicode=false
     jdbc:sqlserver://<host>:1433;database=<database_name>;sendStringParametersAsUnicode=false
     ```

     Caution! Fortify Software Security Center ships with a MSSQL JDBC Driver version that requires an encrypted connection and a trusted server certificate by default. If the connection fails as a result of certificate verification, Fortify recommends that you provide the trust store. If providing a trust store is not an option, you can disable trust verification. If the certificate is trusted but the certificate DNS name does not match the database server hostname, use the `hostNameInCertificate` connection property to provide the correct hostname.

     For more information, see `hostNameInCertificate`, `trustServerCertificate`, and `trustStore* JDBC URL` properties in the "Setting the connection properties" article at https://learn.microsoft.com/en-us/sql/connect/jdbc/setting-the-connection-properties.

e. In the **MAXIMUM IDLE CONNECTIONS** box, type the maximum number of idle connections that can remain in the pool. The default value is 50.
f. In the **MAXIMUM ACTIVE CONNECTIONS** box, type the maximum number of active connections that can remain in the pool. The default value is 100.
g. In the **MAXIMUM WAIT TIME (MS)** box, type the maximum number of milliseconds for the pool to wait for a connection (when no connections are available) before the system throws an exception. The default value is 60000. To extend the wait indefinitely, set the value to zero (0).
h. To test your settings, click **TEST CONNECTION**. Fortify Software Security Center displays a message to indicate whether the test was successful.

Note: If the connection test fails, check the `ssc.log` file (`<fortify.home>/<app_context>/logs` directory) to determine the cause.

13. Before you continue on to the **DATABASE SEEDING** step, run the `create-tables.sql` script. For instructions, see "About the Fortify Software Security Center Database Tables and Schema" on page 69.

Note: If you automate Fortify Software Security Center configuration and you have enabled database migration in the `<app_context>.autoconfig` file, you do not need to run the `create-tables.sql` script. For information about how to automate Fortify Software Security Center configuration, see "Automating Fortify Software Security Center Configuration" on page 435.

14. After you initialize the database, click **NEXT**.
15. (Linux only) If you are using OpenJDK, make sure that you install DejaVu sans fonts and DejaVu serif fonts on the server. You can download these fonts from https://github.com/dejavu-fonts/dejavu-fonts. Without these fonts, Fortify Software Security Center cannot successfully generate reports.
16. On the **DATABASE SEEDING** step, do the following:
    a. In the left pane, use **BROWSE** to locate and select your `Fortify_Process_Seed_Bundle-2023_Q1_<build>.zip` file, and then click **SEED DATABASE**.
    b. Use **BROWSE** to locate and select your `Fortify_Report_Seed_Bundle-2023_Q1_<build>.zip` file, and then click **SEED DATABASE**.
    c. (Optional) Use **BROWSE** to locate and select your `Fortify_PCI_SSF_Basic_Seed_Bundle-2023_Q1_<build>.zip` file, and then click **SEED DATABASE**.

Note: Use the PCI SSF Basic seed bundle to begin to understand how software security issues can affect evaluation under these new PCI SSF standards. For more information, see "Unpacking and Deploying Fortify Software Security Center Software" on page 50.

    d. (Optional) Use **BROWSE** to locate and select your `Fortify_PCI_Basic_Seed_Bundle-2023_Q1_<build>.zip` file, and then click **SEED DATABASE**.

For descriptions of the available seed bundles, see "Unpacking and Deploying Fortify Software Security Center Software" on page 50.

17. Click **NEXT**.
18. Click **FINISH**.
19. Restart Tomcat Server.

After you finish the initial Fortify Software Security Center configuration, complete the configuration of the core parameters and configure additional settings in the ADMINISTRATION view. (For information about the ADMINISTRATION view, see "Additional Fortify Software Security Center Configuration" on page 82.)

Note: If you later find that you need to change any of the configuration settings, you can place Fortify Software Security Center in maintenance mode, and then make any necessary changes. For instructions on how to place Fortify Software Security Center in maintenance mode, see "Placing Fortify Software Security Center in Maintenance Mode" on page 185.

See Also

"Configuring Fortify Software Security Center After an Upgrade" on page 198

Chapter 5: Logging in to Fortify Software Security Center

After you create and initialize your Fortify Software Security Center database, configure Tomcat Server, and deploy Fortify Software Security Center in Tomcat, you can log in to Fortify Software Security Center.

Important! After you log in, create at least one non-default administrator account, and then delete the default administrator account. For more information about how to manage Fortify Software Security Center user accounts and roles, see "About Fortify Software Security Center User Administration" on page 179.

To log in to Fortify Software Security Center:

1. In a web browser, type the URL for your Fortify Software Security Center instance.

   Note: For a normal deployment, the default Fortify Software Security Center URL is `https://<ssc_host>:<port>/ssc`. For a deployment to a Kubernetes cluster, the default URL is `https://<ssc_host>:<port>/` (without `ssc` at the end).

2. Type your username and password.

   If you are logging on to Fortify Software Security Center for the first time, type **admin** in both the **Username** and **Password** fields. These are the default credentials for a new installation.

3. Click **LOGIN**.

   If you are logging on to Fortify Software Security Center for the first time, you are prompted to change your password.

4. If Fortify Software Security Center prompts you to change your password, enter a new one. Make sure that you specify a password that does not include your username or common phrases (names, movie or song titles, dates, or number or letter sequences). A combination of three or four unrelated words such as "myredhorsedance" can work well. After your password is evaluated as strong, you can save it, and then log in.

See Next

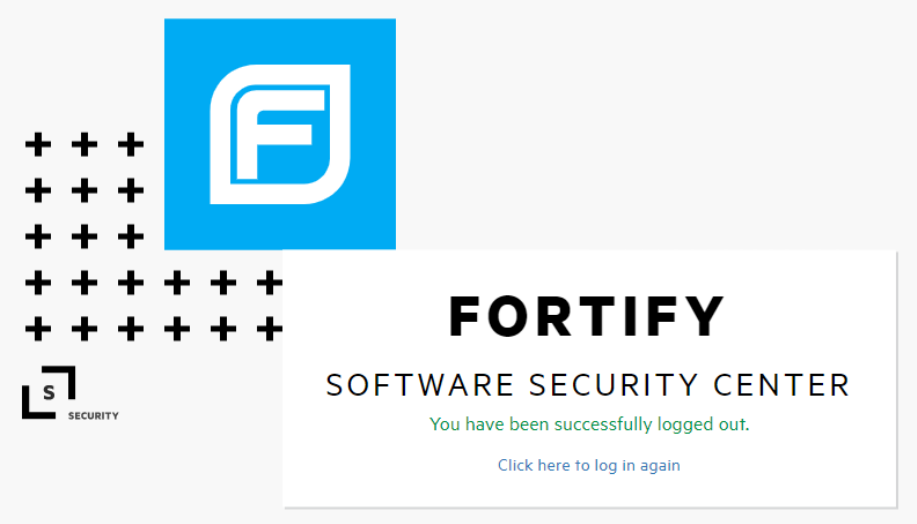
"About Session Logout" on the next page

"Additional Fortify Software Security Center Configuration" on page 82

"Setting the Required Password Strength for Fortify Software Security Center Login" on page 168

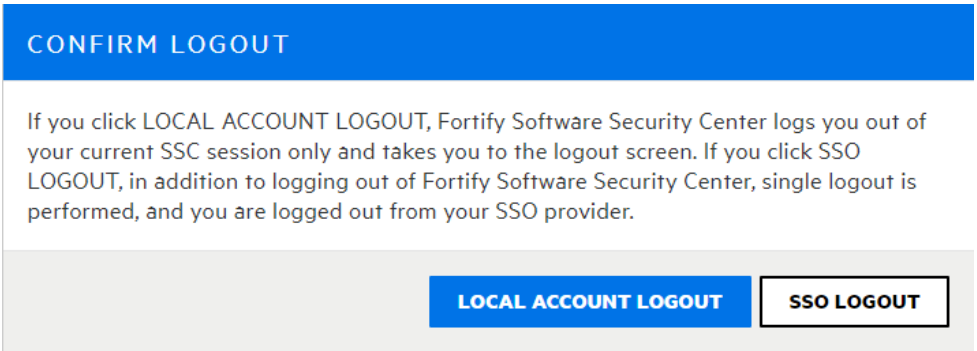
About Session Logout

If you logged in to Fortify Software Security Center using local login (through the login dialog box with username and password to LDAP or local account), and you then log out, Fortify Software Security Center takes you to the logout screen shown here.



If you logged in using an SSO account for which single logout is supported, at logout, you will see a session logout screen that lets you logout from either your local account, or your SSO account.

Note: Fortify Software Security Center supports single logout for Central Authorization Server and for SAML.



If you click **LOCAL ACCOUNT LOGOUT**, Fortify Software Security Center logs you out of your current session only and takes you to the logout screen.

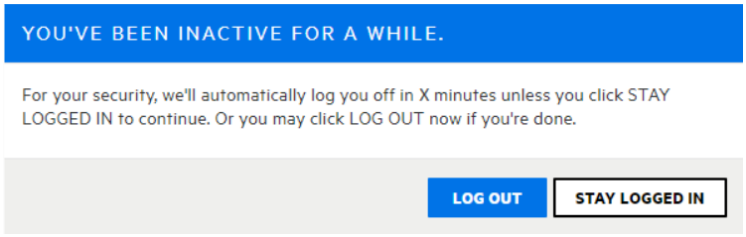
If you click **SSO LOGOUT**, in addition to logging out of Fortify Software Security Center, single logout is performed, and you are logged out from your SSO provider.

Note: To log out of Fortify Software Security Center completely, close all of your browser windows.

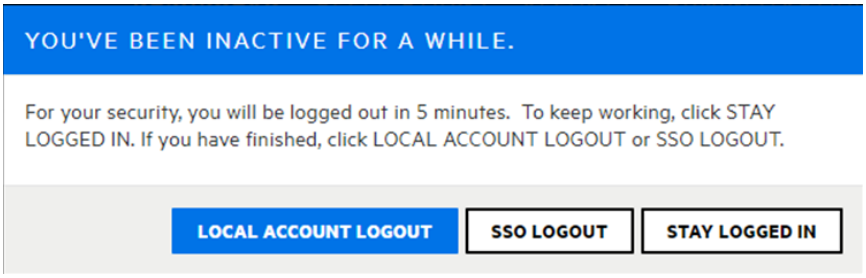
Inactive Session Timeout

If you have been inactive and your Fortify Software Security Center session is about to time out, Fortify Software Security Center displays one of two dialog boxes:

- If you logged in using local login (through the login dialog box with username and password to LDAP or local account), and your session is about to time out, you see a dialog box that lets you either log out or stay logged in.



  If you click **LOG OUT** or your session times out due to further inactivity, Fortify Software Security Center logs you out of the session and takes you to the logout screen.
- If you are logged on to Fortify Software Security Center through an SSO provider for which single logout is supported, you see a dialog box that lets you log out of your local user account, perform an SSO logout, or stay logged in.



  If you click **LOCAL ACCOUNT LOGOUT** or your session times out due to further inactivity, Fortify Software Security Center logs you out of the SSC session only and then takes you to the logout screen.

  If you click **SSO LOGOUT**, Fortify Software Security Center logs you out of the SSC session, and then logs you out of your SSO provider.

  For information about how to configure session timeout, see "Configuring Core Settings" on page 99.

Note: To log out completely from Fortify Software Security Center, close your browser (all tabs).

Logout Screen

If you logged in to Fortify Software Security Center using local login, the **Click here to log in again** link takes you to the login screen, where you can log in again.

If you logged in to Fortify Software Security Center through an SSO provider, the **Click here to log in again** link initiates SSO login.

Chapter 6: Additional Fortify Software Security Center Configuration

After you finish the preliminary Fortify Software Security Center configuration and deploy the `ssc.war` file, you complete the configuration from the Fortify Software Security Center ADMINISTRATION view.

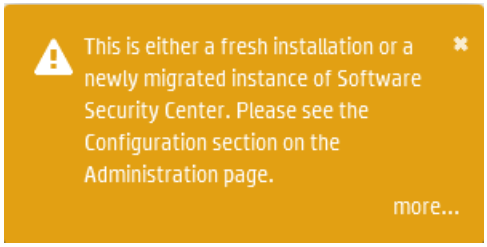
You can configure and update other settings in the ADMINISTRATION view later, as necessary.

Accessing the Configuration Settings in the ADMINISTRATION View

You complete the Fortify Software Security Center configuration from the **Configuration** category in the ADMINISTRATION view.

To access the **Configuration** category:

1. Log in to Fortify Software Security Center as an administrator user. For log-in instructions, see "Logging in to Fortify Software Security Center" on page 78.
2. Do one of the following:
   - If you are accessing Fortify Software Security Center for the first time, a banner similar to the following is displayed at the top of the page. Click **Go** to open the **Configuration** category in the ADMINISTRATION view.

     Otherwise,
     a. On the Fortify header, click **ADMINISTRATION**.

        In the ADMINISTRATION view, the navigation pane on the left displays links to the categories that are available in the ADMINISTRATION view. The Event Logs page is displayed by default.
     b. In the left pane, select **Configuration**.

The pane displays the configuration category options. For information about these options, see "Configuration Options Available in the ADMINISTRATION View" on page 85.

Configuring Issue Stats Thresholds

The Issue Stats dashboard page shows summary information about issues for the application versions on Fortify Software Security Center, including the number of days that it is taking to review and fix them. To provide a visual cue as to how quickly issues are being handled, the Issue Stats page displays colored bars next to the values for the **Average Days to Review** and **Average Days to Remediate**. A green bar indicates that issues are being managed quickly, a red bar indicates that issue management is too slow, and an orange bar indicates that issue management is somewhere between these two extremes.

How Average Days to Review and Average Days to Remediate are Calculated

Before it calculates the **Average Days to Review** and **Average Days to Remediate** values, Fortify Software Security Center applies the following rules:

- Fortify Software Security Center excludes the following issues from its calculations:
  - All issues that were audited or removed 365 days ago or earlier
  - All suppressed issues
  - Issues that have not been either audited or removed
- To calculate issue aging for audited issues, Fortify Software Security Center uses the date and time on which the issue was first audited.
- For issues that were not audited but were removed, Fortify Software Security Center uses the removal date as the audit date.
- To calculate issue dates, Fortify Software Security Center performs the following to clean up dates and times:
  - Adjusts issue found dates and times to 12:00 AM of the date the issues were found.
  - Adjusts issue audited dates and issue removed dates to 12:00 am of next day.

  These adjustments are required to calculate average dates correctly. For example, without these adjustments, the calculated averages would be zero for issues that were found and audited on the same date, which is not correct. For an issue found on March 2 and audited at March 5, the days to review is 5 – 2 + 1, or 4 days.

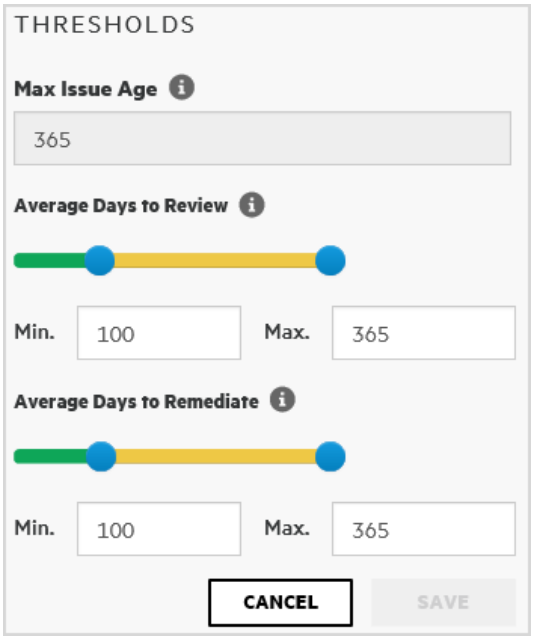
After it applies all of these rules and makes time and date adjustments, Fortify Software Security Center calculates the average of two values—(auditTime - foundDate) and (removedDate - foundDate)—to get average number of days to audit and remediate issues

Setting the Issue Stats Thresholds

You set the thresholds that determine what users see when they review summary information about the application versions to which they have access. By default, the Issue Stats page displays values of fewer than 100 days (minimum) in a green bar, any values greater that 365 days (maximum) in red, and values in between as yellow.

To set the color thresholds for **Average Days to Review** and **Average Days to Remediate**:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, under **Metrics & Tracking**, select **Issue Age**.
   The Issue Age page opens. The minimum and maximum values for **Average Days to Review** and **Average Days to Remediate** are set to 100 and 365, respectively.



3. To reset the thresholds for the average number of days to review Issues, under for **Average Days to Review**, do one of the following:
   - Adjust the slider control.
   - Change the values shown in the **Min.** and **Max.** combo boxes.
4. To reset the thresholds for the average number of days to remediate Issues, under for **Average Days to Remediate**, do one of the following:
   - Adjust the slider control.
   - Change the values shown in the **Min.** and **Max.** combo boxes.
5. Click **SAVE**.

The color coded values on the Issue Stats dashboard page reflect your changes.

Configuration Options Available in the ADMINISTRATION View

The following table lists the configuration options available in the ADMINISTRATION view. (On the Fortify header, select **ADMINISTRATION**. Then, in the left pane, select **Configuration**.)

Note: Changes to some configuration options do not take effect until the system is restarted.

Option	Description	Instructions
AppSec Training	Use to enable and configure application security training. This makes the **GET TRAINING** button available on the issue details section of the AUDIT page.	"Configuring Application Security Training" on page 88
Audit Assistant	Use to enable and configure Audit Assistant, which uses Fortify Scan Analytics to automatically audit Fortify Static Code Analyzer scans.	"Configuring Audit Assistant" on page 90
BIRT Reports	Use to apply enhanced security to reporting in Fortify Software Security Center.	"Configuring Security for BIRT Reporting" on page 96
Core	Use to configure core Fortify Software Security Center settings such as the timeout and lockout settings and the proxy for secure coding Rulepacks updates.	"Configuring Core Settings" on page 99
Email	Use to configure the server settings used to send email alerts to users.	"Configuring Email Alert Notification Settings" on page 102
Issue Audit	Use to select the setting that determines how issue audit conflicts are resolved.	"Setting the Strategy for Resolving Issue Audit Conflicts" on page 105

Option	Description	Instructions
JMS	Use to configure Fortify Software Security Center to publish system events to the Java Message Service (JMS).	"Configuring Java Message Service Settings" on page 107
LDAP Servers	Use to configure LDAP authentication and LDAP server options for one or more LDAP servers.	"Configuring LDAP Servers" on page 111
Maintenance	If, at any time, you need to change any server configuration settings, you can place Fortify Software Security Center in maintenance mode, and then make the necessary changes. From here, you can also pause job execution in preparation for server shutdown.	"Placing Fortify Software Security Center in Maintenance Mode" on page 185
Proxy	Use to configure a single proxy for Rulepack updates, the connection to Audit Assistant, and for bug tracker plugins.	"Configuring a Proxy for Fortify Software Security Center Integrations" on page 132
ScanCentral DAST	Use to configure Fortify Software Security Center to manage and run dynamic scans from the SCANCENTRAL view in Fortify Software Security Center.	"Enabling the Running and Management of ScanCentral DAST Scans from Fortify Software Security Center" on page 135
SCIM	Use to enable SCIM for provisioning of externally-managed users and groups.	"Enabling SCIM for Provisioning of Externally Managed Users and Groups" on page 132
SSO	Use to configure Fortify Software Security Center to work with one of the following SSO solutions:	"Configuring Fortify Software Security Center to Work with Single Sign-On" on page 148

Option	Description	Instructions
	• CAS SSO • SPNEGO/KERBEROS SSO • SAML SSO • HTTP SSO • X.509 SSO	
ScanCentral SAST	Use to configure Fortify Software Security Center to monitor ScanCentral SAST and to display ScanCentral SAST results in the SCANCENTRAL view in Fortify Software Security Center.	"Configuring ScanCentral SAST Monitoring in Fortify Software Security Center" on page 134
Scheduler	Use to configure the Fortify Software Security Center job scheduler settings.	"Configuring Job Scheduler Settings" on page 135
Security	Use to configure the Fortify Software Security Center security features.	"Configuring Browser Access Security for Fortify Software Security Center" on page 146
Seed Bundles	Use to seed the database with seed bundles distributed in a quarterly security content release.	"Seeding the Database with Report Seed Bundles Delivered with Quarterly Security Content Releases" on page 204
Web Services	Use to configure Fortify Software Security Center web services.	"Configuring Web Services to Require Token Authentication" on page 161
Webhooks	Use to create and manage webhooks that keep your systems updated on events that occur in Fortify Software Security Center.	"Creating Webhooks" on page 292

Configuring Application Security Training

If your organization has access to an application security training platform, you can integrate that training with Fortify Software Security Center. After you do, your users can access context-appropriate guidance on the issues they assess and how best to mitigate them as they audit.

To enable application security training on Fortify Software Security Center:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Configuration**, and then select **AppSec Training**.
3. On the AppSec Training page, leave the **Enable Training** check box selected.
4. To determine whether your online training vendor has integrated with Fortify Software Security Center and to obtain the corresponding training URL, contact Fortify Customer Support (https://www.microfocus.com/support).
5. In the **Training URL** box, type your application security training URL.
6. Click **SAVE**.

Users can now see the **GET TRAINING** button in the details section for issues on the AUDIT page. Users can click **GET TRAINING** to go to the application security training website you have specified.

See Also

"Auditing Scan Results" on page 340

About Audit Assistant

Audit Assistant is an optional tool that you can use with Fortify Scan Analytics to help determine whether or not the issues returned from Fortify Static Code Analyzer scan results represent true vulnerabilities. To make its determinations, Audit Assistant needs data to establish a baseline for its audits. This data consists of the decisions users have made during scan audits about how to characterize various issues.

You can use Fortify shared data (pooled, anonymized data from Fortify users and Fortify's security team), or use audit data that your security team has completed. Audit Assistant's assessments of the actual threats that issues represent become more accurate as it receives more training data.

You can submit training data (metadata derived from historical human-audited scan results) without having submitted anything for prediction.

Audit Assistant can also learn through corrections that are included in the training or prediction data set. A correction is registered after a user reviews the prediction Audit Assistant assigned to an issue, disagrees with it, adjusts the value, and then includes the issue in the data set for additional training.

The following sections describe how to obtain an authentication token from Fortify Scan Analytics, and then use that token to configure a connection to Fortify Scan Analytics. Later sections describe how to prepare Scan Analytics for metadata submission, submit data, review Audit Assistant results, and then submit corrected audit data.

See Also

"Configuring Audit Assistant" on the next page

"Enabling Auto-Apply and Auto-Predict for an Application Version" on page 253

"Using Audit Assistant" on page 360

"About Prediction Policies" on page 361

"Defining Prediction Policies" on page 362

"Enabling Metadata Sharing" on page 363

"Submitting Training Data to Audit Assistant" on page 363

"Reviewing Audit Assistant Results" on page 364

Getting a Fortify Scan Analytics Authentication Token

To integrate with Audit Assistant, you must first obtain a Fortify Scan Analytics authentication token.

To obtain a Fortify Scan Analytics authentication token:

1. Log on to Fortify Scan Analytics (https://analytics.fortify.com).
2. On the Fortify header, select **ADMINISTRATION**, and then select **TOKENS**.
3. On the Tokens page, click **+ADD**.
4. In the **Name** box, type a name for the token to generate.
5. Click **SAVE**.
   The Tokens page lists the new token.
6. To the right of the token name, click the view icon ( ).
   The Token window opens.
7. Select and copy the token text, and then click **CLOSE**.

Use the copied token to configure the integration with Audit Assistant. (See "Configuring Audit Assistant" below.)

Configuring Audit Assistant

Audit Assistant works with Fortify Scan Analytics to help determine whether or not the issues returned from Fortify Static Code Analyzer scan results represent true vulnerabilities.

To configure Fortify Software Security Center to use Audit Assistant with your applications:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Configuration**, and then select **Audit Assistant**.
3. Configure the settings on the Audit Assistant page as described in the following table.

Field* Required	Description
Enable Audit Assistant	Select this check box to enable the remaining fields.
* Authentication token	Paste the authentication token you obtained from Fortify Scan Analytics here. For instructions on how to get a token, select **How do I get a token?** or, see "Getting a Fortify Scan Analytics Authentication Token" above.

Field* Required	Description
* Fortify Scan Analytics server URL	Specify the URL for the Fortify Scan Analytics server.
Use SSC proxy for Audit Assistant	If you have configured a proxy for all Fortify Software Security Center integrations (see "Configuring a Proxy for Fortify Software Security Center Integrations" on page 132, you can select this check box to use that proxy for Audit Assistant.

4. To test the connection to the Application Security Analytics server, click **TEST CONNECTION**.

   After the connection is successfully tested, you can go ahead and configure the settings in the **Audit settings** section.
5. Click **REFRESH POLICIES** to populate the **Default prediction policy** list with the current server policies on the Fortify Scan Analytics server.

   Note: Audit Assistant prediction policies set for individual application versions can become invalid if available policies are changed on the Fortify Scan Analytics server. Fortify Software Security Center verifies new policies it receives from Fortify Scan Analytics every time a user clicks **REFRESH POLICIES**.) If Fortify Software Security Center detects one or more invalid policies, it displays a table that shows the mapping from the original policy to the changed policy. You can then identify each obsolete policy and map its valid replacement. Fortify Software Security Center updates the policies based on the changes you submit in the mapping table.
6. From the **Default prediction policy** list, select the name of the prediction policy to apply to all application versions. (Policies are defined in Fortify Scan Analytics.)
7. If you plan to specify prediction policies at the application version level and override the default global prediction policy, select **Enable specific application version policies**. Otherwise, Audit Assistant uses the default global prediction policy you specified in the previous step.

   Note: You can specify the policy for an application version from the APPLICATION PROFILE dialog box. For instructions, see "Configuring Audit Assistant Options for an Application Version" on page 273.
8. To enable Audit Assistant to automatically send issues not yet assessed to Fortify Scan Analytics for assessment, select the **Enable auto-predict** check box. (For information about the auto-predict feature, see "About Audit Assistant

Auto-Prediction" on the next page.)

Note: If you enable auto-predict here, open the APPLICATION PROFILE dialog box for each application version for which you want to use auto-prediction, and enable it there as well.

9. To enable the application of the analysis values that Audit Assistant assesses for issues to your Analysis custom tag values system-wide, select the **Enable auto-apply** check box. After you do, you must enable this functionality on a per-application version project basis from the APPLICATION PROFILE window.

   Note: If you enable auto-apply here, open the APPLICATION PROFILE dialog box for each application version for which you want to use auto-apply, and enable it there as well.

   Important! Before you can use the auto-apply feature, you must first map Audit Assistant analysis tag values to Fortify Software Security Center Analysis tag values.

10. If you selected the **Enable auto-apply** check box, and you want to map Audit Assistant analysis tag values to Fortify Software Security Center Analysis tag values now, click the **here** link to go to the Custom Tags page, and then follow the instructions provided in "Mapping Audit Assistant Analysis Tag Values to Fortify Software Security Center Custom Tag Values" on the next page.
11. Click **SAVE**.

About Audit Assistant Auto-Prediction

You can configure Fortify Software Security Center to send issues for Audit Assistant prediction automatically after FPRs are successfully uploaded and processed. (If you prefer to submit FPRs for prediction manually, then there is no need to configure auto-prediction.)

If both auto-predict and auto-apply are enabled for an application version, then Audit Assistant automatically applies predicted values to custom tags on new issues after prediction is completed. (Audit Assistant prediction results are always applied to an application version, but if auto-apply *is not* enabled, the information is stored only in Audit Assistant-specific tags. If auto-apply *is* enabled, Audit Assistant-specific values are also mapped to other tags, based on the configuration.)

Only unpredicted issues (uncovered by a supported analyzer) found at the end of FPR processing are automatically submitted to Audit Assistant for assessment. Once Audit Assistant has assessed an issue, it does not revisit that issue.

Enabling Auto-prediction

Auto-prediction enablement for an application version is a two-step process. First, an administrator enables it system-wide during Audit Assistant configuration. "Configuring Audit Assistant" on page 90.) After this, users can enable auto-

prediction on a per-application-version basis from the PROFILE window. (See "Enabling Auto-Apply and Auto-Predict for an Application Version" on page 253.)

Mapping Audit Assistant Analysis Tag Values to Fortify Software Security Center Custom Tag Values

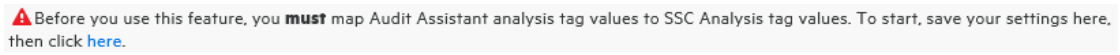
If, when you configured Audit Assistant ("Configuring Audit Assistant" on page 90), you enabled Audit Assistant auto-apply, you must next map Audit Assistant analysis tag values to Fortify Software Security Center custom tag values for one or more list-type custom tags. After you do, you can start using the automated auditing feature.

Note: For Audit Assistant auto-apply to work, you must designate the mapped custom tag as the primary custom tag from the APPLICATION PROFILE dialog box for the application version.

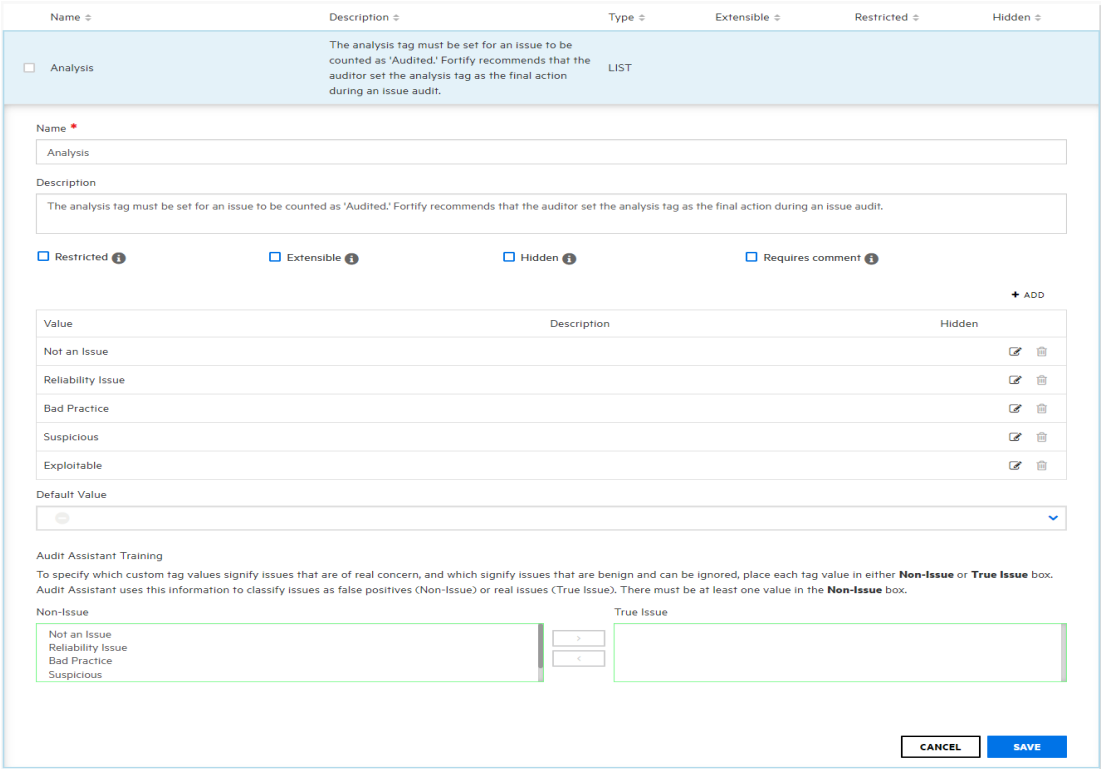
To map Audit Assistant analysis tag values to Fortify Software Security Center list-type custom tag values:

1. After you configure Audit Assistant (and enable Audit Assistant auto-apply), do one of the following:
   - In the left pane of the ADMINISTRATION view, select **Templates**, and then select **Custom Tags**.

   Or

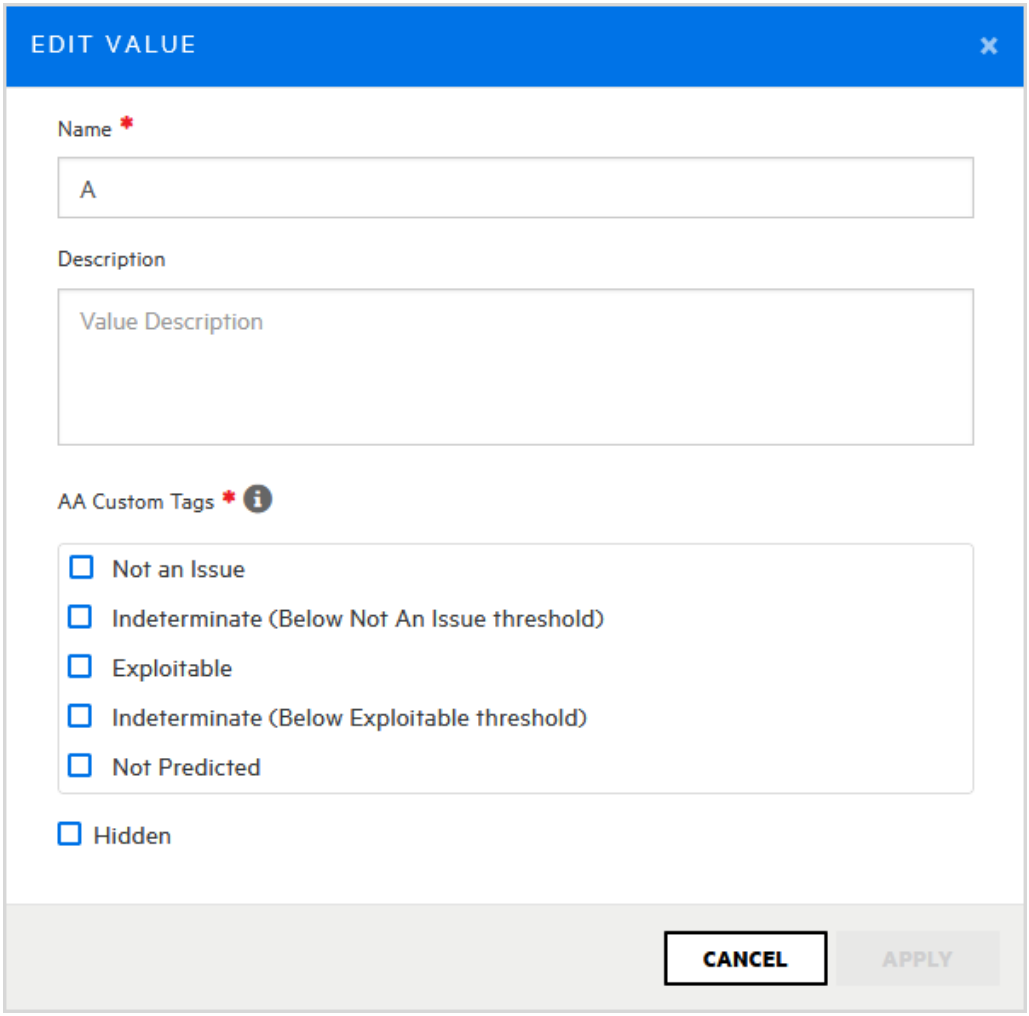
   

   - If you enabled auto-apply, click the **here** link at the bottom of the Audit Assistant page.
2. On the Custom Tags page, expand the row for a list-type custom tag (such as Analysis) for which you want to map values.
3. At the bottom right of the expanded section, click **EDIT**.



The custom tag values listed in the table become editable, and the **Audit Assistant Training** section is visible.

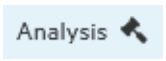
4. In the table of tag values, select the **Edit value** icon (✎) for a listed value.



5. In the EDIT VALUE dialog box, under **AA Custom Tags**, select the check box for the AA custom tag value to map to this custom tag value.
6. Click **APPLY**.

The list of custom tag values now shows the value you just mapped for Audit Assistant.

7. Complete steps 4 through 6 for all of the values that you want to map for automated auditing.
8. Click **SAVE**.



Note that after you save your mapping, Fortify Software Security Center displays a gavel icon to the right of the custom tag name.

Note: The **Audit Assistance Training** section is used for data training purposes. For information about how to configure this section, see "Adding Custom Tags to the System" on page 274.

Configuring Security for BIRT Reporting

You can add an extra measure of security to BIRT reporting by doing one or both of the following:

- Enable the Java security manager
- Limit access to tables and views in the database

Enabling Java Security Manager

To enable Java Security manager:

1. Log in to Fortify Software Security Center as an administrator.
2. On the Fortify header, click **ADMINISTRATION**.
3. In the left pane, select **Configuration**, and then click **BIRT Reports**.
4. On the **BIRT Reports** page, under **Enhanced security**, select the **Turn on security manager** check box.

   Note: If you try to generate a custom report that depends on functionality that the BIRT security manager regards as unsafe, the report generation might fail.

5. Click **SAVE**.

(Linux with OpenJDK only) Installing Required Fonts

If your Fortify Software Security Center is installed on a Linux system, and you are running OpenJDK, you must install fontconfig, DejaVu Sans fonts, and DejaVu serif fonts on the server to enable users to successfully generate reports. Otherwise, report generation will fail. You can download these fonts from https://github.com/dejavu-fonts/dejavu-fonts.

Creating a Database Account for Reporting

To limit write access to tables and views in the database:

1. Create a database user account to use exclusively for BIRT reporting and provide minimum permission required to generate reports.
2. For the new user account, enable read (only) access to the following tables and views:

Tables		
activity	issuecache	reportexecparam
attr	measurement	requirement
auditattachment	measurementhistory	requirementtemplate
auditcomment	metadef	ruledescription
catpackexternalcategory	metadef_t	savedreport
catpackexternallist	metaoption	scan
catpacklookup	metaoption_t	scan_rulepack
datablob	metavalue	seedhistory
documentinfo	metavalueselection	sourcefile
eventlogentry	project	snapshot
f360global	projecttemplate	userpreference
filterset	projectversion	variable
folder	projectversiondependency	variablehistory
foldercountcache	reportexecblob	
Views		
attrlookupview	defaultissueview	ruleview
auditvalueview	metadefview	view_standards
baseissueview	metaoptionview	

3. Log in to Fortify Software Security Center as an administrator.
4. On the Fortify header, click **ADMINISTRATION**.
5. In the left pane, select **Configuration**, and then click **BIRT Reports**.
   Fortify Software Security Center displays the **BIRT Reports** page.
6. In the **DB Username** and **DB Password** boxes, type the credentials for the database account that has read-only database access.

7. To test the database user account access to the database, click **VALIDATE CONNECTION**.
8. Click **SAVE**.

See Also

"Allocating Memory for Report Generation" below

"Setting Report Generation Timeout" below

Allocating Memory for Report Generation

To allocate memory for security for Fortify Software Security Center reports:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Configuration**, and then click **BIRT Reports**.
3. In the **Set up BIRT execution** section, select the default value in the **Maximum heap size (MB)** box, and then type a new value. (For minimum and recommended values for java heap size, see the Micro Focus Fortify Software System Requirements document.)
4. Click **SAVE**.

Setting Report Generation Timeout

To set a report generation timeout value (after which report generation is stopped and set as "failed"):

1. Log in to Fortify Software Security Center as an administrator.
2. On the Fortify header, select **ADMINISTRATION**.
3. In the left pane, select **Configuration**, and then click **BIRT Reports**.
4. Under **Set up BIRT execution**, select the default value in the **Execution timeout (minutes)** box, and then type a new value.
5. Click **SAVE**.

Configuring Core Settings

In addition to the initial configuration you performed on the Setup wizard, you must also configure several core attributes in the **Configuration** section of the ADMINISTRATION view. These attributes include user account timeout and lockout settings, the display of user information, maximum events per Fortify WebInspect Agent issue, the base URL for the runtime event description server, and the user administrator's email address. You also configure the proxy used for Rulepack updates on this page. For information about the Rulepacks updates proxy, see "About Configuring a Proxy for Rulepack Updates" on page 102.

To configure Fortify Software Security Center core settings in the ADMINISTRATION view:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, click **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Configuration**, and then select **Core**.
3. On the Core page, configure the settings described in the following table.

Field	Description
Absolute session timeout (minutes)	Number of minutes a user can be continuously active before Fortify Software Security Center automatically logs a user off. The default value is 240.
Days before password reset	Number of days the Fortify Software Security Center password is valid before the user must change it. The default value is 30.
Login attempts allowed before a user is locked out	Number of times a local user can try to log in to Fortify Software Security Center using invalid credentials before Fortify Software Security Center locks the user's account. If Fortify Software Security Center locks a user out, that user is prevented from attempting a new login for the number of minutes specified in the **Lockout time (minutes)** box. (For information about how to unlock a user account, see "Unlocking Local User Accounts" on page 229. The default value is 3. **Note:** This setting does not apply to LDAP users. If the account lockout threshold was configured using the

Field	Description
	Group Policy editor, the LDAP user account could be locked out in Active Directory if consecutive login attempts have failed.
Lockout time (minutes)	If a user attempts and fails to log in to Fortify Software Security Center the number of times specified for **Login Attempts before Lockout**, Fortify Software Security Center locks the user account for the number of minutes specified in the **Lockout time (minutes)** box. The default value is 30.
User lookup strategy	If LDAP is enabled, select one of the following user lookup strategies from this list: • **Local users first, fallback to LDAP users (compatibility)** Search local users first, then search LDAP users. To avoid potential authorization errors and user confusion, make sure that usernames are not duplicated on the LDAP server and local storage. • **LDAP users first, fallback to local users** Search LDAP users first, then local users. To avoid potential authorization errors and user confusion, make sure that user names are not duplicated on the LDAP server and local storage. • **LDAP users exclusive, fallback to local administrator** (Recommended strategy for SSO) Search LDAP users only, and allow local administrator access.
Display user first/last names and emails in user fields, along with login names	Select this check box to display the following user information, when applicable: login name, first and last names, and email address.
Maximum events per	Determines the maximum number of events to log within a single Fortify WebInspect Agent issue. After that threshold

Field	Description
WebInspect Agent Issue	is reached, new events related to the same issue are ignored. The default value is 5.
Inactive session timeout (minutes)	Type the number of minutes a user can be inactive before Fortify Software Security Center automatically logs the user off. The default value is 30.
Locale for Rulepacks	Type one of the following: • ja (Japanese) • zh_CN (simplified Chinese) • zh_TW (traditional Chinese) • es (Spanish) • pt_BR (Portuguese Brazilian) **Note:** There is no need to specify a value for English.
Rulepack update URL	URL for the Fortify Rulepack update site. **Important!** Do not change the default value of the **Rulepack Update URL** field unless your Fortify Customer Support representative directs you to do so. The default value is `https://update.fortify.com`
Use SSC proxy for Rulepack update	Select this check box to enable the use of the Fortify Software Security Center proxy, if the Rulepack server is behind it. **Note:** The Fortify Software Security Center proxy must be enabled and correctly configured. For information on how to configure a proxy, see "Configuring a Proxy for Fortify Software Security Center Integrations" on page 132.
User	Type the email address of the user who is to receive system email alerts and notifications when email

Field	Description
Administrator's email address (for user account requests)	notifications are enabled. Requests for new user accounts are sent to this address when the **Can't access or need an account**? link is available on the Fortify Software Security Center login page.
Enable export to CSV from the Dashboard and AUDIT views	Select this check box to enable users to export Fortify Software Security Center data to comma-separated values files. **Note:** If you are changing only this property on the Core page, a server restart is not required to implement the change.

4. Click **SAVE**.
5. Restart the server.

See Also

"Unlocking Local User Accounts" on page 229

About Configuring a Proxy for Rulepack Updates

By default, Fortify Software Security Center downloads the current versions of Fortify Secure Coding Rulepacks you subscribe to from the Fortify Customer Portal at https://update.fortify.com.

If your organization uses a proxy to access external resources, Fortify recommends that you configure a proxy for secure coding Rulepacks updates (as well as for bug tracking and, if you use it, Audit Assistant). For instructions on how to configure a single proxy for use with all HTTP(s) protocol-based Fortify Software Security Center integrations, see "Configuring a Proxy for Fortify Software Security Center Integrations" on page 132.

After you configure a single proxy for use with all HTTP(s) protocol-based integrations, you can enable of that proxy for Rulepack update. For instructions, see "Configuring Core Settings" on page 99.

Configuring Email Alert Notification Settings

If you plan to use Fortify Software Security Center to send email alert notifications to your teams, do the following:

1. Create an SMTP email account for Fortify Software Security Center to use.
2. Configure the email settings as described in this topic.

Note: For information about how to enable or disable the receipt of email alerts, see "Enabling and Disabling Receipt of Email Alerts" on the next page.

To configure the settings used for sending email alert notifications, do the following.

Important! If you want to enable team members who do not have an account to request access to Fortify Software Security Center, you must enable and configure the email service settings.

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Configuration**, and then select **Email**.
3. On the Email page, configure the email service attribute settings described in the following table.

Field	Description
Enable email	Select this check box to enable Fortify Software Security Center to send email messages of all types and to add the "Can't access or need an account?" link to the login dialog box. This check box is cleared by default.
From email address	Type the email address that Fortify Software Security Center uses to identify emails sent from Fortify Software Security Center. For example, fortifyserver@example.com.
Default encoding of the email content	Type the encoding method to be used for the email content. The default value is UTF-8.
SMTP server	Type the fully-qualified domain name for the SMTP server. For example, mail.example.com.
SMTP server port	Type the port number for the SMTP server. The default value is 25.
SMTP username	If authentication is required on the SMTP server, type the SMTP username.
SMTP password	If authentication is required on the SMTP server, type

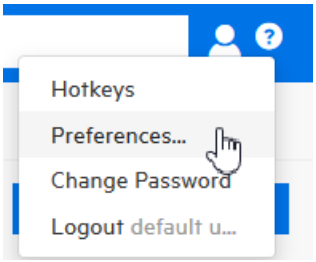
Field	Description
	the SMTP password.
Secure email server connection	Select this check box if you want to configure security for your email server connection.
Enable SSL/TLS encryption	If you selected the **Secure email server connection** check box, then, from this list, select one of the following: • (Optional) If the SMTP server supports it, select **STARTTLS** to upgrade to a TLS/SSL-encrypted SMTP connection. • Select **SSL/TLS Encryption** to enable SSL/TLS encryption when connecting to the SMTP server. • Select **Force STARTTLS** to require an upgrade to TLS/SSL-encrypted SMTP connection. If the SMTP server does not support it, the connection will fail.
Trust the certificate provided by the SMTP server	Select this check box to trust the certificate that the SMTP server provides by skipping certificate validation. **Caution!** For security reasons, Fortify recommends that you leave this check box cleared.

4. Click **SAVE**.

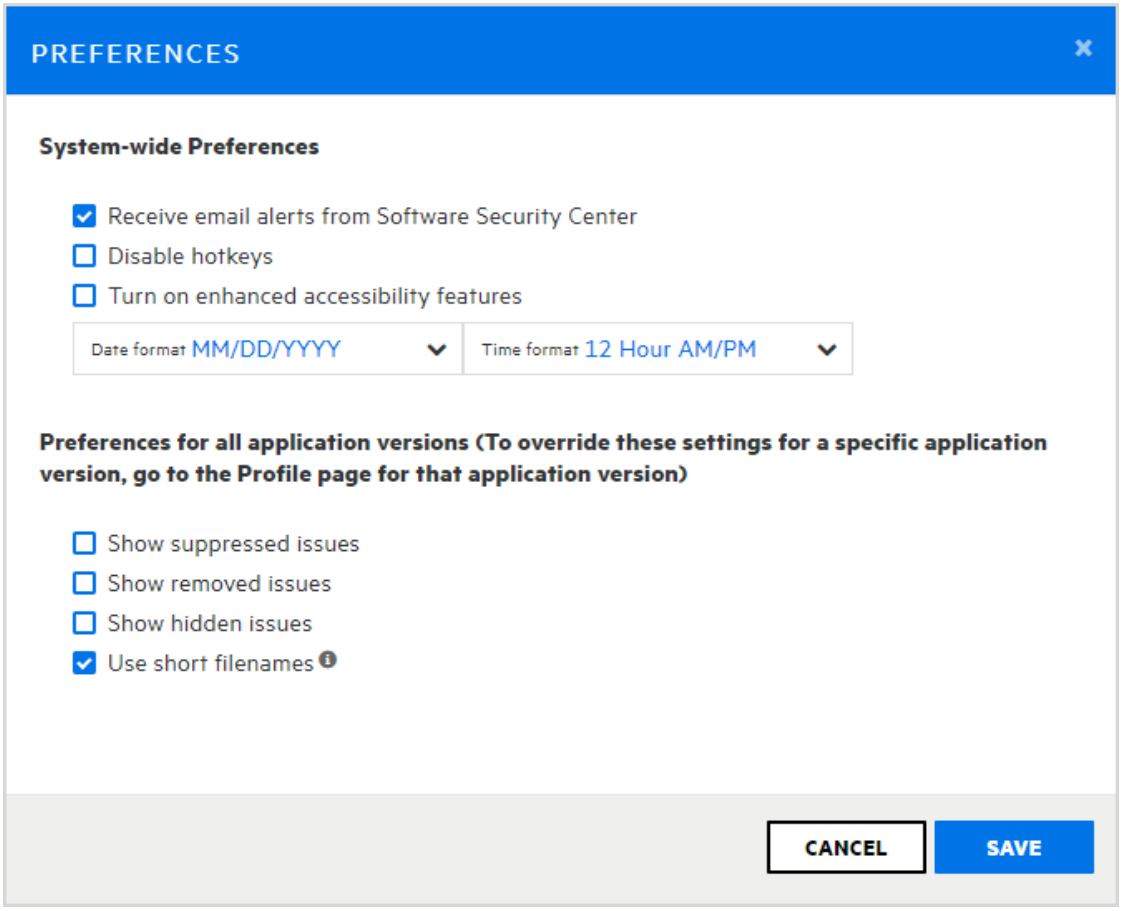
Enabling and Disabling Receipt of Email Alerts

To enable or disable the receipt of email alerts:

1. Log in to Fortify Software Security Center as an administrator.



2. At the right end of the Fortify header, click the user profile icon, and then select **Preferences**.



3. In the PREFERENCES dialog box, do one of the following:
   - To disable the receipt of email alerts, clear the **Receive email alerts from Software Security Center** check box.
   - To enable the receipt of email alerts, select the **Receive email alerts from Software Security Center** check box.
4. Click **SAVE**.

See Also

"Configuring Email Alert Notification Settings" on page 102

"Alert Definitions" on page 305

"Creating Alerts" on page 306

"Deleting Alerts" on page 309

Setting the Strategy for Resolving Issue Audit Conflicts

If multiple auditors are working on the same issue using different products (Fortify Software Security Center, Audit Workbench, or an IDE plugin), they might assign different values to a given custom tag. Previously, if Fortify Software Security

Center detected an audit conflict such as this, it ignored all client-side changes and resolved the conflict in favor of the existing custom tag value on Fortify Software Security Center.

Note: Conflict resolution is not necessary if these auditors work within the same Fortify Software Security Center instance.

Example of the default strategy for resolving audit conflicts:

Audit Workbench users A and B are both auditing the most recent scan results for the same application version.

User A sets custom tag values for the issues uncovered and uploads the results to Fortify Software Security Center.

Fortify Software Security Center accepts the upload and changes the custom tag values for the issues based on the values that user A set for them. Now, the tag values user A set are the current custom tag values for these issues on Fortify Software Security Center.

On a different Audit Workbench instance, user B sets custom tag values for the same issues that user A audited and uploads the results to Fortify Software Security Center. Fortify Software Security Center detects that one or more of the custom tag values that B submitted conflict with the values that user A submitted for the same issues.

Result: Fortify Software Security Center ignores the audit results from user B and retains the values set by user A.

Fortify Software Security Center applies this strategy across all application versions.

You can change this strategy so that Fortify Software Security Center resolves audit conflicts in favor of the most recent changes.

Note: To perform this task, you must have the "Manage issue audit settings" permission.

To set the strategy Fortify Software Security Center uses to resolve audit conflicts:

1. Log in to Fortify Software Security Center as an administrator.
2. On the Fortify header, select **ADMINISTRATION**.
3. In the left pane, select **Configuration**, and then select **Issue Audit**.
   The ISSUE AUDIT page opens.

4. From the **Issue audit conflict resolving strategy** list, select one of the following:
   - **Conflicts are resolved in favor of the SSC changes** (the default)
   - **Conflicts are resolved in favor of the most recent changes**
5. Click **SAVE**.

After you change the setting, the new strategy is applied only to new uploads. All previous conflict resolution results remain unchanged.

See Also

"About Current Issues State" on page 327

Configuring Java Message Service Settings

If you want to publish system events to the Java Message Service (JMS), configure the JMS settings in the Configuration category in the Fortify Software Security Center ADMINISTRATION view.

To configure JMS settings:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Configuration**, and then select **JMS**.
3. On the JMS page, configure the settings as described in the following table.

Field	Description
Publish system events to JMS	Select this check box to publish system events to JMS.
JMS server URL	Type the URL for the JMS server. For example, `tcp://123.0.1.2:12345`.
Include username in JMS body	Select this check box to include the user name in the body of the JMS message. This check box is selected by default.
JMS topic	Type the JMS message topic. The default value is Fortify.Advisory.EventNotification.

4. Click **SAVE**.
5. To implement your changes, restart Tomcat Server.

About Fortify Software Security Center User Authentication

By default, when a user logs on to Fortify Software Security Center or uses a Fortify client to upload Fortify project results files (FPRs), Fortify Software Security Center uses its database to authenticate the user, and then binds the authenticated user to the user's assigned user role (Administrator, Security Lead, Developer, and so on).

Database-only authentication imposes a separate administrative process for creating and managing Fortify Software Security Center user accounts and roles. You can augment the Fortify Software Security Center default database-only authentication using LDAP or an SCIM 2.0 API client. For Information about LDAP user authentication, see "LDAP User Authentication" below. For Information about SCIM 2.0 user provisioning, see "Implementation of SCIM 2.0 Protocol" on page 127.

LDAP User Authentication

The topics in this section provide information about user authentication in Fortify Software Security Center and configuring LDAP authentication and LDAP server options.

Important! Fortify recommends that, before you configure LDAP servers, you create at least one local administrator account in case you encounter problems with your LDAP server at some point.

Important! Although Fortify supports the use of multiple LDAP servers, it does not support the use of multiple LDAP servers behind a load balancer, unless those servers are identical.

Note: For information about how to manage LDAP entities and user roles in Fortify Software Security Center, see "Registering LDAP Entities" on page 123 and "About Managing LDAP User Roles" on page 182.

Preparing to Configure LDAP Authentication

Before you configure Fortify Software Security Center to use LDAP authentication, complete the following tasks:

1. Download an LDAP management application.

   If you are not familiar with the LDAP schema that your LDAP server uses, you can use a third-party LDAP management application such as *JXplorer* to view and modify LDAP authentication directories. (You can download JXplorer for free under a standard OSI-style open source license from http://www.jxplorer.org.)

2. Create an LDAP account for Fortify Software Security Center to use.

   Note: For information about how to configure the primary source for looking up users, see "Configuring Core Settings" on page 99.

   Important! Never use a user account name to provide Fortify Software Security Center access to an LDAP server.

3. Check for conflicts between account names.

   If the LDAP directory contains the default Fortify Software Security Center account `admin`, a conflict occurs that can disable both accounts. If an existing Fortify Software Security Center account has the same name as an account defined for the LDAP server, Fortify Software Security Center account settings and attributes take precedence over those stored on the LDAP server.

   Note: Fortify recommends that no user names in the Fortify Software Security Center be duplicated on an LDAP server.

4. Gather and record required Information.
5. Fortify recommends that you disable the referrals feature. See "About the LDAP Server Referrals Feature" on the next page and "Disabling LDAP Referrals Support" on page 111.

Requirements for Multiple LDAP Servers

If you plan to use more than one LDAP server, the following requirements apply:

- **Usernames must be unique across all of the LDAP servers:**

  Fortify strongly recommends that usernames be unique across all LDAP configurations. Fortify Software Security Center searches for users based on the usernameAttribute specified for a given LDAP server configuration. Because the searches are performed across all the servers, it is important that the searches return just a single result. Be sure to use username attributes that result in unique search hits across all your configured LDAP servers. For example, if you use multiple Active Directories, it may make sense to use `userPrincipalName` as the username attribute in your configurations instead of the default `sAMAccountName`, which may not be unique across AD servers.

  If this requirement is not satisfied…

  In some circumstances, it may be difficult for administrators to avoid duplicate usernames. If Fortify Software Security Center finds a given username in more than one LDAP server during login, it tries to resolve this by using the password with all instances of the username, and then uses the instance that the password authenticates first. In most cases, a user with a non-unique username can successfully log in to Fortify Software Security Center and access most of the user interface functionality. However, some functionality, including report generation, token-based authentication, and DAST integration, is not supported for such users.

- **Separate LDAP server configurations must manage completely independent namespaces (trees)**

  This requirement ensures unique lookup of LDAP DNs by Fortify Software Security Center. The simplest (and recommended) way to achieve this is to ensure that none of the configured baseDNs is a suffix of any of the others.

  In more complex cases, it may be possible to delegate a subtree to be managed by a second LDAP server configuration. In that case, however, all transitive DN references (for example, group member DNs) must also be managed by the second LDAP server. For example, if you have one LDAP server configuration with the base DN `DC=acme,DC=com`, but the `OU=org,DC=acme,DC=com` subtree is managed by another LDAP server, you can set up a second LDAP configuration to manage just the `OU=org,DC=acme,DC=com` LDAP subtree. But you *must* ensure that none of the LDAP objects registered in Fortify Software Security Center from the first LDAP server reference (directly or transitively) the `OU=org,DC=acme,DC=com` subtree, and vice versa.

  If this requirement is not satisfied…

  If an LDAP object DN matches the base DN of more than one LDAP server, Fortify Software Security Center performs a lookup against the LDAP server whose base DN best matches match the given LDAP object DN. This may lead to Fortify Software Security Center using the data of unintended LDAP object in processing and result in unexpected behavior.

See Also

"Configuring LDAP Servers" on the next page

About the LDAP Server Referrals Feature

Some LDAP servers use a special feature called *referrals*. A referral is an entity that contains the names and locations of other objects. A referral is used to redirect a client request to another server. It is sent by the server to indicate that the information that the client has requested can be found at another location (or locations), possibly at another server or several servers.

If Fortify Software Security Center requests an LDAP object and this object is a referral, Fortify Software Security Center must request additional information about the LDAP object from another server, the address of which is returned in the REF object attribute. These additional requests can decrease LDAP communication speed. Even if the LDAP server does not use the referrals feature, additional operations that support referrals are performed.

If referrals are not used on your LDAP server, Fortify recommends that you disable referrals support in the LDAP library. Disabling this option on the Fortify Software Security Center server side makes Fortify Software Security Center-to-LDAP communication much faster. For instructions, see "Disabling LDAP Referrals Support" on the next page.

Note: For a complete description of referrals, go to http://docs.oracle.com/javase/jndi/tutorial/ldap/referral/overview.html.

Disabling LDAP Referrals Support

To disable referrals support:

1. On the Fortify header, click **ADMINISTRATION**.
2. In the left pane, select **Configuration**, and then select **LDAP Servers**.
3. On the LDAP servers page, click the LDAP server connection for which you want to disable referrals support.

   The row expands to reveal details about the LDAP server.
4. Click **EDIT**.
5. Scroll down to the **ADVANCED INTEGRATION PROPERTIES** section.
6. From the **LDAP referrals processing strategy** list, select **ignore**.
7. Click **SAVE**.

Configuring LDAP Servers

The following procedure describes how to configure an LDAP authentication server for use with Fortify Software Security Center.

Important! Before you configure the properties on the LDAP page, you must prepare for LDAP authentication as described in "LDAP User Authentication" on page 108. That section includes requirements and recommendations for configuring multiple LDAP servers.

Important! Fortify recommends that you maintain a couple of local administrator accounts in case you encounter problems with your LDAP server at some point.

To configure an LDAP server connection for Fortify Software Security Center:

1. On the Fortify header, click **ADMINISTRATION**.
2. In the navigation pane on the left, select **Configuration**, and then select **LDAP Servers**.
3. On the Integration with LDAP servers page, click **NEW**.
4. In the CREATE NEW LDAP CONFIGURATION dialog box, configure the attributes described in the following table.

Field	Description
BASIC SERVER PROPERTIES	

Field	Description
Enable this LDAP configuration	Select this check box to make this LDAP server available for Fortify Software Security Center to use.
Server name **Important!** If you configure multiple LDAP servers, make sure that you specify a unique server name for each.	Type a unique name for this server.

Server URL (ldap://<host>:<port>)	Type the LDAP authentication server URL.
	If you use unsecured LDAP, enter the URL in the following format:
	`ldap://<hostname>:<port>`
	If you specify an `ldap://` protocol, and either the **SSL trust check** or the **Hostname validation** check box is selected, StartTLS is used to connect to the LDAP server. Otherwise, an unencrypted connection is used.
	If you use secured LDAPS, enter the URL in the following format:
	`ldaps://<hostname>:<port>`
	LDAPS ensures that only encrypted user credentials are transmitted.

Base DN **Important!** If you configure more than one LDAP server for Fortify Software Security	Type the Base Distinguished Name (DN) for LDAP directory structure searches. For example, the Base DN for `companyName.com` is `dc=companyName,dc=com`. All DN values are case-sensitive, must not contain extra spaces, and must exactly match LDAP server entries.

Field	Description
Center, then you must set a unique Base DN for each of them.	If you specify no value, Fortify Software Security Center searches from the root of LDAP objects tree. With multiple LDAP servers, the Base DN must be unique for each. If the Base DN for one server is empty, it cannot be empty for another LDAP server.

Bind user DN	Type the full distinguished name (DN) of the account Fortify Software Security Center uses to connect to the authentication server.
	The general format for an account specifier is:
	`cn=<accountName>, ou=users,dc=<domainName>,dc=com`
	where `<accountName>` represents the minimum privilege, read-only authentication server account you created for exclusive use by Fortify Software Security Center.
	Caution! For security reasons, never use a real user account name in a production environment.
	If you use Active Directory, specify the domain name and username in the following format:
	`<domain_name>\<username>`

Bind user password	Type the password for the Bind User DN account.
Show password	Select this check box to show entered passwords.
Relative search DNs (1 per line)	(Optional) Type the Relative Distinguished Name (RDN). An RDN defines the starting point from the Base DN for LDAP directory searches. Fortify recommends that you search from the base DN. However, if your

Field	Description

	LDAP directory is so large that searching for Fortify Software Security Center users takes too long, use an RDN to limit the number of LDAP entries searched. You can also use an RDN to hide some part of the LDAP tree from Fortify Software Security Center for security reasons.
	Example: To search within the base DN companyName.com and all entries under that base DN, specify the following to recursively search all entries under that path:
	`cn=users`
	or
	`cn=users,ou=divisionName`

Ignore partial result exception	To avoid search failures when search results include more records than the LDAP server can return, leave this check box selected. You can also enable this flag to hide LDAP server misconfiguration. For example, if the LDAP server limits the number of query results to 500, but there are 600 actual results, with this flag enabled, Fortify Software Security Center silently returns only 500 records.
LDAP server type	From this list, select the type of LDAP server you are connecting with Fortify Software Security Center (either **ACTIVE_ DIRECTORY** or **OTHER**).
SECURITY	
SSL trust check	If the domain controller is enabled for SSL, leave this check box selected to verify that the certificate presented by the LDAP server was issued by a trusted authority. If the domain controller is not configured for SSL, clear this

Field	Description
	check box.
Hostname validation	If the domain controller is enabled for SSL, leave this check box selected to ensure that the LDAP server hostname matches the hostname for which the certificate was issued. If the domain controller is not configured for SSL, clear this check box.
Enable user status mapping	(Microsoft Active Directory only) Select this check box to enable Fortify Software Security Center to retrieve status information for users on this LDAP server. The information is used for enhanced authentication checks during token-based and SSO-based authentication schemes.
BASE SCHEMA	
Object class attribute	Type the class of the object. For example, if this is set to `objectClass`, Fortify Software Security Center looks at the `objectClass` attribute to determine the entity type to search. The default value is `objectClass`.
Organizational unit class	Type the object class that defines an LDAP object as an organizational unit. The default value is `container`.
User class	Type the object class that identifies an LDAP object type as a user. The default value is `organizationalPerson`.
Organizational unit name attribute	Type the group attribute that specifies the organizational unit name. The default value is `cn`.
Group class	Type the object class that identifies an LDAP object type as a group. The default value is `group`.

Field	Description
Distinguished name (DN) attribute	Type the value that determines the attribute Fortify Software Security Center looks at to find the distinguished name of the entity. The default value is `distinguishedName`.
USER LOOKUP SCHEMA	
User firstname attribute	Type the user object attribute that specifies a user's first name. The default value is `givenName`.
User lastname attribute	Type the user object attribute that specifies a user's last name. The default value is `sn`.
Group name attribute	Type the group attribute that specifies the group name. The default value is `cn`.
User username attribute	Type the user object attribute that specifies a username. The default value is `sAMAccountName`.
User password attribute	Type the user object attribute that specifies a user's password. The default value is `userPassword`.
Group member attribute	Type the group attribute that defines the members of the group. The default value is `member`.
User email attribute	Type the user object attribute that specifies a user's email address. The default value is `mail`.
User memberOf attribute	Type the name of an LDAP attribute that includes the LDAP group names for LDAP users.

Field	Description
USER PHOTO	
User photo enabled	Select this check box to enable the retrieval of user photos from the LDAP server.
User thumbnail photo attribute	The thumbnailPhoto attribute for Active Directory
User thumbnail MIME default attribute	Thumbnail MIME default attribute
ADVANCED INTEGRATION PROPERTIES	
Cache LDAP user data **Note:** Fortify recommends that you leave LDAP user caching enabled. Fortify Software Security Center periodically updates the LDAP cache automatically.	Select this check box to enable LDAP user data caching in Fortify Software Security Center. You can refresh the LDAP cache manually from the ADMINISTRATION view in Fortify Software Security Center. For instructions, see "Refreshing LDAP Entities Manually" on page 125.
Cache: Max threads per cache	Type the maximum number of threads dedicated for each update process (user action). Each time a user clicks **Update**, a new update process starts. The default value is 4.
Cache: Initial thread pool size	Type the initial number of available cache update threads. This value is used to configure the thread pool for the task executor, which updates the LDAP cache in several threads simultaneously. The default value is 4.
Cache: Max thread pool size	Type the maximum number of threads that can be made available if the initial thread pool size is not adequate for the update process.

Field	Description
	The default value is 12.
Enable paging in LDAP search queries **Note:** Not all LDAP servers support paging. Check to make sure that your LDAP server supports this feature.	Select this check box to enable paging in LDAP search queries.
Page size of LDAP search request results	If your LDAP server limits the size of the search results by a certain number of objects and **Enable paging in LDAP search queries** is selected, type a value that is less than or equal to your LDAP server limit. The default value is `999`.
LDAP referrals processing strategy **Note:** If referrals are not used on your LDAP server, see "About the LDAP Server Referrals Feature" on page 110.	If you have only one LDAP server, Fortify recommends that you select **ignore** so that LDAP works faster. If you have a multi-domain LDAP configuration and you use LDAP referrals, select `follow`. The default value is `ignore`.
LDAP authenticator type	From this list, select one of the following LDAP authentication types to use: • **BIND_AUTHENTICATOR**– Authentication directly to the LDAP server ("bind" authentication). • **PASSWORD_COMPARISON_ AUTHENTICATOR**–The password the user supplies is compared to the one stored in the repository. For more information about LDAP authentication types, see

Field	Description
	http://docs.spring.io/spring-security/site/docs/3.1.x/reference/ldap.html.
LDAP password encoder type	Select a value from this list only if the LDAP authentication method is password comparison. You must select the encoder type that the LDAP server uses. Fortify Software Security Center compares encoded passwords. If, for example, the LDAP server uses LDAP_SHA_PASSWORD_ENCODER to encode passwords, but you select **MD4_PASSWORD_ENCODER**, password comparisons will fail.
Enable nested LDAP groups **Note:** Use nested LDAP groups only if you absolutely must. Enabling nested LDAP groups forces Fortify Software Security Center to perform extra tree traversals during authentication. Fortify strongly recommends that you clear this check box if you do not plan to use nested groups.	Select this check box to enable nested group support for LDAP in Fortify Software Security Center (wherein a given group member might itself be a group).
Interval between LDAP server validation attempts (ms)	Number of milliseconds the LDAP server waits after a validation attempt before next attempting a validation. The default value is `5000`.

Field	Description
Time to wait LDAP validation (ms)	Type the length of time (in milliseconds) that Fortify Software Security Center is to wait for a response after sending a request to the LDAP server to update the cache. If a response is not received at the end of the designated time, the update is not performed. The request is sent again at the frequency determined by the value set for the Interval between LDAP server validation attempts field. The default value is `5000`.
Base SID of Active Directory objects	(Microsoft Active Directory only) Specify the base security identifier (SID) of LDAP directory objects.
Object SID (objectSid) attribute	(Microsoft Active Directory only) Type the name of the attribute that contains the LDAP entity's objectSid (Object Security Identifier). This attribute is used to search for users based on their object security IDs. It is required if you use Active Directory and more than one LDAP server.

5. To check the validity of the configuration, click **VALIDATE CONNECTION**.
6. To check the validity of and save the configuration, click **SAVE**.
7. To configure another LDAP server, repeat steps 3 through 6.

Important! If you configure multiple LDAP servers, you must make sure that you specify a unique server name and a unique Base DN for each.

Although Fortify supports the use of multiple LDAP servers, it does not support the use of multiple LDAP servers behind a load balancer, unless those servers are identical.

See Also

"Editing an LDAP Server Configuration" below

"Importing an LDAP Server Configuration" on the next page

"LDAP User Authentication" on page 108

"Registering LDAP Entities" on page 123

"Deleting an LDAP Server Configuration" below

"About Managing LDAP User Roles" on page 182

Editing an LDAP Server Configuration

To edit an LDAP server connection:

1. On the Fortify header, click **ADMINISTRATION**.
2. In the left pane, select **Configuration**, and then select **LDAP Servers**.
3. On the Integration with LDAP servers page, click the LDAP server connection that you want to edit.

   The row expands to reveal the LDAP server details.
4. Click **EDIT**.
5. Make all necessary changes to the attributes described in "Configuring LDAP Servers" on page 111.
6. To check the validity of the configuration, click **VALIDATE CONNECTION**.
7. To save the configuration after successful validation, click **SAVE**.

See Also

"Registering LDAP Entities" on page 123

"LDAP User Authentication" on page 108

"About Managing LDAP User Roles" on page 182

Deleting an LDAP Server Configuration

If multiple LDAP servers are configured for your Fortify Software Security Center instance, you can delete any of these, except for the default server, which you can only disable.

To delete an LDAP server connection:

1. On the Fortify header, click **ADMINISTRATION**.
2. In the left pane, select **Configuration**, and then select **LDAP Servers**.
3. Do one of the following:

- On the Integration with LDAP Servers page, select the check box for the LDAP server that you want to delete, and then, on the LDAP Servers toolbar, click **DELETE**.

  Alternatively,

- On the Integration with LDAP Servers page, click the LDAP server connection that you want to delete, and then, at the lower right of the expanded server details section, click **DELETE**.

The DELETE LDAP CONFIGURATION dialog box prompts you to confirm that you want to proceed with the deletion.

4. Click **OK**.
5. To force all LDAP users to re-authenticate, restart the Fortify Software Security Center server.

See Also

"LDAP User Authentication" on page 108

"Registering LDAP Entities" on the next page

"About Managing LDAP User Roles" on page 182

Importing an LDAP Server Configuration

As part of upgrading a Fortify Software Security Center instance, you must import your existing LDAP configuration.

To import your legacy LDAP server configuration:

1. On the Fortify header, click **ADMINISTRATION**.
2. In the left pane, select **Configuration**, and then scroll down and select **LDAP Servers**.
3. On the LDAP Servers header, click **IMPORT**.
4. In the IMPORT LEGACY LDAP CONFIGURATION dialog box, manually copy the content of your legacy `ldap.properties` file for the LDAP configuration to import, and paste it into the text box.

   If Fortify Software Security Center detects problems with the copied content, it displays an error message and a link to click for more information.

   Note: The encoded Bind User DN (`ldap.user.dn`) and Bind User Password (`ldap.user.password`) values are not imported. You must enter these manually (see "Configuring LDAP Servers" on page 111).

5. Correct any problems, and then click **NEXT**.
6. Configure the attributes described in the table in step 4 in "Configuring LDAP Servers" on page 111.
7. To check the validity of the configuration, click **VALIDATE CONNECTION**.
8. To check the validity of and save the configuration, click **SAVE**.

See Also

"Registering LDAP Entities" below

"LDAP User Authentication" on page 108

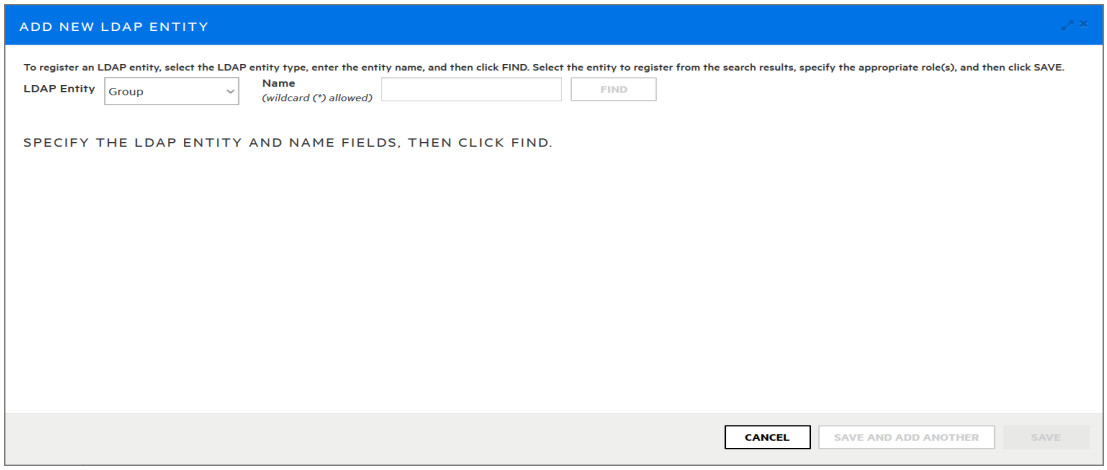
"About Managing LDAP User Roles" on page 182

Registering LDAP Entities

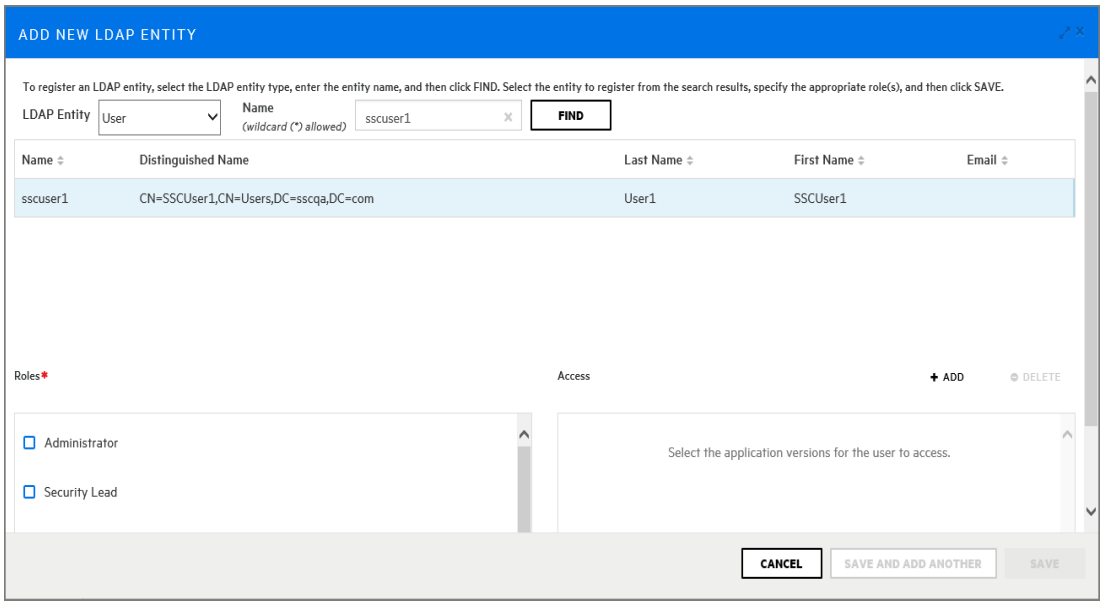
Users who have Administrator-level accounts can add LDAP groups, organizational units, and users to the list of Fortify Software Security Center users. Fortify Software Security Center automatically updates access control as users join and leave groups.

To register an LDAP organizational unit, group, or user with Fortify Software Security Center:

1. Log in to Fortify Software Security Center as an Administrator, and then, on the Fortify header, click **ADMINISTRATION**.
2. In the left pane, click **Users**, and then select **LDAP Entities**.
3. On the **LDAP** toolbar, click **+ADD**.



4. In the ADD NEW LDAP ENTITY window, from the **LDAP Entity** list, select the type of LDAP entity you want to register (**Group**, **User**, or **Organizational Unit**).
5. In the list of returned entities, select the user, group, or organizational unit that you want to register.



6. In the **Roles** section, select the check boxes that correspond to the roles you want to assign to the selected entity.
7. To provide the LDAP entity access to versions of an application, in the **Access** section, do the following.

   Note: You can add versions for multiple applications, but you must add them one at a time using the following steps.

   a. Click **+ ADD**.
   b. From the **Application** list in the SELECT APPLICATION VERSION dialog box , select the name of an application that you want the LDAP entity to access.

      Fortify Software Security Center lists all active versions of the application.
   c. To display inactive versions of the application, select the **Show inactive versions** check box.
   d. Select the check boxes for all of the versions that you want the entity to access.
   e. Click **DONE**.

   The **Access** section lists the application versions you selected.
8. Do one of the following:
   - To save your changes and close the Add New LDAP Entity dialog box, click **SAVE**.
   - To save your changes and register another LDAP entity, click **SAVE AND ADD ANOTHER**.

   Fortify Software Security Center adds the entities to its list of users.

Fortify Software Security Center periodically refreshes the LDAP server cache automatically.

For information about how to configure LDAP servers, see "Configuring LDAP Servers" on page 111.

See Also

"LDAP User Authentication" on page 108

"About Managing LDAP User Roles" on page 182

Refreshing LDAP Entities Manually

Fortify Software Security Center periodically refreshes the LDAP server cache automatically. If you make changes to an LDAP entity, you can initiate the LDAP refresh process manually so that your changes are evident sooner than they would be otherwise.

To initiate the LDAP refresh process manually:

1. Log in to Fortify Software Security Center as an Administrator, and then, on the Fortify header, click **ADMINISTRATION**.
2. In the left pane, select **Users**, and then select **LDAP Entities**.
3. In the list of LDAP entities, select the check box for the LDAP entity to refresh.
4. On the LDAP toolbar, click **REFRESH**.

For information about how to configure LDAP servers, see "Configuring LDAP Servers" on page 111.

See Also

"LDAP User Authentication" on page 108

"Registering LDAP Entities" on page 123

"About Managing LDAP User Roles" on page 182

Handling LDAP Entries Marked "Invalid"

If a registered LDAP entity is no longer present in the LDAP server and you no longer need it in Fortify Software Security Center, remove it from the entities list. Alternatively, if the distinguished name of the LDAP entity was changed, you can update the DN value in Fortify Software Security Center to reflect that.

Note: The following steps apply to LDAP groups and organizational units, as well as to individual users.

To update the DN value for an LDAP entity:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Users**, and then select **LDAP Entities**.

3. Select the row for the entity you need to modify, and then click **EDIT**.
4. Click **UPDATE DISTINGUISHED NAME**. (This button is visible only if the current DN is invalid.)
5. In the UPDATE DISTINGUISHED NAME dialog box, select the now invalid value in the **Distinguished name** field, and replace it with the updated distinguished name.
6. Click **SAVE**.

See Also

"Configuring LDAP Servers" on page 111

Enabling Persistence of the LDAP Cache

By default, an LDAP cache is only in memory and is lost during server shutdown. If your organization has a large volume of LDAP users, the loss of the LDAP cache can significantly slow the next server startup.

Note: If your organization has a large volume of LDAP users, the next server startup may take a significant amount of time because the cache must be rebuilt.

To enable the LDAP cache to persist after server shutdown:

1. Shut down Fortify Software Security Center.
2. Navigate to the `<fortify.home>/<app_context>/conf` directory and open the `app.properties` file in a text editor.
3. Set the `ldap.cache.persistence.enabled` property to `true`.
4. Save and close your `app.properties` file.
5. Restart Fortify Software Security Center.

Changing the Default Cache Refresh Interval

The default cache refresh interval is one hour. If large LDAP groups are registered with Fortify Software Security Center, a frequent cache refresh can place an extra load on Fortify Software Security Center and the LDAP server and thereby affect performance. To reduce the impact, you can increase the interval, as follows:

1. Shut down Fortify Software Security Center.
2. Navigate to the `<fortify.home>/<app_context>/conf` directory and open the `app.properties` file in a text editor.
3. Add the following line:

   `ldap.cache.refresh.interval.hours=<whole number value between 1 and 12>`
4. Restart Fortify Software Security Center.

Implementation of SCIM 2.0 Protocol

When you enable System for Cross-domain Identity Management (SCIM) in Fortify Software Security Center, a SCIM 2.0 API client pushes users and groups to Fortify Software Security Center via the SCIM 2.0 protocol for provisioning and managing identity data. So, you do not have to go through the Fortify Software Security Center ADMINISTRATION view to add users. Instead, you configure users and groups from the SCIM 2.0 API client.

Note: You can integrate with any SCIM 2.0 API client. However, if you do, you must test its interoperability with Fortify Software Security Center independently. For now, only Azure AD integration is officially supported.

Because users provisioned using the SCIM API are externally managed and single sign-on users only, the following apply:

- You can only assign roles and application versions to externally managed users from Fortify Software Security Center.
- Users can only log in using SSO.
- If a username created locally (**ADMINISTRATION** > **Users** > **Local Users**) already exists in Fortify Software Security Center, a user with the same username cannot be provisioned using SCIM. Users created from the ADMINISTRATION view are read-only for SCIM provisioning.

Supported SCIM Resources

Fortify Software Security Center supports the following SCIM resources:

- User (`urn:ietf:params:scim:schemas:core:2.0:User schema`)

  Fortify Software Security Center accepts all standard attributes of the User Schema, but stores only a subset of these (see "User Attribute Mappings" on the next page). Also accepts Enterprise User extension attributes (`urn:ietf:params:scim:schemas:extension:enterprise:2.0:User schema`) but does not store them.

- Group (`urn:ietf:params:scim:schemas:core:2.0:Group schema`)

  Fortify Software Security Center accepts all standard attributes from the Group Schema, but stores only a subset of these (see "Group Attribute Mappings" on the next page).

Optional features supported:

- Resource filtering (RFC 7644 - 3.4.2.2 Filtering)
- PATCH operations (RFC 7644 - 3.5.2 - Modifying with PATCH)

User Attribute Mappings

The following table shows how SCIM user attributes map to Fortify Software Security Center user attributes.

SCIM User Attribute	SSC User Attribute	Comment
meta.created	created	Read-only
meta.lastModified	lastModified	Read-only
id	N/A	Read-only, Unique, Opaque
userName	userName	Unique, Required
active	suspended (not)	The Suspended option in Fortify Software Security Center is set accordingly.
name.givenName	firstName	
name.familyName	lastName	
emails[type="work"].value	email	

Group Attribute Mappings

The following table shows how SCIM group attributes map to Fortify Software Security Center group attributes.

SCIM Group Attribute	SSC Group Attribute	Comment
meta.created	created	Read-only
meta.lastModified	lastModified	Read-only
id	N/A	Read-only, Unique, Opaque
displayName	name	Required
members	N/A	Must reference existing users and / or groups

See Also

"Using SCIM 2.0 and SAML 2.0 to Configure a Connection to Azure AD for User Provisioning" below

"Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single Sign-On" on page 150

Using SCIM 2.0 and SAML 2.0 to Configure a Connection to Azure AD for User Provisioning

You can use the System for Cross-domain Identity Management (SCIM) protocol to provision Fortify Software Security Center with user accounts from Azure Active Directory (Azure AD). The following table lists the tasks required to use this feature, in the order in which they must be performed.

Task	For Details
Enable SCIM from Fortify Software Security Center.	"Enabling SCIM for Provisioning of Externally Managed Users and Groups" on page 132
In Microsoft Azure, go to Azure Active Directory and create an enterprise application.	Microsoft Azure documentation (https://docs.microsoft.com/en-us/azure/active-directory) **Note:** When Azure AD prompts you to indicate what you want to do with the new application, select the Integrate any other application you don't find in the gallery (Non-gallery) option.
From Azure, assign users and groups to the new application.	Microsoft Azure documentation (https://docs.microsoft.com/en-us/azure/active-directory)
From Azure, provision the application. Note the following: • Set **Provisioning Mode** to **Automatic**. • Use the SSC URL for the **Tenant URL** value, and append to it the following string: `/api/scim/v2?aadOptscim062020`	Microsoft Azure documentation (https://docs.microsoft.com/en-us/azure/active-directory)

Task	For Details
Note: `/api/scim/v2` is the URL for the SSC SCIM endpoint. The `aadOptscim062020` query parameter improves Azure AD compliance with SCIM v2.0. • For the **Secret Token** value, use the token you created in SSC (**SCIM Token** - see "Enabling SCIM for Provisioning of Externally Managed Users and Groups" on page 132.)	
From Azure AD, change the attribute mappings for data flow between Azure AD and Fortify Software Security Center. Delete all but the following attributes for your users (for groups, you change no attribute mappings): • userName • active • emails[type eg "work"].value • name.givenName • name.familyName • externalID Make sure that you move the **Provisioning Status** toggle to **On**.	Microsoft Azure documentation (https://docs.microsoft.com/en-us/azure/active-directory)
Azure AD SAML metadata is signed. For Fortify Software Security Center to successfully verify the signature, you must download the SAML signing certificate from Azure and import it into the keystore to be used in the SSO SAML configuration (SAML keystore location).	• Microsoft Azure Active Directory documentation (https://docs.microsoft.com/en-us/azure/active-directory) • "Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single

Task	For Details
In Azure, navigate to the created enterprise application. On the SAML-based Sign-on page, download the signing certificate, and then import it into the keystore.	Sign-On" on page 150
Set up SAML single sign-on from Fortify Software Security Center.	"Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single Sign-On" on page 150
Acquire the metadata XML file from Fortify Software Security Center and save it locally. This file can be accessed only if SAML SSO is enabled in Fortify Software Security Center and successfully initialized.	`<ssc_hostname>:<port>/<context>/saml/metadata`
In Azure, upload the saved metadata file, and then complete the SAML single sign-on setup using data from the uploaded metadata file.	Microsoft Azure documentation (https://docs.microsoft.com/en-us/azure/active-directory)
From Fortify Software Security Center, assign roles and application versions to externally managed users and groups.	"Viewing Externally Managed Users and Groups" on page 230

Enabling SCIM for Provisioning of Externally Managed Users and Groups

To enable SCIM for provisioning of externally-managed users and groups:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, click **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Configuration**, and then scroll to and select **SCIM**.
3. Select the **Enable SCIM** check box.
4. In the **SCIM Token** box, enter the SCIM token you want to use as a bearer token to authenticate with the Fortify Software Security Center SCIM API. (Use that token as a Secret Token in Azure AD when you configure the connection between Fortify Software Security Center and Azure AD.)

   Important! The token can include upper and lower case letters, numbers, hyphens and underscores. The token must contain at least 32 characters, and no more than 512 characters. Because the token allows access to user management in Fortify Software Security Center, it must be protected. Fortify recommends that you use a secure random string generator to generate the token.

5. Click **SAVE**.

See Also

"Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single Sign-On" on page 150

"Implementation of SCIM 2.0 Protocol" on page 127

"Viewing Externally Managed Users and Groups" on page 230

Configuring a Proxy for Fortify Software Security Center Integrations

You can configure a single proxy for use with all HTTP(s) protocol-based integrations with Fortify Software Security Center. Once you configure the proxy, you can then enable its use (select the **Use SSC proxy for...** check box) for components such as Audit Assistant ("Configuring Audit Assistant" on page 90), the Rulepack update URL ("Configuring Core Settings" on page 99), and bug tracker plugins ("Assigning a Bug Tracking System to an Application Version" on page 260).

To configure a single proxy for use with all HTTP(s) protocol-based Fortify Software Security Center integrations:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Configuration**, and then select **Proxy**.

   On the Proxy page, provide values for the settings described in the following table.

Setting	Description
Enable SSC proxy	Select this check box to enable proxy use.
HTTP proxy	
HTTP proxy host	Type the name of an HTTP proxy host (without a protocol part and port number) For example, some.proxy.com.
HTTP proxy port	Type the HTTP proxy port number.
HTTP proxy user	If HTTP authentication is required, type a user name.
HTTP proxy password	If HTTP authentication is required, type a password.
HTTPS proxy	
Set up a different HTTPS proxy	Select this check box to enable the use of a different secure proxy for HTTPS requests.
HTTPS proxy host	Type the name of an HTTPS proxy host (without a protocol part and port number). For example, some.secureproxy.com.
HTTPS proxy port	Type the HTTPS proxy port number.
HTTPS proxy user	If HTTPS authentication is required, type a user name.
HTTPS proxy password	If HTTPS authentication is required, type a password.

3. Click **SAVE**.

Fortify Software Security Center displays a message at the upper right to indicate that the proxy configuration was successful.

See Also

"Configuring Audit Assistant" on page 90

"Configuring Core Settings" on page 99

"Assigning a Bug Tracking System to an Application Version" on page 260

Configuring ScanCentral SAST Monitoring in Fortify Software Security Center

With Fortify ScanCentral SAST, Fortify Static Code Analyzer users can maximize their resource use by offloading the processor-intensive scanning phase to a dedicated Fortify Static Code Analyzer scan farm. You can monitor ScanCentral SAST and display its results in Fortify Software Security Center. You can also create and manage ScanCentral SAST sensor pools. To enable this functionality, you must configure the integration in Fortify Software Security Center.

Note: For information about how to install, configure, and use Fortify ScanCentral SAST to streamline the static code analysis process, see the *Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

To configure the integration between Fortify Software Security Center and ScanCentral SAST:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, click **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Configuration**, and then select **ScanCentral SAST**.
3. On the ScanCentral SAST page, select the **Enable ScanCentral SAST** check box.
4. In the **ScanCentral Controller URL** box, type the URL for your ScanCentral SAST Controller.

   Important! The Controller must be the same or later version as Fortify Software Security Center.

5. In the **ScanCentral poll period (seconds)** box, type the number of seconds to elapse between sessions of data polling from ScanCentral SAST.
6. In the **SSC and ScanCentral controller shared secret** box, type the shared secret key (unencrypted) for Fortify Software Security Center to use to request data from the Controller. (If you use clear text, this string must match the value stored in the Controller `config.properties` file for the `ssc_scancentral_ctrl_secret` key.)

   The Controller verifies the shared secret key when requested for administration console data.
7. Click **SAVE**.
8. Restart the Fortify Software Security Center server.

See Also

"ScanCentral SAST Permissions" on page 382

"Viewing ScanCentral Controller Information" on page 387

"About ScanCentral SAST Sensor Pools" on page 390

"Creating ScanCentral SAST Sensor Pools" on page 391

Enabling the Running and Management of ScanCentral DAST Scans from Fortify Software Security Center

Fortify ScanCentral DAST is a dynamic application security testing tool that consists of the Fortify WebInspect sensor service and other supporting technologies that you can use in conjunction with Fortify Software Security Center.

To enable the running and management of ScanCentral DAST dynamic scans:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, click **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Configuration**, and then select **ScanCentral DAST**.
3. On the ScanCentral DAST page, select the **Enable ScanCentral DAST** check box.
4. In the **ScanCentral DAST server URL** box, enter the URL for your ScanCentral DAST server.

   The ScanCentral DAST server URL should resemble one of the following:

   `http://<DAST_API_Hostname>:<Port>/api/`

   `http://<DAST_API_IP_Address>:<Port>/api/`

   You can use the https protocol instead.

   Important! Make sure that you include the trailing /api/ in the URL.
5. Click **SAVE**.

For information about how to perform the following tasks, see the *ScanCentral DAST Configuration and Usage Guide*:

- Manage ScanCentral DAST pools and sensors
- Create, run, change, and delete ScanCentral DAST scans, schedules, and settings

Configuring Job Scheduler Settings

You configure the Fortify Software Security Center job scheduler from the **Configuration** section of the ADMINISTRATION view.

To configure job scheduler settings:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Configuration** > **Scheduler**.

3. On the Scheduler page, configure the settings as described in the following table.

Field	Description
Number of days after which executed jobs are removed	The number of days after which finished jobs are removed from Fortify Software Security Center. The default value is 1 (day). Canceled jobs are removed daily.
Job execution strategy	Select the job execution strategy to use. Options are as follows: • **Conservative:** Default strategy balancing job concurrency, throughput and job stability. This job execution strategy works as follows: ◦ Some jobs, such as delete jobs, are considered low concurrency, or *exclusive* jobs. Only one such exclusive job can run at a time. (Running an exclusive job reduces running jobs to 60 percent of configured capacity.) ◦ At most, `${job.numberOfConcurrentReports}` report jobs can run concurrently. ◦ At most, `${numberOfConcurrentExclusiveJobs}` exclusive jobs can run concurrently. (The default is 1.) ◦ At most, `${jobs.threadCount}` jobs can run at the same time. Of that number, `${job.numberOfDedicatedDataExports}` threads are reserved for comma-separated values (CSV) file export jobs. Other jobs cannot use those threads. • **Flexible (technical preview):** This strategy provides the same options as the conservative strategy, but improves job queue worker use. • **Aggressive:** Enables high concurrency. With this option, the job scheduler does not enforce any limitations on how jobs are executed. All jobs are equal and executed on all available workers. • **Exclusive jobs:** Enables jobs to run in sequence, one at a time.

Field	Description
	The default value is **Conservative**. **Note:** Two worker threads are dedicated to exporting to comma-separated values (CSV) jobs for both conservative and aggressive strategies. (See "Exporting Data to Comma-Separated Values Files" on page 216.)
Pause job execution	This check box (not selectable from the Scheduler page) shows whether job execution has been paused (from the Maintenance page) in preparation for server shutdown / system maintenance. To proceed to the Maintenance page to select or clear this check box, click the **here** link. A change to this setting takes effect immediately after you save the change from the Maintenance page. No server restart is required. After you pause job execution, jobs (artifact processing, report generation, data export requests, and so on) that are currently running continue to completion. Any new jobs submitted are queued for processing once the **Pause job execution** check box is clear and normal processing resumes. **Important!** Fortify strongly recommends that you pause job execution immediately before server shutdown, and keep it paused for as short a period of time as possible. This will prevent a high volume of jobs from queuing up for processing later. **Caution!** Job execution does not automatically resume after the server comes back up after maintenance. To resume job execution, you must return to the Maintenance page and clear the **Pause job execution** check box.
Token management	
Token	Number of days before token expiration that users are

Field	Description
expiration alerts	notified of the upcoming expiration. Valid values range from 3 to 30 days, inclusive. The default value is 7 (days). **Note:** The start of the day is 12 AM in the Fortify Software Security Center server locale.
Snapshot refresh - Use the fields in this section to schedule the snapshot job. A snapshot is application version information captured at a given moment in time. This information includes variables and performance indicator values, which are used to calculate application versions trends at the scheduled times.	
Days of week	Type a CRON expression to specify the days of the week on which the historical snapshot job is to be run. You can enter the value as a three-letter abbreviation for the day of the week (for example, type THU for Thursday) or as a single digit, by entering a 1 for Sunday, a 2 for Monday, and so on. To run the scheduler on multiple days, separate the entries with a comma. For example, type **SUN, WED, FRI** or **1, 4, 6**. **Note:** The three-letter abbreviations must be entered as upper-case letters. Spaces between the entries are optional. To enter consecutive days, separate the entries with a dash. For example, type **MON-FRI** to run the scheduler on week days only. Type ***** if the scheduler is to run every day (the default).
Hours	Type the hour, using 24-hour time notation, at which the recurring scheduler job is to start running. For example, type **1** to start the job at 1 A.M. Type ***** if the scheduler is to run every hour. **Note:** The values you enter in the **Days of Week**, **Hours**, and **Minutes** fields are concatenated to create the CRON expression used by the scheduler.

Field	Description
	The default value is 0 (midnight).
Minutes	Type the minute at which the recurring scheduler job is to start running. For example, type **24** to start the job at 24 minutes past the hour that you entered in the **Hours** box. The default value is 0 (indicating the job starts running in the first minute).
Index maintenance Use the fields in this section to schedule your Fortify Software Security Center full text search index maintenance. Fortify recommends that you run this job daily.	
Days of week	Type a CRON expression to specify the days of the week on which the index maintenance job is to be run. You can enter the value as a three-letter abbreviation for the day of the week (for example, type THU for Thursday) or as a single digit, by entering a 1 for Sunday, a 2 for Monday, and so on. To run the scheduler on multiple days, separate the entries with a comma. For example, type **SUN, WED, FRI** or **1, 4, 6**. **Note:** The three-letter abbreviations must be entered as upper-case letters. Spaces between the entries are optional. To enter consecutive days, separate the entries with a dash. For example, type **MON-FRI** to run the scheduler on week days only. Type ***** if the scheduler is to run every day. The default value is *.
Hours	Type the hour, using 24-hour time notation, at which the recurring index maintenance job is to start running. For example, type **1** to start the job at 1 A.M. Type ***** if the scheduler is to run every hour. **Note:** The values you enter in the **Days of Week**, **Hours**, and **Minutes** fields are concatenated to create

Field	Description
	the CRON expression used by the scheduler. The default value is 0 (midnight).
Minutes	Type the minute at which the recurring index maintenance job is to start running. For example, type **24** to start the job at 24 minutes past the hour that you entered in the **Hours** box. The default value is 0 (indicating the job starts running in the first minute).
Events maintenance	
Days to preserve	Type the number of days after which Micro Focus removes past events. To specify no event removal, type **0** (zero). Fortify Software Security Center uses the new value during the next run of the dedicated cleaning job. A new job is created daily at 11:30 p.m. and if it is not blocked, it starts its work immediately. The default value is 0. (No cleanup occurs.)
Reports maintenance	
Days to preserve	Type the number of days Fortify Software Security Center is to retain generated reports. The default value is 0. (No cleanup occurs.) To ensure that the cleanup job is not too time- or resource-intensive, each nightly run clears a maximum of 2000 old reports (and associated entities). Fortify SSC then gradually cleans up the remaining reports over the following days.
Data export maintenance	
Days to preserve	Type the number of days Fortify Software Security Center is to retain exported audit reports. The default value is 2. **Note:** This job is run every day at 11:45 PM (23:45)

4. Click **SAVE**.
5. To implement your settings, restart the server.

See Also

"Setting Job Execution Priority" below

"Canceling Scheduled Jobs" on page 143

"Recurring Cleanup Jobs" on page 143

Setting Job Execution Priority

All new jobs in Fortify Software Security Center are scheduled with priority set to "very low." Multiple jobs that have the same priority are processed in the order in which they are added to the jobs queue. That is, the first job added to the queue is the first job processed. Jobs with higher priority values set are processed before those assigned lower priority.

If you are a Fortify Software Security Center administrator or a security lead, you can change the priority of scheduled jobs that are in the PREPARED state. (Job state can be PREPARED, RUNNING, FINISHED, FAILED, or CANCELED.)

To set the priority for a scheduled job:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Metrics & Tracking**, and then select **Jobs**.
3. On the right end of the **Jobs** toolbar, from the **Filter by** list, select **Prepared**.
4. Scroll through the listed jobs and expand (click) the row for the job you want to re-prioritize.
5. From the **SET PRIORITY** list, select one of the following priority values:
   - Very Low
   - Low
   - Medium
   - High
   - Very High

   Changing job priority may affect other jobs in the queue. If the priority you set for a job potentially affects other jobs, Fortify Software Security Center displays a message to advise you of the potential effect, and prompts you to confirm that you want to continue with the change.
6. To continue, click **OK**.

The jobs table now reflects the changed priority setting.

See Also

"Canceling Scheduled Jobs" on page 143

"Configuring Job Scheduler Settings" on page 135

Canceling Scheduled Jobs

If you are a Fortify Software Security Center administrator or a security lead, you can cancel scheduled jobs that are still in the prepared state. (The job state can be prepared, running, finished, failed, or cancelled.)

To cancel a job:

1. Log in to Fortify Software Security Center as an administrator or security lead, and then, on the Fortify header, select **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, under **Metrics & Tracking**, select **Jobs**.
3. On the far right of the **Jobs** toolbar, from the **Filter by** list for job state, select **Prepared**.
4. Scroll through the listed jobs and click the row for the job you want to cancel.
5. Click the row for the job to expand it and view the details.
6. Click **CANCEL**.

   Fortify Software Security Center prompts you to confirm that you want to cancel the job.
7. Confirm that you want to cancel the job.

See Also

"Configuring Job Scheduler Settings" on page 135

Recurring Cleanup Jobs

Fortify Software Security Center performs several cleanup jobs on a recurring basis. These are described in the following table.

Job Name and Description	Affected Tables	Default Schedule
Data Export Cleanup Removes exported data (such as CSV files) that were more than the specified number of days old. (See "Configuring Job Scheduler Settings" on page 135.)	dataexport, documentinfo, and datablob	Daily at 23:45 h For instructions on how to schedule this job from the Fortify Software Security Center user interface, see "Configuring Job Scheduler Settings" on page 135.
Event Log Cleanup	eventlogentry	Daily at 23:30 h

Job Name and Description	Affected Tables	Default Schedule
Removes event records older than the number of days specified on the Scheduler page.		For instructions on how to schedule this job from the Fortify Software Security Center user interface, see "Configuring Job Scheduler Settings" on page 135.
Expired Tokens Cleanup Removes expired tokens with elapsed expiration dates.	agentcredential	Daily, every six hours, starting at 00:00 h
ID Table Cleanup Removes IDs, used for filtering while working with user permissions and generating reports.	id_table pv_id_table	Daily at 23:00 h For instructions on how to schedule this job from the Fortify Software Security Center user interface, see "Configuring Job Scheduler Settings" on page 135.
Job Cleanup Removes finished jobs. (Failed jobs are removed after the set number of days, beginning with their start time. Canceled jobs are cleaned up without regard to start time.)	jobqueue	Daily at 23:00 h
Orphaned Data Cleanup Removes metadata associated with attachments that are no longer needed.	documentinfo	Every Sunday at 23:30 h

Job Name and Description	Affected Tables	Default Schedule
Orphaned Source Files Cleanup Removes source files that are no longer referenced by any existing issue.	sourcefile	Daily at 00:00 h Set using job.sourceFileCleanup.cron
Report Cleanup Removes generated reports that are older than the number of days specified for **Days to preserve** on the Scheduler page.	savedreport documentinfo datablob	No cleanup scheduled For instructions on how to schedule this job from the Fortify Software Security Center user interface, see "Configuring Job Scheduler Settings" on page 135.
Webhook History Cleanup Removes old webhook event entries.	webhookhistory	Daily at 03:30 h
Index Maintenance Resolves inconsistencies between global search (fulltext) indexes and existing database entries (for example, resulting from unclean server shutdown or indexing job failures).	N/A	Daily at 00:00 h For instructions on how to schedule this job from the Fortify Software Security Center user interface, see "Configuring Job Scheduler Settings" on page 135.
LDAP Refresh Updates caches associated with LDAP entities.	N/A	Hourly
Historical Snapshot	N/A	Daily at 00:00 h

Job Name and Description	Affected Tables	Default Schedule
Re-creates out-of-date snapshots.		For instructions on how to schedule this job from the Fortify Software Security Center user interface, see "Configuring Job Scheduler Settings" on page 135."Configuring Job Scheduler Settings" on page 135
Alert Reminder Sends reminder alerts.	N/A	Daily at 03:00 h
Token Expiry Alerts Notifies users of any tokens to expire soon.	N/A	Daily at 03:00 h

Configuring Browser Access Security for Fortify Software Security Center

To configure security for browsers that access the Fortify Software Security Center domain:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Configuration**, and then select **Security**.
3. On the Security page, configure the settings as described in the following table.

Field	Description
Content-Security-Policy	Specify what (if any) level of CSP to use. Using the HTTP Content-Security-Policy header controls the resources browsers can load and what actions they can perform on pages loaded from Fortify Software Security Center. This helps guard against cross-site scripting attacks. Select one of the following options: • To restrict access to only the base URL configured

Field	Description
	using the `host.url` property (set using the Fortify Software Security Center configuration wizard), select **Strict**. • To enable a less restrictive policy than strict CSP, select **Relaxed**. This is the default setting. It allows access to the Fortify Software Security Center domain from any host:port. • To disable the Content-Security-Policy header, select **Disabled**. Although Fortify recommends that you *not* disable the Content-Security-Policy header, this option is available if CSP causes unexpected problems.
Set value for Strict-Transport-Security header	Type the value for the Strict-Transport-Security header. This header signals to browsers to use HTTPS instead of HTTP to communicate with Fortify Software Security Center. **Important!** Please use caution when you set this value. It can have a severe impact on users. For more detail, see the HTTP Strict Transport Security Cheat Sheet (https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet). The Strict-Transport-Security header is sent only through a secure channel determined by Tomcat Server.
Set value for Public-Key-Pins header	Type the value for the Public-Key-Pins header. This decreases the risk of man-in-the-middle (MitM) attacks. **Important!** Please use caution when you set this value. It can have a severe impact on users. For more detail, see the HTTP Strict Transport Security Cheat Sheet (https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet).

Field	Description
	The Public-Key-Pins header is sent only through a secure channel determined by Tomcat Server.

4. Click **SAVE**.

Configuring Fortify Software Security Center to Work with Single Sign-On

The following table lists the single sign-on solutions that Fortify Software Security Center supports, and provides links to the instructions on how to configure Fortify Software Security Center to work with these SSO types.

SSO Solution	Instructions
CAS (Central Authorization Server)	"Configuring Fortify Software Security Center to Work with a Central Authorization Server" on the next page
SPNEGO/ KERBEROS	"Setting up Kerberos Authentication with Fortify Software Security Center" on page 157
SAML 2.0-compliant single sign-on	"Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single Sign-On" on page 150
HTTP headers	"Configuring Fortify Software Security Center to Work with Single Sign-On and Single Logout Solutions that use HTTP Headers" on page 155
X.509 certification	"Configuring Fortify Software Security Center to Use X.509 Certification-based SSO" on page 159

Restrictions on Configuration

Restrictions on configuring Fortify Software Security Center to work with SSO solutions are as follows:

- You can only use the SSO solutions that Fortify Software Security Center supports to give users access to the Fortify Software Security Center user interface.
- At any given time, you can configure only one SSO solution for use with Fortify Software Security Center.

- A user who wants to access Audit Workbench, fortifyclient, or any of the IDE plugins, must use an LDAP or local Fortify Software Security Center user account and password to log in.

For information about how to enable debug logging for SSO, see "Enabling Debug Logging for Single Sign-On Authentication" on page 161.

Restricted Local Login (SPNEGO/Kerberos and x.509 solutions only)

Important! This restriction does not apply to the Central Authorization Server (CAS), SAML, or HTTP Headers SSO solutions. Local login is supported for these SSO solutions.

To improve application security, if SSO authentication is enabled, Fortify Software Security Center prevents both LDAP and local users from using usernames and passwords to log in locally. Users can only use the configured SSO method or an API token to access Fortify Software Security Center. To enable local login with either the SPNEGO/Kerberos or x.509 SSO solution configured, an administrator must use the `sso.localAuthenticationEnabled` property, which is located in the `app.properties` file. For information, see "Enabling Username and Password Login if Fortify Software Security Center is Configured to Use the X.509 or Kerberos SSO Solution" on page 160.

See Also

"About Session Logout" on page 79

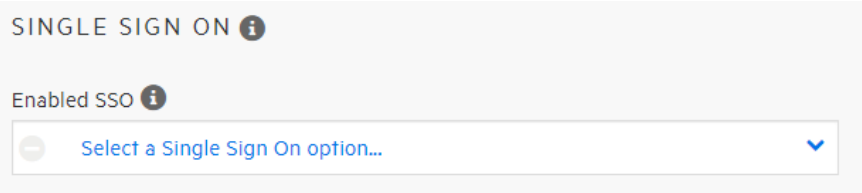
Configuring Fortify Software Security Center to Work with a Central Authorization Server

Note: CAS single logout is supported in Fortify Software Security Center.

To configure Fortify Software Security Center to work with a Central Authorization Server (CAS):

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, click **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Configuration**, and then select **SSO**.

   Note: Only one single sign-on solution can be configured for Fortify Software Security Center at a time.



3. From the list of available single sign-on solutions on the SINGLE SIGN ON page, select **CAS**.
4. In the **Central Authentication Server URL** box, type the URL for the CAS server. The default is `http://localhost:8080/cas`.
5. Verify that the `host.url` property in `<fortify.home>/<app_context>/conf/app.properties` designates a URL that the CAS server can access. The URL is used as a base URL for the Fortify Software Security Center service parameter, which is set to `<host.url>/login/cas`.
6. Click **SAVE**.
7. To implement the configuration, restart the server.

Note: For information about how to obtain extra logging information related to SSO authentication for Fortify Software Security Center, see "Enabling Debug Logging for Single Sign-On Authentication" on page 161.

Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single Sign-On

Before you configure Fortify Software Security Center to work with SAML 2.0 single sign-on, be aware of the following:

- Fortify Software Security CenterFortify Software Security Center supports HTTP REDIRECT and HTTP POST bindings for inbound and outbound SAML messages.
- SAML single logout is supported in Fortify Software Security Center. Logout responses and logout requests sent by IdP *must* be signed.
- For successful SAML integration, the clocks on the client and server machines (IdP and SP) *must* be synchronized.

To configure Fortify Software Security Center to work with SSO that uses SAML 2.0:

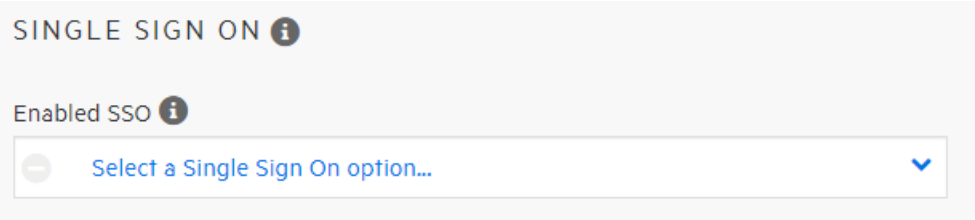
1. If you are using an LDAP directory for users in Fortify Software Security Center and IdP, configure Fortify Software Security Center to use LDAP authentication. Otherwise, IdP users must match local users. (For information, see "LDAP User Authentication" on page 108.)
2. If your IdP runs with SSL (https), configure Fortify Software Security Center to run with SSL. Otherwise, protocol switching while authenticating against IdP could interfere with authentication.

3. Prepare a public/private key pair to be used to digitally sign SAML messages and encrypt SAML Assertions. If your IdP does not require keys signed by a specific certification authority, you can generate your own self-signed key using, for example, OpenSSL or Java's keytool. The following example command generates a keystore that stores a self-signed key under a given alias:

   ```
   keytool -genkeypair -alias <key_alias> -keyalg <RSA_or_EC
   algorithm> -keystore <keystore_filename> -storepass <password_to_
   protect_keystore> -keypass <password_to_protect_key> -validity
   <number_of_days_the_key_is_valid>
   ```

   Make a note of the values for the alias and both passwords. You must provide them later in the Fortify Software Security Center Administration section (**ADMINISTRATION** > **Configuration** > **SSO** > **SAML**).
4. Get SAML metadata from the IdP server and store it on the Fortify Software Security Center file system.
5. Open the metadata file and make a note of the entityID for your IdP EntityDescriptor (<EntityDescriptor entityID="THE_VALUE_YOU_ARE_LOOKING_FOR">). Also check to see whether the metadata is signed (the <Signature> section is present). If the metadata is signed, the signature is verified with the PKIX validation algorithm and uses all public keys present in the keystore as trust anchors. Make sure that you include the root CA certificate and intermediary CA certificates of the signature in your keystore.
6. Log in to Fortify Software Security Center and, on the Fortify header, select **ADMINISTRATION**.
7. In the left pane of the ADMINISTRATION view, select **Configuration**, and then select **SSO**.

   Note: You can configure only one single sign-on solution at a time for Fortify Software Security Center.

   If a single sign-on solution other than SAML is currently configured, its name is displayed in the list on the SINGLE SIGN ON page.
8. From the list of available single sign-on solutions, select **SAML**.

9. Provide the information described in the following table.

Field	Description

IdP metadata location	Location of your identity provider metadata (the metadata obtained in step 3).
	Examples
	`file:///location/of/idp-metadata.xml`
	`https://idp-metadata.example.com`
	Note: If you are integrating with Azure AD, enter the value shown in the **App Federation Metadata Url** field In Azure. (In the left pane in Azure, under **Manage**, select **Single sign-on**, and then select **SAML**. You can see the **App Federation Metadata Url** field under **SAML Signing Certificate**.)
	Note: If your IdP is behind a proxy server, you must download IdP metadata to your local file system and reference it locally. Current SAML implementation does *not* support getting metadata over http proxy.

Default IdP	entityID of your IdP EntityDescriptor (from IdP metadata) **Note:** If you are using the SCIM protocol to provision Fortify Software Security Center with user data from Azure AD, use the value shown in the **Azure AD Identifier** field in Azure. (You can see this field on the SAML-based Sign-on page under **Set up <*application_name*>**.)
SP entity ID	Service provider entity ID value must be a URL that does not exceed 1024 characters, and is globally unique across federations. Fortify recommends that you use the URL of a running Fortify Software Security Center instance.
SP alias	Service provider alias must include only

Field	Description
	alphanumeric characters, colons, dashes, and underscores. It cannot contain slashes, hash marks, semicolons, or question marks. Because this field value plays no significant role, you can specify any general value. For example, you can use `fortify_ssc`.
Keystore location	Location of your keystore that stores the key pair to be used for signing SAML messages and encrypting SAML Assertions **Note:** If IdP metadata is signed, the signature is verified with the PKIX validation algorithm and uses all public keys present in the keystore as trust anchors. Make sure that you include the root CA certificate and intermediary CA certificates of the signature in your keystore.
Keystore password	Keystore file password
Signing & encryption key	Signing/encryption key alias in the keystore file
Signing & encryption key password	Signing/encryption key password
SAML name identifier	Name of the element in the SAML Assertion sent by IdP that holds the authenticated user's username, which matches the Fortify Software Security Center user's username. Use the NameID value if the username is released within the *<NameID>* element. If the username is released within one of the *<Attribute>* elements, provide the name value of the attribute. This information should be available or configurable in your IdP server.

10. Click **SAVE**.
11. Verify that the `host.url` property in `<fortify.home>/<app-context>/conf/app.properties` designates a URL that the IdP server can access. The URL is used as a base URL for constructing

<AssertionConsumerService> and *<SingleLogoutService>* locations in Fortify Software Security Center SAML metadata.

12. If the SAML assertion sent from IdP is encrypted, make sure that the authentication response message is signed.

    Important! If you are integrating with Active Directory Federation Services (AD FS), set the IdP parameter `SamlResponseSignature` to `MessageAndAssertion` (recommended) or `MessageOnly` value.

13. Recent Chrome or Chromium-based browsers default to a `SameSite=Lax` cookie policy, which means that cookies are not sent with sub-requests to third-party sites. As a result, single logout that is not initiated from Fortify Software Security Center does not work correctly.

    Note: Single logout initiated from Software Security Center works correctly, regardless of the cookie policy settings.

    To make single logout work in Chrome or Chromium-based browsers, you must change the `SameSite` policy for session cookies to `None`. Be advised that this denotes a less secure policy than the default, so you must determine whether making the change is the best approach for your organization. To change the policy for container deployments, use the `HTTP_SERVER_SAME_SITE_COOKIES` environment variable. For non-container deployments, add `<CookieProcessor sameSiteCookies="none"/>` to the context section of your Tomcat configuration. For details, see https://tomcat.apache.org/tomcat-9.0-doc/config/context.html#Nested_Components.

14. Restart Fortify Software Security Center.
15. Generate the Fortify Software Security Center (SP) metadata at `<hostname>:<port>/<context>/saml/metadata/<SP_alias>`.
16. Open the metadata generated in previous step and verify that the location URLs in `<AssertionConsumerService>` and `<SingleLogoutService>` are accessible from the IdP server.
17. Upload the Fortify Software Security Center metadata to the IDP server.
18. Try to access `<hostname>:<port>/<app_context>`.

You are redirected to the IdP server, where you can enter your credentials. After successful authentication, the IdP server redirects you back to Fortify Software Security Center.

Note: For information about how to obtain extra logging information related to SSO authentication for Fortify Software Security Center, see "Enabling Debug Logging for Single Sign-On Authentication" on page 161.

Troubleshooting SAML SSO Integration

Issue: After accessing the `<hostname>:<port>/<app-context>/login.jsp` page, a user is not redirected to IdP.

- The login page is excluded from SSO so that a local administrator can access the application and correct the SAML SSO configuration.

Issue: Users are authenticated with IdP, but Fortify Software Security Center does not authorize them.

- The username received in the SAML assertion from IdP does not match any LDAP or local Fortify Software Security Center user (based on user lookup strategy). Verify the following:
  - The "SAML name identifier" in your Fortify Software Security Center SAML configuration is set to an attribute in the SAML assertion that contains the username.
  - The user exists in Fortify Software Security Center and has an assigned role.
  - The user lookup strategy is correctly configured (see "Configuring Core Settings" on page 99).

Issue: You want to set the IdP metadata location as HTTP URL to IdP instead of referencing the IdP metadata locally.

- The configuration accepts the HTTP location but the IdP cannot be behind a proxy server. If the IdP is behind a proxy server, Fortify Software Security Center cannot access the metadata, so the data must be referenced locally.

See Also

"Configuring Fortify Software Security Center to Work with Single Sign-On and Single Logout Solutions that use HTTP Headers" below

Configuring Fortify Software Security Center to Work with Single Sign-On and Single Logout Solutions that use HTTP Headers

To configure Fortify Software Security Center to work with SSO that uses headers:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Configuration**, and then select **SSO**.

   Note: Only one single sign-on solution can be configured for Fortify Software Security Center at a time.
3. From the list of available single sign-on solutions on the SINGLE SIGN ON page, select **HTTP**.
4. Under **HTTP SSO Integration Attributes**, configure the following settings.

Field	Description
HTTP header for username	Type the HTTP header to use for SSO logons.

Field	Description
	The default value is *username*.
IdP login page	Type the URL for the identity provider login page.
SSO Logout page	Type the logout page address to which users are to be redirected after logging out of Fortify Software Security Center.
SSO Logout Response Header	Type the dynamic directive header.
SSO Logout Response Code	Type the dynamic directive code in this box.
SSO Logout Response Text	Type the dynamic directive message in this box.

5. Click **SAVE**.
6. Configure Fortify Software Security Center to use LDAP authentication. For details, see "LDAP User Authentication" on page 108.
7. Restart the server.

Note: For information about how to obtain extra logging information related to SSO authentication for Fortify Software Security Center, see "Enabling Debug Logging for Single Sign-On Authentication" on page 161.

See Also

"Configuring Fortify Software Security Center to Work with Single Sign-On" on page 148

Setting up Kerberos Authentication with Fortify Software Security Center

To set up Kerberos authentication with Fortify Software Security Center.

Caution! SPNEGO/Kerberos SSO may require the transmission of large amounts of data to Fortify Software Security Center via HTTP headers. An insufficient header size limit results in a "Bad Request" error. To increase the header size limit, configure the `maxHttpHeaderSize` property on the Tomcat Server Connector.

1. Create an Active Directory account and register the Service Principal Name (SPN) for the account as follows:

```
setspn -U -S HTTP/SSCServer.mydomain.lan SSCKerberos
```

2. Create a keytab file.

   Example:

```
ktpass -out c:\SSCSERVER.keytab -princ HTTP/
SSCServer.mydomain.lan@mydomain -mapUser mydomain\SSCKerberos -
mapOp set -pType KRB5_NT_PRINCIPAL /crypto all /kvno 0 -pass
3o(t&gSp&3hZ4#t9
```

3. (Linux only) Make sure that, at a minimum, your `krb5.conf` file contains the following:

```
[libdefaults]

   default_realm = EXAMPLE.COM

[realms]
EXAMPLE.COM = {

   kdc = kerberos.example.com

   admin_server = kerberos.example.com

}
```

4. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, select **ADMINISTRATION**.
5. In the left pane of the ADMINISTRATION view, select **Configuration**, and then select **SSO**.

   Note: Only one single sign-on solution can be configured for Fortify Software Security Center at a time.

6. From the **Enabled SSO** list on the SINGLE SIGN ON page, select **SPNEGO/KERBEROS**.
7. Under **SPNEGO/Kerberos Integration Attributes**, provide the information described in the following table.

Field	Description
Service principal name	Service principal name (SPN) of Fortify Software Security Center in the Kerberos realm. The value you specify can include the realm name configured in the Kerberos initialization file.

Keytab location	Location of the keytab file (created in step 2), which contains Fortify Software Security Center principal keys. The location must specify the absolute path to the file using the file URI scheme.
	Windows example:
	`file:///C:/Users/fortify/secrets/krb.keytab`
	Linux example:
	`file:///home/fortify/secrets/krb.keytab`

Krb5.conf location	Location of optional `krb5.conf` file. This sets the `java.security.krb5.conf` property. The location must specify the absolute path to the file using file the URI scheme. See Keytab location for examples.
Enable debug mode	Select this check box to enable debug mode.

8. Click **SAVE**.
9. Check to make sure that the **User username attribute** setting for your LDAP server is correct. (See "Configuring LDAP Servers" on page 111.)
10. Restart the server.
11. Verify that the LDAP user names resolve correctly. Format the LDAP user name values as follows:

```
username@domain
```

12. Check your browser setup, as follows:
    - For Firefox, add the service URL to `network.negotiate-auth.trusted-uris` (`about:config`). For example, `service-machine.my.domain.lan`.
    - For Chrome, add the service URL to your intranet and trusted sites, configure automatic logon only for the local intranet zone settings, and enable integrated Windows authentication.

Important! Check to make sure that the Fortify Software Security Center LDAP configuration username mapping matches the LDAP User entry attribute, where

the attribute holds a username sent in the Kerberos ticket. In configurations that use Microsoft Active Directory, the User Principal Name (UPN) attribute should hold the username sent in the Kerberos ticket. However, verify this before you change configuration settings.

Caution! If Fortify Software Security Center is configured to use the **SPNEGO/Kerberos** SSO solution, and you want users (local and LDAP) to be able to log in using their user names and passwords, you must directly enable it. For instructions, see "Enabling Username and Password Login if Fortify Software Security Center is Configured to Use the X.509 or Kerberos SSO Solution" on the next page.

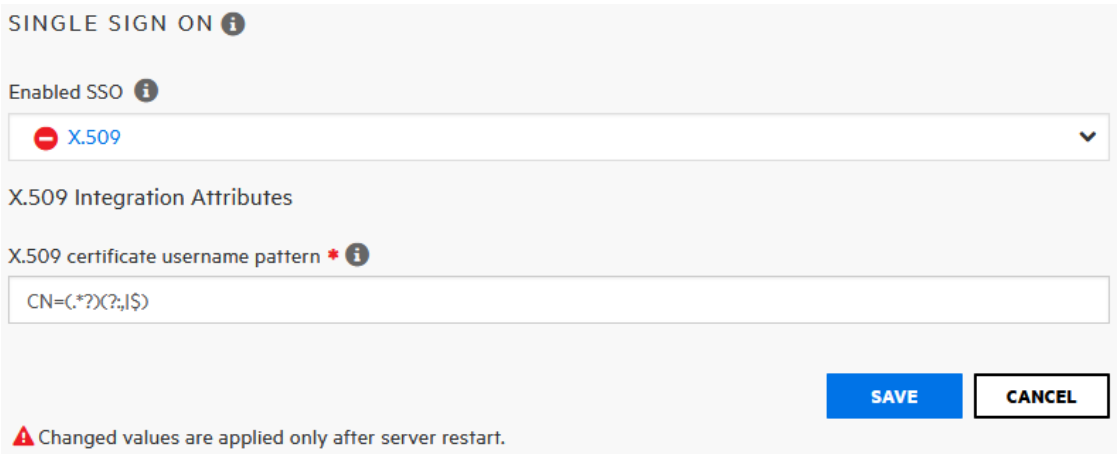
See Also
"Configuring Fortify Software Security Center to Work with Single Sign-On" on page 148

Configuring Fortify Software Security Center to Use X.509 Certification-based SSO

To configure Fortify Software Security Center to use X.509 certification-based SSO:

1. Configure x.509 client certification in Tomcat. See certificateVerification and related options at https://tomcat.apache.org/tomcat-9.0-doc/config/http.html#SSL_Support_-_Certificate for details.
2. Log in to Fortify Software Security Center as an administrator, and then click the **ADMINISTRATION** tab.
3. In the left pane of the ADMINISTRATION view, select **Configuration**, and then click **SSO**.

   Note: You can configure only one sign-on solution for Fortify Software Security Center at a time.

4. From the **Enabled SSO**liston the SINGLE SIGN ON page, select **X.509**.

5. In the **X.509 certificate username pattern** box, type a regular expression for Fortify Software Security Center to specify how to retrieve the username from the client certificate, do one of the following:
   - To retrieve the username from the X.509 certificate Subject field, use a regular expression with capturing groups. The regular expression is then used to match the username from the Subject field value.

     Example: To match the CN attribute of the certificate Subject field, specify the `CN=(.*?)` pattern.
   - To retrieve the username from the X.509 certificate Subject Alternative Name (SAN) extension Other Name, use `$0!OID$regex` pattern, where:
     - `OID` represents the identifier of the Other Name from which to retrieve the username. Only Other Names that contain string values are supported.
     - `regex` represents the regular expression with capturing group to use to retrieve the username from the Other Name value.

     Example: One of the widely used SAN Other Names is User Principal Name (UPN), with `OID1.3.6.1.4.1.311.20.2.3`. Its value takes the form `username@domain`.

     To match the whole `username@domain` under UPN, specify the following pattern:

     ```
     $0!1.3.6.1.4.1.311.20.2.3$(\S+@\S+)
     ```

     To match only the user name before the `@` sign, without the domain, under UPN, specify the following pattern:

     ```
     $0!1.3.6.1.4.1.311.20.2.3$(.+?(?=@))
     ```
6. Click **SAVE**.
7. To implement the configuration, restart the Fortify Software Security Center server.

Caution! If you configure Fortify Software Security Center to use X.509 certification-based SSO, and you want users (local and LDAP) to be able to log in using their user names and passwords, you must directly enable it. For instructions, see "Enabling Username and Password Login if Fortify Software Security Center is Configured to Use the X.509 or Kerberos SSO Solution" below.

Enabling Username and Password Login if Fortify Software Security Center is Configured to Use the X.509 or Kerberos SSO Solution

If Fortify Software Security Center is configured to use the X.509 or Kerberos SSO solution, local login is disabled by default. If you want users (local and LDAP) to be able to log in using their usernames and passwords, you must directly enable local authentication, as follows:

1. Navigate to `<fortify.home>/<app_context>/conf`, and open the `app.properties` file in a text editor.
2. Set the `sso.localAuthenticationEnabled` property to `true`.
3. Save and close the `app.properties` file.
4. Restart the server.

See Also

"Configuring Fortify Software Security Center to Use X.509 Certification-based SSO" on page 159

"Setting up Kerberos Authentication with Fortify Software Security Center" on page 157

Enabling Debug Logging for Single Sign-On Authentication

If you want to get extra logging information related to single sign-on (SSO) authentication for Fortify Software Security Center, you can do so by updating the logging configuration.

To obtain extra logging information related to SSO authentication for Fortify Software Security Center:

1. Go to the `<fortify.home>/<app_context>/conf` directory, and then open the `log4j2.xml` file in a text editor.
2. For single sign-on solutions that use HTTP headers, add the following logger definition to the `log4j2.xml` file:

   ```
   <Logger
   name="com.fortify.manager.web.security.auth.FmHttpSsoAuthenticationFil
   ter" level="debug"/>
   ```
3. For SAML 2.0-compliant single sign-on solutions, locate the section marked `<!-- SSO SAML -->`, and then change the level of each logger in that section to the appropriate debug value.
4. For the CAS single sign-on solution, locate the section marked `<!-- SSO CAS -->`, and then change the level of each logger in that section to the appropriate debug value.

See Also

"Configuring Fortify Software Security Center to Work with Single Sign-On" on page 148

Configuring Web Services to Require Token Authentication

You enable or disable token authentication for web services in the **Configuration** section of the Fortify Software Security Center ADMINISTRATION view.

Fortify Software Security Center supports two types of authentication when the SOAP web services API is used:

- A username and password are provided in every request.
- A temporary security token is generated and passed for authentication.

Token authentication is enabled by default. If you do not want to use token authentication, you must disable it on the WEB SERVICE ATTRIBUTES page.

For additional information about authentication tokens, see "fortifyclient Authentication Tokens" on page 412.

To enable or disable token authentication:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Configuration**, and then select **Web Services**.
3. On the WEB SERVICE ATTRIBUTES page, do one of the following:
   - To enable token authentication, select the **Allow token authentication** check box.
   - To disable token authentication, clear the **Allow token authentication** check box.
4. Click **SAVE**.
5. Restart the server.

Changing Log Levels for Fortify Software Security Center

To change the log level setting for Fortify Software Security Center:

1. Navigate to `<fortify.home>/<app_context>/conf`, and then open the `log4j2.xml` file in a text editor.
2. On line 98, change `<Root level="warn">` to `<Root level="debug">`.
3. Save and close the file.

The modified configuration takes in approximately 10 seconds (as defined by the value of the `monitorInterval` attribute in the configuration).

Note: You cannot add a new logger and set a level for it. Only changes to existing loggers are picked up dynamically.

Configuring Federal Information Processing Standards (for integrating Fortify Software Security Center with Fortify WebInspect Enterprise only)

If you plan to integrate Fortify Software Security Center with Fortify WebInspect Enterprise, you need to enable Federal Information Processing Standards (FIPS) compliance.

To request that OpenSSL be in FIPS mode, at a minimum, you must set the FIPSMode attribute to `on`. To force OpenSSL to enter FIPS mode, set the attribute to `enter` (an error occurs if OpenSSL is already in FIPS mode). To require that OpenSSL already be in FIPS mode (an error occur if OpenSSL is not already in FIPS mode), set the attribute to `require`.

Important! FIPS mode requires that you have a FIPS-capable OpenSSL library, which you must build yourself. If you set the FIPSMode attribute to any of the above values, you must also enable the SSLEngine.

For instructions on how to configure FIPS-compliant cryptography, see the documentation for your operating system.

Customizing the Fortify Banner for Your Organization

You can customize the Fortify banner to display information about your organization's Fortify Software Security Center website either when customers log on, or when they switch between views (DASHBOARD, APPLICATIONS, REPORTS, and so on).

Caution! Each time you upgrade your Fortify Software Security Center instance, you must recreate the banner.

To create a custom Fortify Software Security Center logon experience for your users:

1. Navigate to the `<ssc.war>/WEB-INF/lib` directory.
2. Extract the contents of the `ssc-htmlui-<version>.jar` file into a new directory (referred to as `<new_directory>` in the remaining steps).
3. Navigate to the `<new_directory>/META-INF/resources/html/login` directory.
4. Open the `login.html` file in a text editor.
5. Uncommment the text `<!--<center><font color="red">Add your custom banner here</font></center>-->`, and then specify the HTML elements to set the look, feel, and content of the message displayed where indicated.

The following example adds a banner with red text to the top center of the web page. The banner is displayed whenever the user logs on to Fortify Software Security Center.

```
<center><font color=red size=10>Message_text</font></center>
```

Caution! Space limitations restrict the message text to a single line. Additional lines interfere with user interface display.

6. Change the name of the `ssc-htmlui-<version>.jar` file to `ssc-htmlui-<version>.jar.orig`.
7. Create a new archive named `ssc-htmlui-<version>.jar` that contains all of the files under `<new_directory>`.

   Note: *Do not* include `<new_directory>` itself in the new archive.

8. Restart the Fortify Software Security Center server.

To create a message banner to display each time a user switches views in Fortify Software Security Center (DASHBOARD, APPLICATIONS, REPORTS, and so on):

1. Navigate to the `<ssc.war>/WEB-INF/lib` directory.
2. Extract the contents of the `ssc-htmlui-<version>.jar` file into a new directory (referred to as `<new_directory>` in the remaining steps).
3. Navigate to the `<new_directory>/META-INF/resources/html/ssc` directory.
4. Open the `index.html` file in a text editor, and then go to line 41.
5. Uncomment the text `<div style="text-align: center;"><span style="color: red; ">Add your custom banner here</span></div>`, and then specify the HTML elements to set the look, feel, and content of the message displayed where indicated.

   The following example adds a banner with red text to the top center of the web page. The banner is displayed whenever the user logs on to Fortify Software Security Center.

   ```
   <div style="text-align: center;"><span style="color: red; "> Message text x</span></div>
   ```

   Caution! Space limitations restrict the message text to a single line. Additional lines interfere with user interface display.

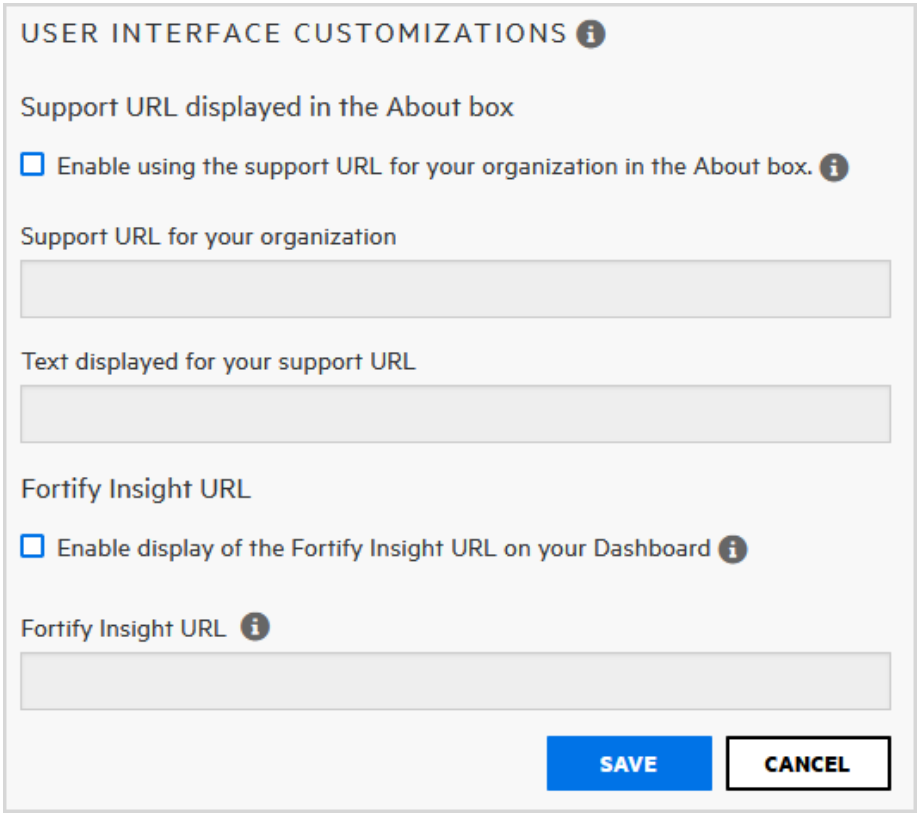
6. Change the name of the `ssc-htmlui-<version>.jar` file to `ssc-htmlui-<version>.jar.orig`.
7. Create a new archive named `ssc-htmlui-<version>.jar` that contains all of the files and directories under `<new_directory>`.
8. Restart the Fortify Software Security Center server.

Adding a Fortify Insight Link to the Dashboard

If you have purchased Fortify Insight, you can link your Fortify Software Security Center to your Fortify Insight dashboard by adding a Fortify Insight link to your Fortify Software Security Center Dashboard.

To add the Fortify Insight link to your Fortify Software Security Center Dashboard:

1. Log in to Fortify Software Security Center as an administrator user.
2. On the Fortify header, click **ADMINISTRATION**.
3. In the left pane, expand **Configuration**, and then select **Customization**.



4. Under **Fortify Insight URL**, select the **Enable display of the Fortify Insight URL on your Dashboard** check box.
5. In the **Fortify Insight URL** box, enter the URL for your Fortify Insight page.
6. Click **SAVE**.

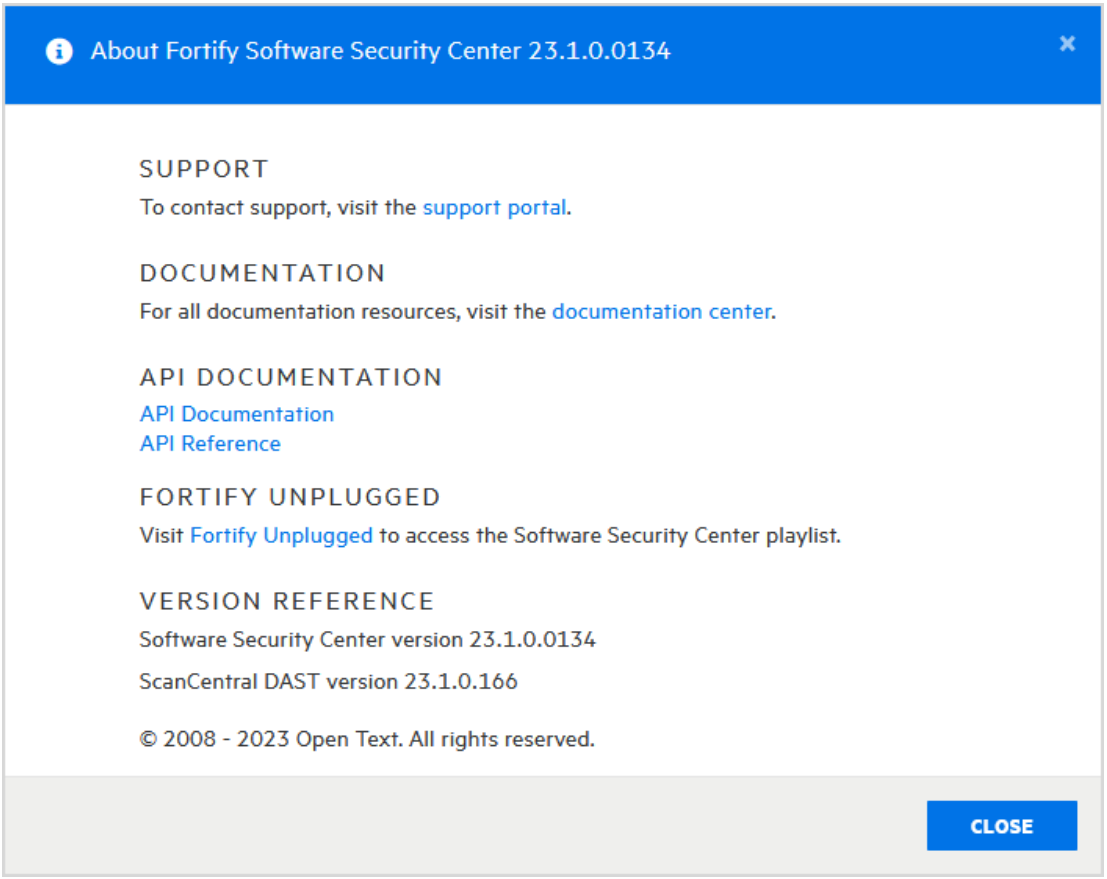
See Also

"Customizing the Fortify Banner for Your Organization" on page 163

"Changing the Support Contact Link in the About Fortify Software Security Center Box" on the next page

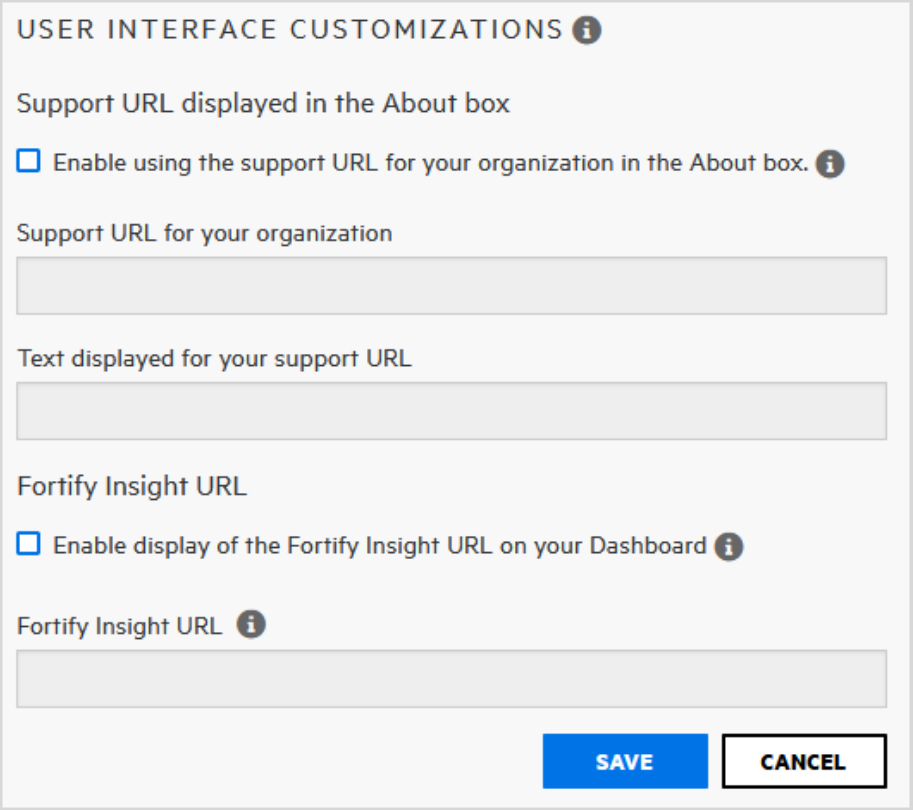
Changing the Support Contact Link in the About Fortify Software Security Center Box

By default, the About Fortify Software Security Center *<version>* box displays a link to the Support portal. You can replace that link with a link to the support portal for your organization.



To display your support portal in the About Fortify Software Security Center box:

1. Log in to Fortify Software Security Center as an administrator user.
2. On the Fortify header, click **ADMINISTRATION**.
3. In the left pane, expand **Configuration**, and then select **Customization**.



4. Select the **Enable using the support URL for your organization in the About box** check box.
5. In the **Support URL for your organization** box, enter the URL for the support portal for your organization.
6. In the **Text displayed for your support URL** box, type the text to display in the new link to support.
7. Click **SAVE**.

See Also

"Customizing the Fortify Banner for Your Organization" on page 163

"Adding a Fortify Insight Link to the Dashboard" on page 165

Customizing Fortify Software Security Center Logging

To customize logging for a Fortify Software Security Center instance, you can provision a custom `log4j2` configuration file to override or add to the standard `log4j2` configuration file in *<fortify.home>*`/`*<app_context>*`/conf`.

To provision the custom `Log4j2` configuration override file, set the `COM_FORTIFY_SSC_LOG4J2_OVERRIDE` system environment variable or the `com.fortify.ssc.log4j2.override` JVM system property to an absolute path for the custom `Log4j2` XML configuration file.

Fortify strongly recommends that you use one of these methods rather than modifying the *<fortify.home>*/*<app_context>*/conf/log4j2.xml file directly because it provides you with better control.

Setting the Required Password Strength for Fortify Software Security Center Login

You can use the password.strength.min.score property (located in *<fortify.home>*/*<app_context>*/conf/app.properties) to adjust the required password strength. The following table lists the valid values and the strength each represents.

Value	Password Strength
0	Poor
1	Weak
2	Medium
3	Strong
4	Very strong

Password strength is not determined based on requirements such as one upper-case character, one special character, and so on. Instead, it is calculated based on a dedicated password strength library that uses methods such as estimating the time to crack the password, determining whether the password contains predictable character sequences or a username, and checking against common password dictionaries.

See Next

"About Session Logout" on page 79

"Additional Fortify Software Security Center Configuration" on page 82

Chapter 7: Additional Installation-Related Tasks

This section addresses additional tasks related to a new Fortify Software Security Center installation.

Blocking Data Export to CSV Files

By default, users can export Fortify Software Security Center data displayed in the Dashboard and AUDIT views to comma-separated values (CSV) files. You can block this functionality.

To prevent users from exporting Fortify Software Security Center data to CSV files:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, click **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Configuration**, and then select **Core**.
3. Scroll to the bottom of the Core page, and then clear the **Enable Export to CSV** check box.
4. Click **SAVE**.

See Also

"Configuring Core Settings" on page 99

"Exporting Data to Comma-Separated Values Files" on page 216

About Bug Tracker Integration

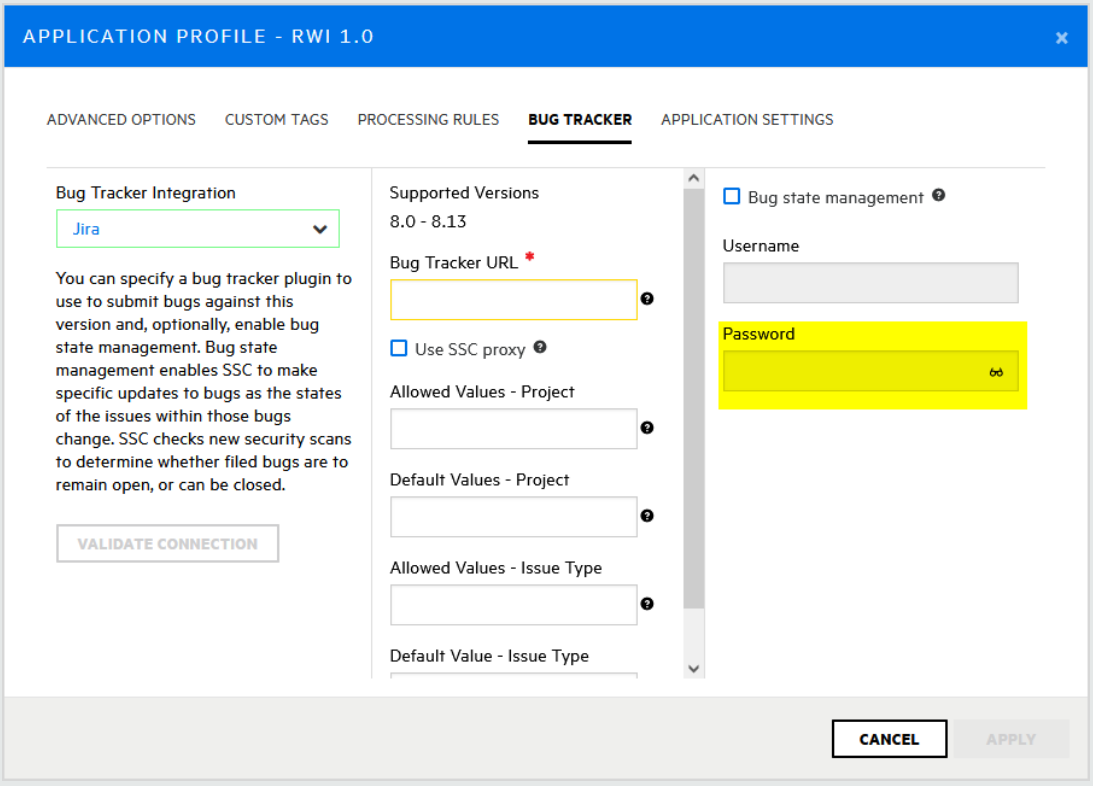
Fortify Software Security Center enables your team to submit bugs to your bug tracking system from Fortify Software Security Center during issue auditing. Fortify Software Security Center supports integration with the following bug tracking systems:

- Bugzilla

  Note: Integration with the Bugzilla bug tracker plugin requires that you enable XML-RPC in Bugzilla. For instructions, see https://www.bugzilla.org/docs/4.4/en/html/api/Bugzilla/WebService/Server/XMLRPC.html

- Jira
- Jira Cloud

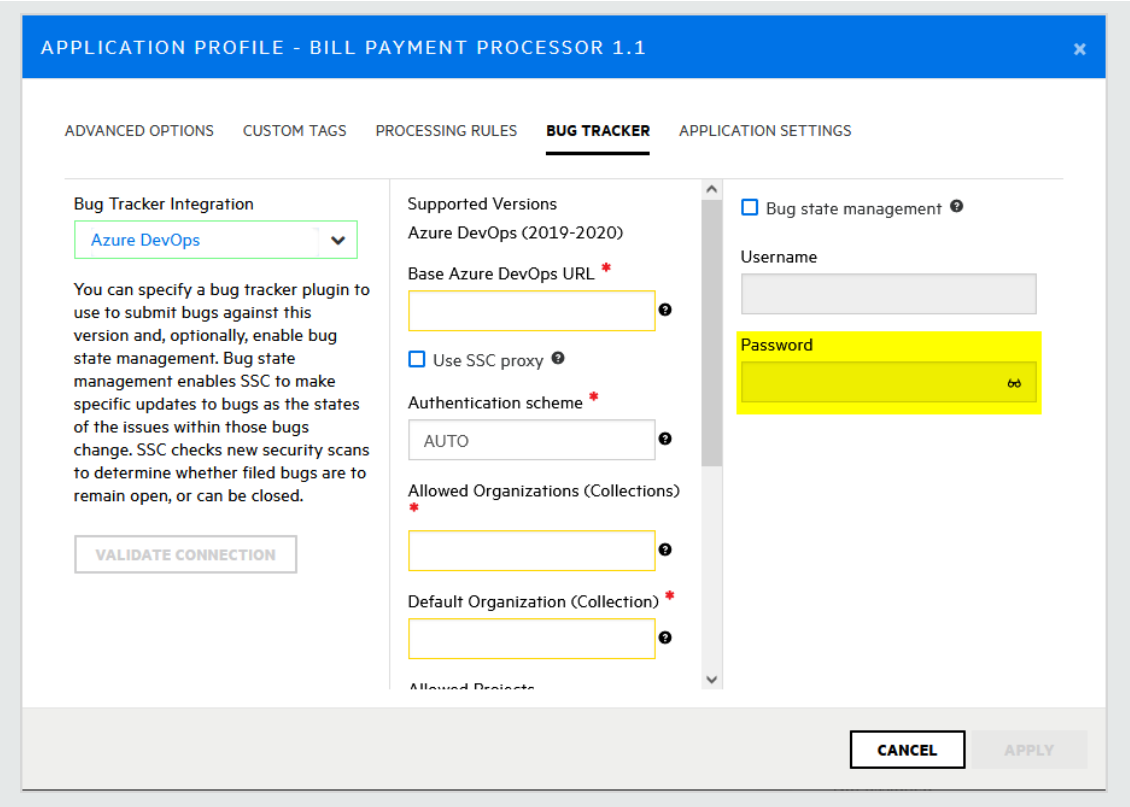
Note: If you use Jira Cloud, you must use your Jira authentication token in the **Password** field at login.



- ALM
- Azure DevOps Server

Important! The **Repro Steps** field in Azure DevOps, which displays Fortify bug descriptions, is hidden by default for issue work items. If you use Azure DevOps 2019.1 or later version, and you use the Basic process, you must customize Issue work items to see the **Repro Steps** field.

Important! If you use Azure DevOps, you must use a personal access token generated from Azure DevOps in the **Password** field at login. For information about Azure DevOps personal access tokens, see https://learn.microsoft.com/en-us/azure/devops/organizations/accounts/use-personal-access-tokens-to-authenticate?view=azure-devops&tabs=Windows.



Note: If your organization uses a bug tracking system other than those that Fortify supplies, you can author a new plugin for that system. For instructions, see "Authoring Bug Tracker Plugins" on page 423.

For information about how to set up and use bug tracking systems to manage the security vulnerabilities for your application versions, see "Using Bug Tracking Systems to Help Manage Security Vulnerabilities" on page 255.

Managing Bug Tracker Plugins

The following sections describe how to add and remove bug tracker plugins to and from the system.

Important! Successful integration with the Bugzilla bug tracker plugin requires that you enable XML-RPC in Bugzilla. For instructions, see https://www.bugzilla.org/docs/4.4/en/html/api/Bugzilla/WebService/Server/XMLRPC.html.

Adding Bug Tracker Plugins

If you are a Fortify Software Security Center administrator, you can connect Fortify Software Security Center to third-party bug tracker plugins.

Important! Using a proxy with authentication and an https bug-tracker domain does not work. For a successful connection, use one of the following:
- Proxy with authentication plus http://bugtracker.domain.com
- Proxy without authentication plus https://bugtracker.domain.com
- Proxy without authentication plus http://bugtracker.domain.com

To add a bug tracker plugin to the system:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, select **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Plugins**, and then select **Bug Tracking Plugins**.
3. On the Bug Tracking page header, click **NEW**.

   Fortify Software Security Center displays the UPLOAD PLUGIN WARNING dialog box.
4. Read the warning and, if you accept the potential risk involved in uploading the plugin, click **OK**.
5. In the UPLOAD PLUGIN BUNDLE dialog box, click **BROWSE**, and then locate and select the JAR file for your plugin. You can use either a Fortify Software Security Center-provided JAR file, or the JAR file for a bug tracker plugin that you have authored (see "Authoring Bug Tracker Plugins" on page 423).

   You can find the JAR files for the bug trackers that Fortify Software Security Center provides in the following locations.

Bug Tracker Plugin	Directory/File
Bug Tracker Plugin for ALM	*<ssc_install_dir>*/ plugins/BugTrackerPluginAlm/ com.fortify.BugTrackerPluginAlm-*<version>*.jar
Bug Tracker Plugin for Bugzilla	*<ssc_install_dir>*/plugins/BugTrackerPluginBugzilla/ com.fortify.BugTrackerPluginBugzilla-*<version>*.jar
Bug Tracker Plugin for Jira	*<ssc_install_dir>*/plugins/BugTrackerPluginJIRA7/ com.fortify.BugTrackerPluginJira7-*<version>*.jar
Bug Tracker Plugin for Azure DevOps	*<ssc_install_dir>*/plugins/BugTrackerPluginTFS/ com.fortify.BugTrackerPluginTFS-*<version>*.jar

6. Click **START UPLOAD**.

   After the upload is completed, the Bug Tracking table lists the new plugin.
7. To enable the bug tracker plugin, click **ENABLE**.

The **Plugin State** field for the plugin now displays the value **ENABLED**.

See Also

"Assigning a Bug Tracking System to an Application Version" on page 260

Removing Bug Tracker Plugins

If you are a Fortify Software Security Center administrator, you can remove third-party bug tracker plugins from the system.

To remove a bug tracker plugin from the system:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, select **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Plugins**, and then select **Bug Tracking Plugins**.
3. On the Bug Tracking page, expand the row for the plugin you want to remove.
4. Click **Disable**, and then, after the plugin is disabled, click **REMOVE**.

See Also

"About Bug Tracker Integration" on page 169

"Adding and Managing Parser Plugins" on page 175

"Authoring Bug Tracker Plugins" on page 423

Securing Logon Credentials for Bug Tracking Systems

When you file a bug from Fortify Software Security Center, you provide a username and password for the bug tracking system. The username and password pair is saved in the HTTP session and mapped to the bug tracker for each application.

Each bug tracker has a different set of bug parameters and requires different user input. These parameters are dynamic and could be fetched from the bug-tracking system itself. Default values may be provided for some parameters.

After you complete and save the bug settings, a bug is created on the bug tracking system and Fortify Software Security Center saves the bug ID for the issue.

Important! If Fortify Software Security Center is configured to communicate over SSL, you must also import the required bug tracker certificates to the java virtual machine where Fortify Software Security Center is deployed.

Bug Tracker Parameters

A bug submitted with a bug tracker requires that a standard summary and bug description be entered in the **Submit Bug** dialog box. You can also add values for priority level, a due date for the fix, and the assignee. Fortify Software Security

Center fetches values for the **Issue Type** and **Affects version** fields dynamically from the bug tracking system based on the selected application.

If your application requires additional fields, you might need to modify the plugin before you use it. For instructions, see "Authoring Bug Tracker Plugins" on page 423 or contact Fortify Support (https://www.microfocus.com/support).

ALM Parameters

In the Submit Bug dialog box for the ALM defect tracker, you select the parameters that reflect your ALM installation:

- Bug Summary
- Bug Description
- ALM Domain
- ALM Project
- Severity

If your ALM project integrates with ALI (details below) you can see that the defect description includes candidate changesets that could have introduced the issue.

There are several key points of ALM integration to remember. For changeset discovery to be functional, the following conditions must be met:

- Each Fortify Static Code Analyzer scan must be tagged with a build-label, which Fortify Software Security Center uses to map the scan with a source-control revision number. To do this, include the `-build-label <SVN_Revision_Number>` command option when you run the source analyzer tool to translate source code into the analysis model.
- You must enable the ALI extension for the individual project in ALM and configure appropriate source control repositories. If the ALI extension is successfully enabled for the individual project, you can view the **Code Changes** tab after you log in to ALM.
- ALM bugs are logged, regardless of whether the changeset discovery requirements are met. If the prerequisites are not met, then the changeset discovery message is skipped.
- Currently, Subversion is the only source control repository supported for changeset discovery.

Note: To view an ALM bug, you must have the ALM browser plugin installed and use an ALM-compatible browser.

For more information about ALI and ALM, see the documentation for those products.

Adding and Managing Parser Plugins

If you are a Fortify Software Security Center administrator, you can connect Fortify Software Security Center to third-party parser plugins.

Tip: You can write your own parser plugin for Fortify Software Security Center. For instructions, see the "Sample parser plugin" page on GitHub (https://github.com/fortify/sample-parser).

To add a parser plugin to the system:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Plugins**, and then select **Parser Plugins**.
3. On the Parsers page header, click **NEW**.

   Fortify Software Security Center displays the Upload Plugin Warning to advise you of the risk of uploading third-party plugins.
4. To acknowledge the warning and continue, click **OK**.
5. In the Upload Plugin Bundle dialog box, click **BROWSE**, and then locate and select the bundle file (JAR file) for your plugin.
6. Click **START UPLOAD**.

   The Parsers page lists the plugin you uploaded.
7. To expand the row that displayed the parser name, click it.
8. To enable the parser plugin, click **ENABLE**.

   Fortify Software Security Center displays the Enable Plugin Warning to advise you of the risk of enabling untested plugins.
9. Click **OK**.

See Also

"Managing Bug Tracker Plugins" on page 171

Preparing Fortify Software Security Center to Display Sonatype Results

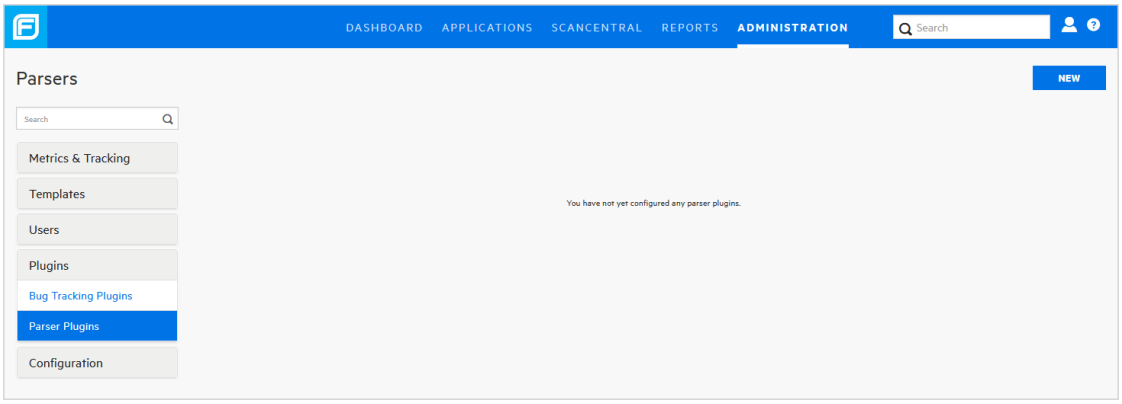
You can view open source security data from Sonatype's Nexus Lifecycle solution scan results for an application version from the AUDIT page or from the OPEN SOURCE page in Fortify Software Security Center. To do so, you must first download and install the required Sonatype Parser Plugin. After you do, Sonatype scan results uploaded to Fortify Software Security Center (using Fortify SourceAndLibScanner) are visible.

To obtain Fortify SourceAndLibScanner, go to https://marketplace.microfocus.com/cyberres/content/fortify-sourceandlibscanner. For information about how to use SourceAndLibScanner to upload open Sonatype scan results to Fortify Software Security Center, see the *Micro Focus Fortify*

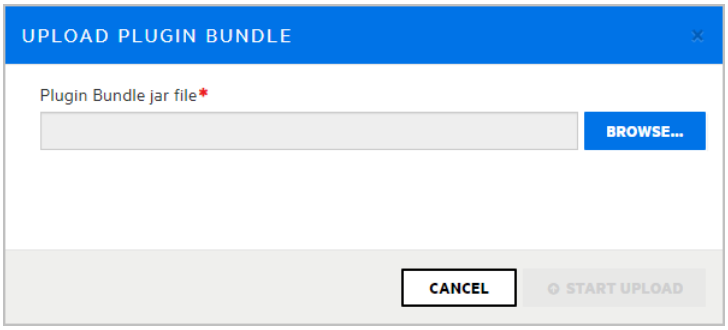
SourceAndLibScanner User Guide, which is packaged with the Fortify SourceAndLibScanner utility.

To prepare Fortify Software Security Center to display uploaded Sonatype data:

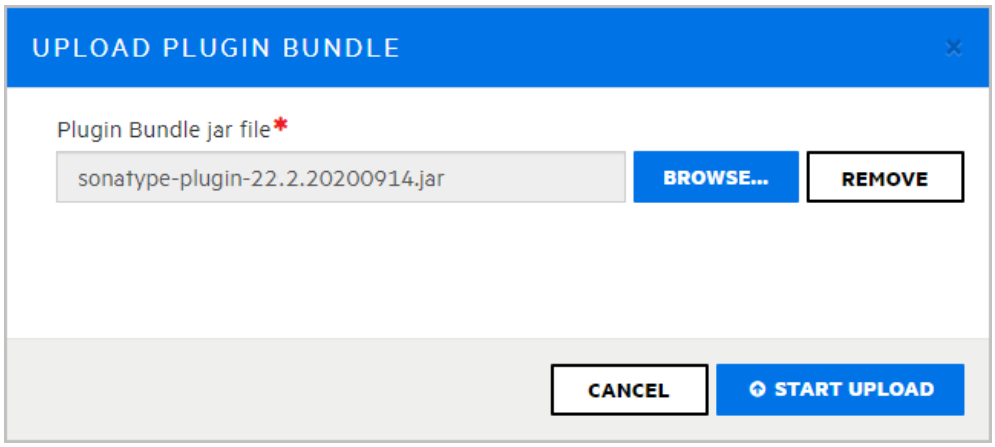
1. Open a browser window and navigate to the Fortify Marketplace (https://marketplace.microfocus.com/cyberres/content/sonatype-nexus-lifecycle-integration-with-ssc).
2. On the **Sonatype Nexus Lifecycle integration with SSC** page, click **DOWNLOAD**.
3. Unzip the `SonatypeFortifyBundle.zip` file contents to a local directory.
4. Log on to Fortify Software Security Center as an administrator.
5. On the Fortify header, select **ADMINISTRATION**.
6. In the left pane, expand the **Plugins** section, and then select **Parser Plugins**.



7. On the Parsers page, click **NEW**.
8. To dismiss the UPLOAD PLUGIN WARNING, click **OK**.



9. In the UPLOAD PLUGIN BUNDLE dialog box, click **BROWSE**, and then navigate to and select the `sonatype-plugin-<version>.jar` file.



10. In the UPLOAD PLUGIN BUNDLE dialog box, click **START UPLOAD**.
    Fortify Software Security Center displays a message to let you know the upload was successful. The Parsers page now lists the Sonatype Vulnerability Parser.
11. Expand the row for the Sonatype Vulnerability Parser, and then click **ENABLE**.
12. Read the ENABLE PLUGIN WARNING, and then click **OK**.

See Also

"Uploading Scan Artifacts" on page 311

"About Susceptibility Analysis of Web Applications" on page 370

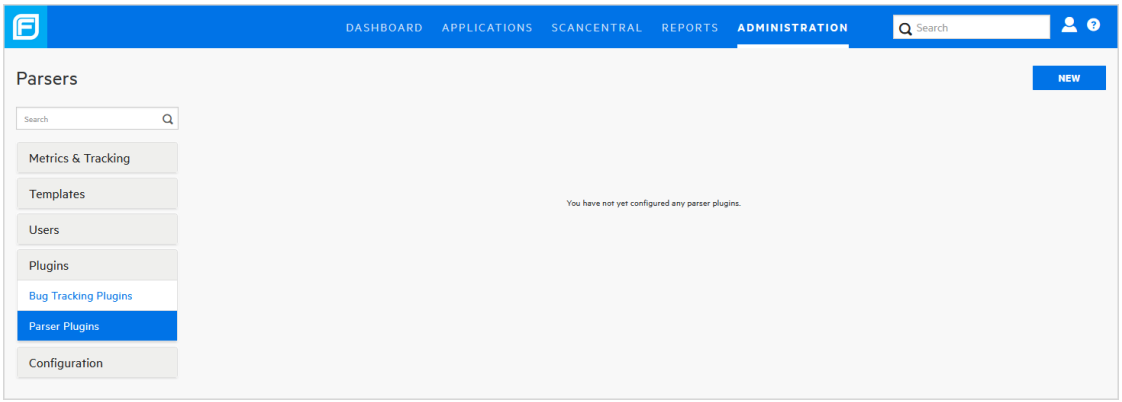
Preparing Fortify Software Security Center to Display Debricked Results

You can view open source security data from Debricked and view the scan results from the AUDIT page or from the OPEN SOURCE page in Fortify Software Security Center. To do so, you must first download and install the required parser plugin. After you do, the open source scan results uploaded to Fortify Software Security Center are visible.

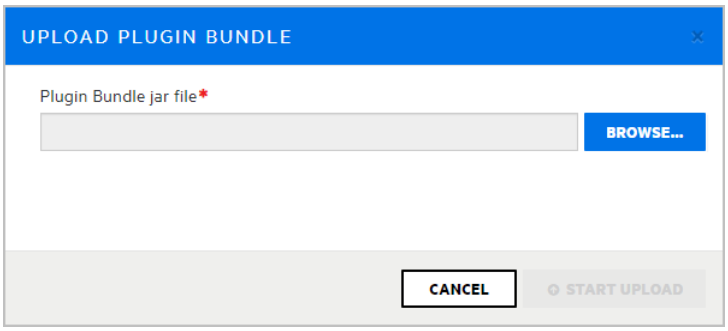
To prepare Fortify Software Security Center to display Debricked data:

1. Open a browser window and navigate to https://github.com/fortify/fortify-ssc-parser-debricked-cyclonedx/releases.
2. Click (expand) **Assets** and select one of the following:
   - To download a parser that enables the display of Debricked data on both the AUDIT and OPENSOURCE pages in Fortify Software Security Center, select `fortify-ssc-22.2+-parser-debricked-cyclonedx-1.0.0.zip`.
   - To download a parser that enables the display of Debricked data on only the AUDIT page in Fortify Software Security Center, select `fortify-ssc-parser-debricked-cyclonedx-1.0.0.zip`.
3. Go to your **Downloads** folder and extract the contents of the downloaded ZIP file to a local directory.

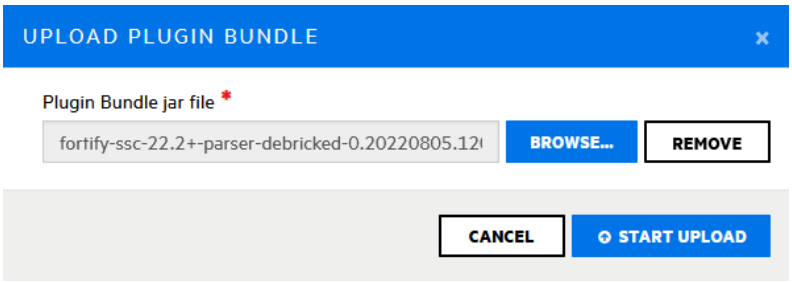
4. Log on to Fortify Software Security Center as an administrator.
5. On the Fortify header, select **ADMINISTRATION**.
6. In the left pane, expand the **Plugins** section, and then select **Parser Plugins**.



7. On the Parsers page, click **NEW**.
8. To dismiss the UPLOAD PLUGIN WARNING, click **OK**.



9. In the UPLOAD PLUGIN BUNDLE dialog box, click **BROWSE**, and then navigate to and select the extracted JAR file.



10. In the UPLOAD PLUGIN BUNDLE dialog box, click **START UPLOAD**.

    Fortify Software Security Center displays a message to let you know the upload was successful. The Parsers page now lists the Debricked parser plugin for SSC.
11. Expand the row for the Debricked parser plugin, and then click **ENABLE**.
12. Read the ENABLE PLUGIN WARNING, and then click **OK**.

See Also

"Uploading Scan Artifacts" on page 311

"Viewing Open Source Data" on page 367

Administrator Accounts

Users who have Administrator accounts have complete access to all Fortify Software Security Center user and application version data and can manage the entire Fortify Software Security Center system. Only users who have Administrator accounts can create, edit, or delete other user accounts. To change a local user account, you must be a local administrator.

Fortify recommends that you create only the Administrator-level accounts necessary to create and edit local or LDAP Fortify Software Security Center user accounts. The Security Lead and lesser accounts can perform all other application-related activity.

Fortify Software Security Center permits the explicit addition of Administrator-level accounts to application versions. This enables Administrator users to be assigned issues from the AUDIT page.

See Also

"Viewing Permission Information for Fortify Software Security Center Roles" on page 181

About Fortify Software Security Center User Administration

This section provides information about the different types of Fortify Software Security Center user accounts and how to create these accounts for your users.

Topics covered in this section:

Fortify Software Security Center User Accounts

In addition to the administrator-level account used to administer user accounts, Fortify Software Security Center supports the following user account types, in descending order of level of authority:

- **Administrator**: An Administrator has access to all application versions and can perform all actions in the system.
- **Security Lead**: A Security Lead has access to all administrative operations except user account creation and editing. The Security Lead can create application versions and edit all aspects of the versions that they created or to which they are assigned.
- **Manager**: A Manager has read-only access to most administrative data. Managers can create and edit all data for the application versions to which they are assigned.
- **Developer**: A Developer has read-only access to some administrative data. Developers can create and edit a subset of data for the application versions to which they are assigned.
- **View-Only**: A View-Only user can view general information and issues for application versions to which he has access. A View-Only user cannot upload analysis results or audit issues.
- **Application Security Tester**: An Application Security Tester can perform operations that pertain to execution of dynamic scan requests. An Application Security Tester can view application versions, view and generate reports, process dynamic scans, upload results and audit issues.
- **WebInspect Enterprise System**: Users assigned the Fortify WebInspect Enterprise System role can register and de-register a Fortify WebInspect Enterprise instance from Software Security Center and can retrieve issue audit information. This role is intended for Fortify WebInspect Enterprise use only.

For more information about user accounts, see "User Accounts and Access" on page 208.

Related Topics

"About Creating User Accounts" below

"Unlocking Local User Accounts" on page 229

About Creating User Accounts

The Fortify Software Security Center Users module provides the tools you use to edit, delete, or suspend local user accounts.

Fortify recommends that after you log on to Fortify Software Security Center for the first time, you create at least one non-default administrator account, and then delete the default administrator account.

After you create the non-default administrator account, use the new account to create the user accounts.

Note: As a Fortify Software Security Center administrator, you can delete or suspend all user accounts except for the last remaining administrator-level

account. Fortify Software Security Center automatically disables the suspend and delete features for such an account.

For instructions on how to create a user account, see "Creating Local User Accounts" on page 225.

For information about how to configure Fortify Software Security Center user account timeout and lockout settings, see "Configuring Core Settings" on page 99. For more information about user account privileges, see "Fortify Software Security Center User Account Management" on page 221.

See Also

"Viewing Permission Information for Fortify Software Security Center Roles" below

"Unlocking Local User Accounts" on page 229

Preventing Destructive Library and Template Uploads to Fortify Software Security Center

Caution! A malicious user might modify a report library or template so that it contains arbitrary and potentially destructive SQL queries and commands. Upload only libraries and templates that are written by trusted users and that have been reviewed for malicious queries and commands.

Only users who have permission to manage report definitions and libraries can upload custom report libraries and templates to Fortify Software Security Center. To prevent templates that execute arbitrary and potentially destructive commends from being uploaded to Fortify Software Security Center, make sure that you:

- Assign access permissions to trusted users only.
- Check all custom templates for arbitrary SQL queries and commands before you upload them to Fortify Software Security Center.

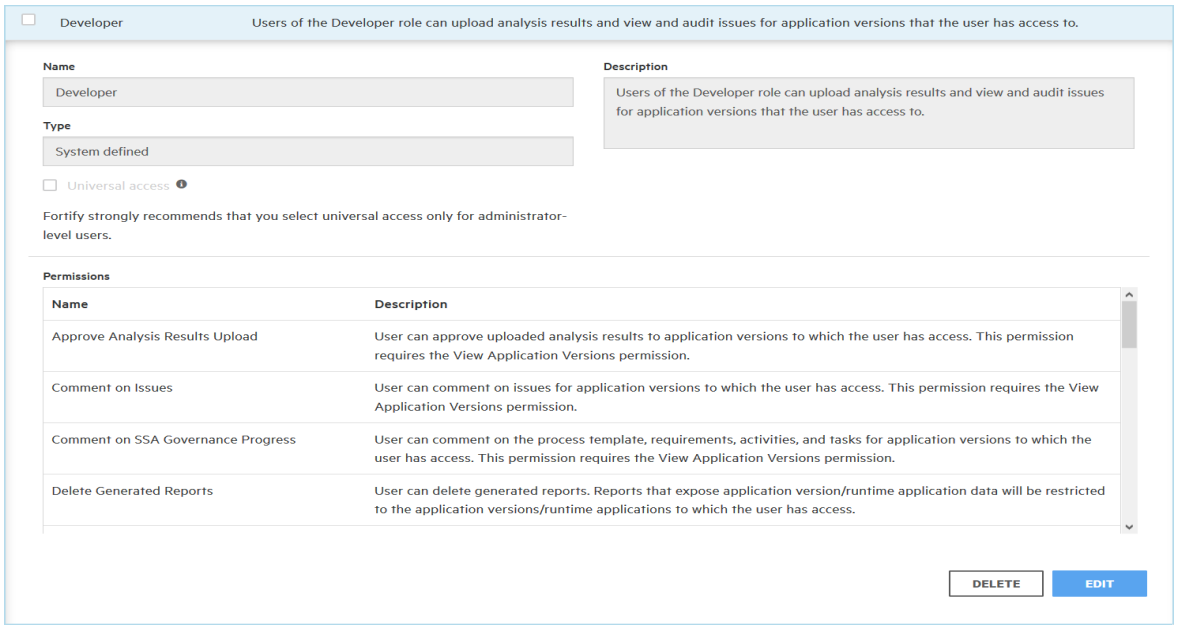
Viewing Permission Information for Fortify Software Security Center Roles

To view detailed information about the actions that users assigned the various Fortify Software Security Center roles can perform:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Users**, and then select **Roles**.

   The Roles page lists the names and descriptions of all of the roles in the system.
3. Select the row for the role you are interested in.

The row expands to reveal details for the role, including a table that lists all of the permissions granted to users assigned that role.



For more information about user accounts, see "Managing User Accounts" on page 221.

Related Topics

"About Creating User Accounts" on page 180

"Pre-configured Roles" on page 221

"Unlocking Local User Accounts" on page 229

About Managing LDAP User Roles

A relative distinguished name (RDN) further qualifies a base distinguished name (DN). For example, if the base DN for a given LDAP directory is `dc=domainName, dc=com,` and the full DN is `cn=group1,ou=users,dc=domainName,dc=com,` then the RDN is `cn=group1,ou=users.`

The topics in this section describe how to use LDAP RDNs to determine user roles.

Group Membership in Fortify Software Security Center

For Fortify Software Security Center to recognize a user as a member of a particular group, the user account must refer to a group object in the LDAP directory. When the user logs on, Fortify Software Security Center looks up the user in the LDAP directory. Fortify Software Security Center determines the user's group by the common name (CN) specified in the group membership attribute. If the user belongs to multiple groups, and those groups are mapped to different roles, Fortify Software Security Center assigns the user all roles.

Fortify Software Security Center supports nested groups. For example, if a user is a member of group A and group A is a member of group B, Fortify Software Security Center recognizes that the user is a member of both groups.

Important! Use nested LDAP groups only if you absolutely must. Enabling nested LDAP groups forces Fortify Software Security Center to perform extra tree traversals during authentication. Fortify strongly recommends that you clear this check box if you do not plan to use nested groups.

See Also

"Handling Failed LDAP User Logins" below

Handling Failed LDAP User Logins

If you have configured nested LDAP groups for your Fortify Software Security Center server, and LDAP authentication fails during an attempted login because of incorrect credentials, then the log includes a message about bad credentials. However, if the log contains the text "user is not authorized," check the following:

- Is the user registered in Fortify Software Security Center and assigned a role? Check with the LDAP administrator to determine whether the user is actually a member of the group to which they are assumed to belong.
- If user does belong to the LDAP group, check to see whether that the group is registered with Fortify Software Security Center and assigned a role.
- Special case: If the user belongs to the LDAP group that is registered to Fortify Software Security Center, but was added to the group only within the last few hours, refresh the LDAP cache manually or wait a few hours for it to automatically refresh.

To manually request an LDAP cache refresh:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Users**, and then select **LDAP Entities**.
3. Select the check box for the LDAP server.
4. On the LDAP page header, click **REFRESH**.
5. To determine whether the LDAP cache refresh has completed, from the ADMINISTRATION view, check either the Event Logs page or the Jobs page.

Note: An LDAP cache refresh can take a long time to complete.

See Also

"Group Membership in Fortify Software Security Center" on the previous page

About Mapping Fortify Software Security Center Roles to LDAP Groups

In most environments, the LDAP directory contains some users who do not need access to Fortify Software Security Center. Also, certain groups of users may require different access privileges.

Before you configure LDAP user authorization, you must decide which LDAP groups to associate with the Fortify Software Security Center roles (Administrator, Manager, Developer, and Auditor). Fortify recommends that you create new LDAP groups that map directly to the different Fortify Software Security Center roles. For example, you might create a FORTIFY_ADMINS group and a FORTIFY_DEVELOPERS group.

Global Search Functionality in Fortify Software Security Center

Fortify Software Security Center provides global, category-based search functionality that applies search terms across application versions, issues, reports, comments, and users. Newly added documents (artifacts, application versions, users) are indexed automatically and immediately.

You can enable global searches during configuration at first login or after an upgrade. (See "Configuring Fortify Software Security Center for the First Time" on page 72.)

Note: Indexing of uploaded FPR files is not immediate because it is performed as a separate Index New Issues job, which is scheduled to occur at the end of an artifact upload job.

To enable global searching on your Fortify Software Security Center server, you must provide Tomcat Server with read and write access to the search index directory.

Recommended disk size

The optimum disk size for the requisite indexing for global searches varies based on the characteristics of the data, but the Lucene indexes are much smaller than the data in the database. For example, the index size required for a database issue volume of 18 GB (with db indexes) is approximately 2 GB.

See Also

Troubleshooting Search Index Issues

About Global Search Functionality

Fortify Software Security Center provides global, category-based search functionality that applies search terms across application versions, issues, reports,

comments, and users. You can enable global searches during configuration at first login or after an upgrade. (See "Configuring Fortify Software Security Center for the First Time" on page 72 or "Configuring Fortify Software Security Center After an Upgrade" on page 198.)

Recommended disk size

The optimum disk size for the requisite indexing for global searches varies based on the characteristics of the data, but the Lucene indexes are much smaller than the data in the database. For example, the index size required for a database issue volume of 18 GB (with db indexes) is approximately 2 GB.

See Also

"Global Search Functionality in Fortify Software Security Center" on the previous page

"Troubleshooting Search Index Issues" below

Troubleshooting Search Index Issues

As an indicator of search index health, the search index directory (specified in the configuration wizard) includes the marker file `healthy.index`. If this file is not present in the search index directory, Fortify Software Security Center attempts to recreate the index on each startup.

If Fortify Software Security Center repeatedly fails to create the initial index, remove the entire index directory, and then restart Fortify Software Security Center.

If you are working with a very large database (hundreds of GB), the Full Reindex job may fail because of limited system memory. If this occurs, increase the Java heap size for Fortify Software Security Center and then restart Fortify Software Security Center. (For minimum and recommended values for java heap size, see the *Micro Focus Fortify Software System Requirements* document.)

Search Index Maintenance

The *index maintenance* job, which is performed once a day, keeps the index healthy. You can change its run time from the ADMINISTRATION view. Fortify recommends that this job be scheduled to run once a day. For instructions on how to re-schedule executed jobs, see "Configuring Job Scheduler Settings" on page 135.

Placing Fortify Software Security Center in Maintenance Mode

If, at any time, you need to change any server configuration settings, you can place Fortify Software Security Center in maintenance mode, and then make the

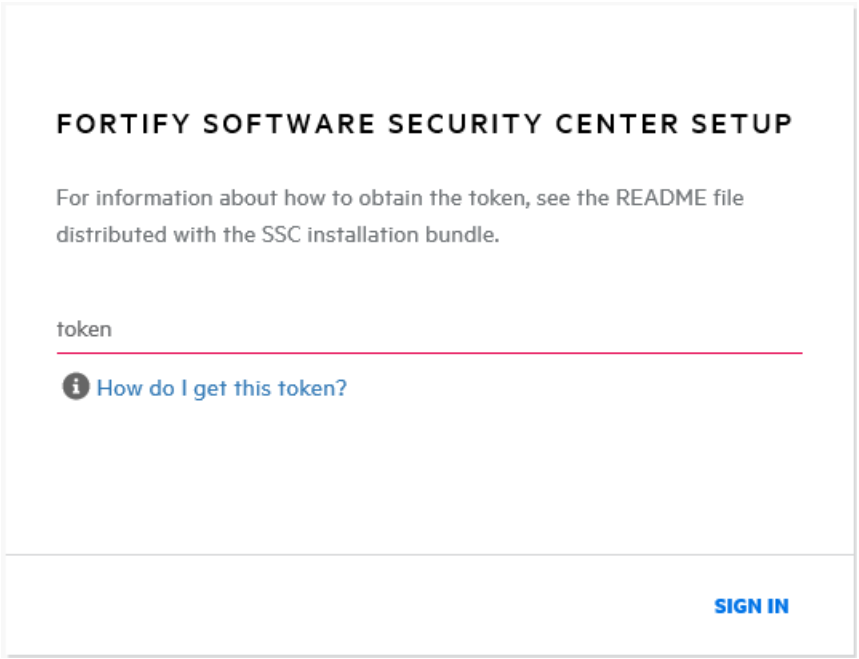
necessary changes.

To place Fortify Software Security Center in maintenance mode:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Configuration**, and then select **Maintenance** .
3. On the Maintenance page, select the **Set to maintenance mode** check box, and then click **SAVE**.
4. Restart the server.
5. Go to the `<fortify.home>/<app_context>` directory, and open the `init.token` file.
6. Copy the contents of the `init.token` file to the clipboard.
7. Open a web browser window and type the URL for your Fortify Software Security Center instance.

8. In the upper right corner of the Fortify Software Security Center Setup screen, click **ADMINISTRATORS**.

9. Paste the string you copied from the `init.token` file in the text box, and then click **SIGN IN**.

   The Fortify Software Security Center Setup wizard displays all of the current configuration settings. For information about server configuration, see "Configuring Fortify Software Security Center for the First Time" on page 72.
10. After you successfully complete the server configuration, restart Tomcat.

Note: Alternatively, you can set the following Java option to re-initialize the setup wizard after you complete the setup: `-Dcom.fortify.ssc.forceInit`

Note: If your Fortify Software Security Center instance appears to be stuck in maintenance mode, try one of the possible solutions described in "If Fortify Software Security Center is Stuck in Maintenance Mode" below.

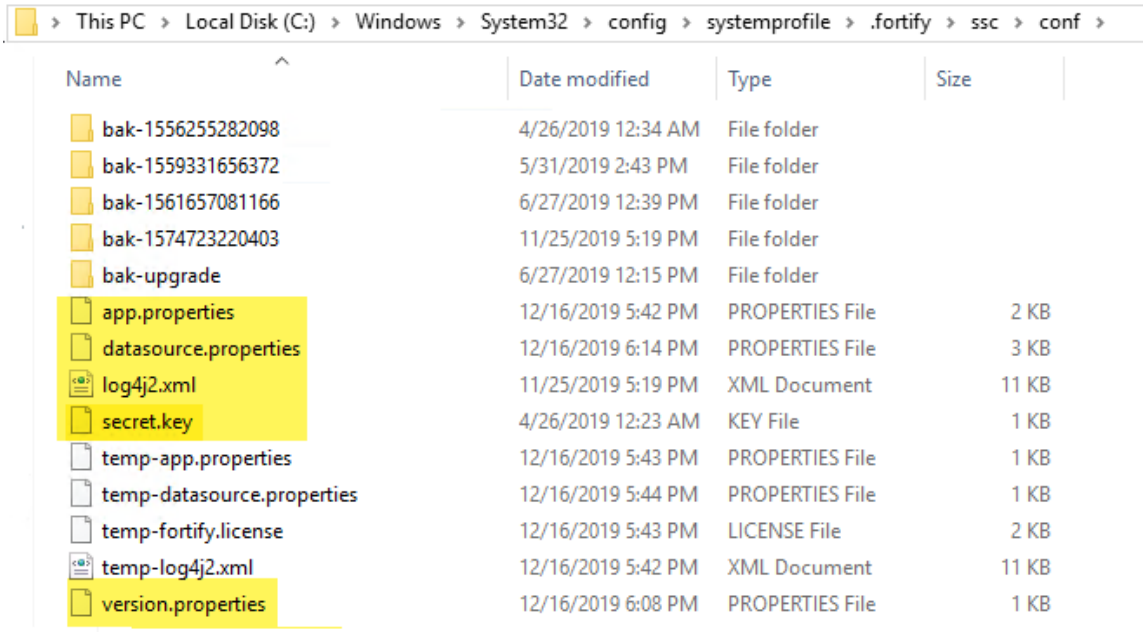
To facilitate server maintenance, you can pause job execution, which allows running jobs to finish but prevents new jobs from executing. For details, see "Pausing and Resuming Job Execution" on the next page.

If Fortify Software Security Center is Stuck in Maintenance Mode

Fortify Software Security Center goes into maintenance mode when it is placed there from the ADMINISTRATION view (see "Placing Fortify Software Security Center in Maintenance Mode" on page 185), or it cannot locate the `version.properties` in the `fortify.home\ssc\conf` directory.

If your Fortify Software Security Center instance is stuck in maintenance mode, try one of the following:

- Reconfigure Fortify Software Security Center. For instructions, see "Configuring Fortify Software Security Center for the First Time" on page 72.
- Navigate to the `fortify.home\ssc\conf` directory and, in the `version.properties` file, set `maintenance.mode` to `false`.
- Restore the missing files from the `fortify.home\ssc\conf` directory.



Note: The `datasource.properties` file and some database fields contain encrypted entries that rely on the `secret.key` file. So, if you are moving your Fortify Software Security Center instance from one computer to another, you must also move the `secret.key` file (not just your database files).

Pausing and Resuming Job Execution

If, for any reason, you need to shut down the server, you can temporarily pause user activity and disable the running of new jobs for all users in the system, while allowing Fortify Software Security Center to just finish jobs in progress. This helps to ensure that no data are corrupted or lost when the server is shut down.

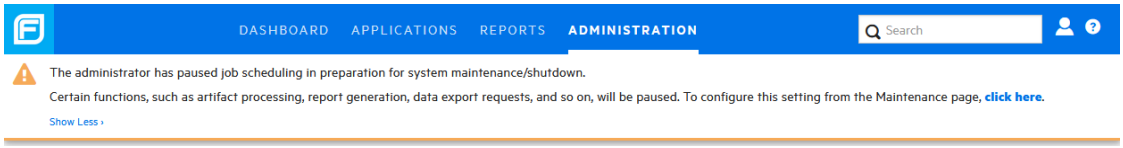
To pause job execution on the server:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Configuration**, and then select **Maintenance**.
3. On the Maintenance page, select the **Pause job execution** check box, and then click **SAVE**.

   Immediately after you save the setting:

   Important! To prevent the queuing up of a large number of jobs, Fortify recommends that you avoid leaving this setting enabled for long periods of time. After you pause job execution, make sure that you allow time for queued jobs to process completely before you shut down the server.

   - All jobs in progress are allowed to complete.
   - All new jobs that users subsequently submit are queued for running later, after the **Pause jobs execution** check box is cleared.
   - Fortify Software Security Center displays a banner to notify users that job execution has been paused.



4. After you next start the server, return to the Maintenance page, clear the **Pause job execution** check box, and then click **SAVE**.

See Also

"Placing Fortify Software Security Center in Maintenance Mode" on page 185

About Fortify Software Security Content

Fortify products use a knowledge base of rules to enforce secure coding standards applicable to the codebase for analysis. Fortify software security content consists of Fortify Secure Coding Rulepacks (Rulepacks) and external metadata:

- Rulepacks describe general secure coding idioms for popular languages and public APIs.

  You can write custom rules that add to the functionality of Fortify analyzers and Rulepacks. For example, you might need to enforce proprietary security guidelines or analyze an application that uses third-party libraries or other pre-compiled binaries that are not already covered by the Secure Coding Rulepacks. For instructions on how to write custom rules, see the *Fortify Static Code Analyzer Custom Rules Guide* (available only with the Fortify Static Code Analyzer product download).

  For information on how to manage Rulepacks, see:

  - "Updating Rulepacks from theFortify Update Server" on the next page
  - "Importing Security Content" on page 191
  - "Deleting Rulepacks" on page 191
  - "Exporting Rulepacks" on the next page
  - "Seeding the Database with Report Seed Bundles Delivered with Quarterly Security Content Releases" on page 204
- External metadata provides mappings from the Fortify vulnerability categories to alternative categories (such as CWE, OWASP Top 10, and PCI).

  Fortify recommends that you *not* modify the external `metadata.xml` file. If you do, your changes are overwritten whenever your Rulepacks are updated quarterly. (See "Seeding the Database with Report Seed Bundles Delivered with Quarterly Security Content Releases" on page 204.) You can, however, create a `customexternalmetadata.xml` file in which you can create new, and extend existing, mappings. You can map Fortify issues to different taxonomies, such as internal application security standards or additional compliance obligations. This custom file is left undisturbed when you update your security content. For instructions on how to create your own custom rules or custom external metadata, see the *Fortify Static Code Analyzer Custom Rules Guide*.

  The schema for external metadata mappings is located in `fortify.home\Core\config\schemas\externalmetadata.xsd`.

  For information on how to manage your external metadata, see:

  - "Extending a Current Mapping" on page 192
  - "Creating a New Mapping" on page 193

Note: It is important that you work with the newest Rulepacks available. Fortify recommends that you periodically update your security content.

Updating Rulepacks from theFortify Update Server

It is important that you work with the newest Rulepacks available. If you want to make sure that you have the latest Rulepack, you can import it from the Fortify server.

Note: You can use the Fortify Software Security Center proxy to update Rulepacks, if the Fortify update server is behind it. For information about how to set up a consolidated proxy for Fortify Software Security Center, see "Configuring a Proxy for Fortify Software Security Center Integrations" on page 132.

To import the latest Rulepacks:

1. Log in to Fortify Software Security Center as an administrator or security lead, and then, on the Fortify header, select **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, under **Metrics & Tracking**, select **Rulepacks**.
3. On the Rulepacks page, click **UPDATE FROM SERVER**.

   Fortify Software Security Center displays information about what the Rulepack update involves, and prompts you to indicate whether you want to continue.
4. To continue with the download, click **OK**.

   After the update is complete, Fortify Software Security Center displays a list of any imported rules.
5. Click **CLOSE**.

See Also

"Deleting Rulepacks" on the next page

"Seeding the Database with Report Seed Bundles Delivered with Quarterly Security Content Releases" on page 204

"Exporting Rulepacks" below

"Importing Security Content" on the next page

Exporting Rulepacks

You can, if necessary, move Rulepacks between one Fortify Software Security Center instance and another instance, or between Fortify Software Security Center and Fortify Audit Workbench.

Export Rulepacks with the same file names used to import them, including the file extension (`.bin` or `.xml`).

To export a Rulepack:

1. Log in to Fortify Software Security Center as an administrator or security lead.
   On the Fortify header, click **ADMINISTRATION**.
2. In the left pane, under **Metrics & Tracking**, select **Rulepacks**.
3. On the Rulepacks page, select the check boxes for the Rulepacks you want to export, and then click **EXPORT**.

Note: If a Rulepack that you select has multiple versions, only the latest version is exported.

See Also

"Importing Security Content" below

"Deleting Rulepacks" below

Importing Security Content

You can import security content, including custom Rulepacks created using the Fortify Custom Rules Editor, extended mapping files, and custom mapping files so that they are available to Fortify Static Code Analyzer and Fortify Audit Workbench.

To import security content:

1. Log in to Fortify Software Security Center as an administrator or security lead.
   On the Fortify header, click **ADMINISTRATION**.
2. In the left pane, under **Metrics & Tracking**, select **Rulepacks**.
3. On the Rulepacks page, select **IMPORT**.
4. In the IMPORT RULEPACK dialog box, click **+ ADD FILES**.
5. In the File Upload dialog box, navigate to and select the file(s) to upload.

Note: If you upload an FPR file to that contains an extended mapping, and that mapping is not present on the server, Fortify Software Security Center displays a processing warning.

See Also

"Exporting Rulepacks" on the previous page

"Deleting Rulepacks" below

Deleting Rulepacks

You can remove old Rulepacks from Fortify Software Security Center.

To delete Rulepacks:

1. Log in to Fortify Software Security Center as an administrator or security lead.
   On the Fortify header, click **ADMINISTRATION**.
2. In the left pane, under **Metrics & Tracking**, select **Rulepacks**.
3. On the Rulepacks page, select the check boxes for the Rulepacks to delete, and then click **DELETE**.
   Fortify Software Security Center prompts you to verify that you want to delete the selected Rulepack(s) and, if the system contains multiple versions of the Rulepack, all of the versions it includes are deleted.
4. Click **OK**.
   Fortify Software Security Center displays a message to indicate whether the deletion was successful.
5. If the deletion fails, click **more** to open the DETAILS window and find out what caused the failure.

See Also

"Exporting Rulepacks" on page 190

"Importing Security Content" on the previous page

"Updating Rulepacks from theFortify Update Server" on page 190

Extending a Current Mapping

You can extend the mappings that Fortify Software Security Center delivers with the external metadata, or create new mappings. If you do, keep the following in mind:

- You can only add new mappings.
- You cannot overwrite existing mappings.

To extend the current mapping, use the following format:

```
<ExternalListExtension>
        <ExternalListID>
        F2FA57EA-5AAA-4DDE-90A5-480BE65CE7E7
        </ExternalListID>
        <ExternalCategoryDefinition>
                <Name>APP100 CAT I</Name>
                <Description>
                Description for APP100 CAT I.
                </Description>
                <OrderingInfo>1</OrderingInfo>
        </ExternalCategoryDefinition>
        <Mapping>
                <InternalCategory>
                Poor Style: Identifier Contains Dollar Symbol ($)
                </InternalCategory>
                <ExternalCategory>APP100 CAT I</ExternalCategory>
        </Mapping>
</ExternalListExtension>
```

Important! After you extend your mapping file, you must upload it to Fortify Software Security Center. For instructions, see "Importing Security Content" on page 191.

If you upload an FPR file that contains an extended mapping, and that mapping is not present on the server, Fortify Software Security Center displays a processing warning.

See Also

"Creating a New Mapping" below

"About Fortify Software Security Content" on page 189

Creating a New Mapping

You can use `<ExternalList>` to create a `custom_metadata.xml` file, as follows:

```
<ExternalList>
        <OrderingInfo>1</OrderingInfo>
        <ExternalListID>
        F2FA57EA-5BBB-4DDE-90A5-480BE65CE7E7
        </ExternalListID>
        <Name>My Custom Mapping</Name>
        <Shortcut>MCM</Shortcut>
        <Description>My Custom Mapping description</Description>
        <Group>MCM</Group>
        <ExternalCategoryDefinition>
                <Name>Custom Mapping CAT 1</Name>
                <Description>
                Description for Custom Mapping CAT 1
                </Description>
                <OrderingInfo>1</OrderingInfo>
        </ExternalCategoryDefinition>
        <Mapping>
                <InternalCategory>SQL Injection</InternalCategory>
                <ExternalCategory>Custom Mapping CAT 1
        </ExternalCategory>
        </Mapping>
</ExternalList>
```

Important! After you create your custom mapping file, you must upload it to Fortify Software Security Center. For instructions, see "Importing Security Content" on page 191.

If you upload an FPR file that contains a custom mapping, and that mapping is not present on the server, Fortify Software Security Center displays a processing warning.

See Also

"Extending a Current Mapping" on page 192

"About Fortify Software Security Content" on page 189

Chapter 8: Upgrading Fortify Software Security Center

To perform a direct upgrade to the latest Fortify Software Security Center version, you must have one of the last three versions installed. For example, to upgrade to version 23.1.0, you must have version 21.2.x, 22.1.x or 22.2.x installed. If you have version 21.1.x or earlier installed, you must first upgrade to version 21.2.x, 22.1.x or 22.2.x before you can migrate to version 23.1.0.

The following table shows the upgrade path required to upgrade to Fortify Software Security Center 23.1.0.

Upgrade Paths for Fortify Software Security Center Versions
21.1.x > 22.2.x > 23.1.0
21.2.x > 23.1.0 (direct)
22.1.x > 23.1.0 (direct)
22.2.x > 23.1.0 (direct)

If you cannot directly upgrade your current Fortify Software Security Center version to the latest version, see the version-specific Fortify Software Security Center documentation for instructions on how to upgrade to the previous release (or the release immediately before that).

Important! Full ScanCentral SAST-related functionality in Fortify Software Security Center requires updated ScanCentral Controller and sensors. If you do not need sensor metrics, you can use existing sensors. You can use existing ScanCentral clients without limiting functionality.

You must upgrade the ScanCentral Controller before you upgrade the ScanCentral sensors and clients, *and* before you upgrade the Fortify Software Security Center server. For information about how to upgrade ScanCentral Components, see the *Micro Focus Fortify ScanCentral Installation, Configuration, and Usage Guide*.

Fortify Software Security Center Database Upgrade Tasks

Upgrade the Fortify Software Security Center database by performing the tasks described in the following table in the order listed.

Task	Description
1	Stop Tomcat Server.
2	Delete the SSC folder and the SSC WAR file from the `<tomcat>/webapps` directory.
4	Copy the new WAR file to the `<tomcat>/webapps` directory.
5	Start Tomcat Server.
6	Open a browser and enter your Fortify Software Security Center URL to start Fortify Software Security Center in initialization mode. (See "Configuring Fortify Software Security Center After an Upgrade" on page 198.)
7	Use the Setup wizard to generate the migration SQL script. (See "Configuring Fortify Software Security Center After an Upgrade" on page 198.)
8	Run the migration script on your database. (See "Preparing to Run the Database Upgrade Script" on the next page.) **Note:** Databases that contain over 1 TB of data might take five or more hours to migrate. **Important!** (Microsoft SQL databases only) After you migrate Fortify Software Security Center to a new SQL database version and back up and restore the database, make sure that you change the compatibility level (from SQL Server Management Studio) to reflect the SQL engine that currently hosts the Fortify Software Security Center database.
9	Use the Setup wizard to reseed the database.
10	Restart Tomcat Server.
11	Bug tracker plugins are not included in the `ssc.war` file. After you

Task	Description
	upgrade and start Fortify Software Security Center, be sure to disable and remove old bug tracker plugins, and then install new plugins from the current distribution file. For more information, see "About Bug Tracker Integration" on page 169.

Preparing to Upgrade the Fortify Software Security Center Database

The Fortify Software Security Center database migration process creates larger transactions than those created during regular use. For Fortify Software Security Center databases that have been successfully run in production environments, database migration does not typically require changes to your database configuration or resources. For large databases, Fortify recommends that you review and, if necessary, increase the database resources and settings required to accommodate the migration process.

If you are upgrading a MySQL database, see "Setting the Innodb Buffer Pool Size when Upgrading a MySQL Server Database" below.

Setting the Innodb Buffer Pool Size when Upgrading a MySQL Server Database

If you are upgrading a MySQL database, Fortify recommends that you set the `innodb_buffer_pool_size` variable to at least 2.5 GB. After the upgrade, revert to your previous setting.

For information about how to configure MySQL for use with Fortify Software Security Center, see "Configuring a MySQL Database" on page 65.

Preparing to Run the Database Upgrade Script

The Fortify Software Security Center database upgrade scripts require the same database privileges that the database creation scripts require.

Before you run the database upgrade script, perform the following tasks:

- Back up your existing Fortify Software Security Center database using your database client tool.
- Acquire the database account information that was used to create the existing Fortify Software Security Center database. See "Database User Account Privileges" on page 63.

Note: Databases that contain over 1 TB of data might take five or more hours to migrate.

Updating and Deploying the WAR File

To update the SSC WAR file:

1. Undeploy the currently deployed SSC WAR file. For instructions, see the documentation for Tomcat Server.
2. Deploy the new SSC WAR file.

After you deploy the new WAR file, complete the configuration tasks on the Setup wizard steps and in the ADMINISTRATION view. For information and instructions, see "Configuring Fortify Software Security Center After an Upgrade" below and "Additional Fortify Software Security Center Configuration" on page 82.

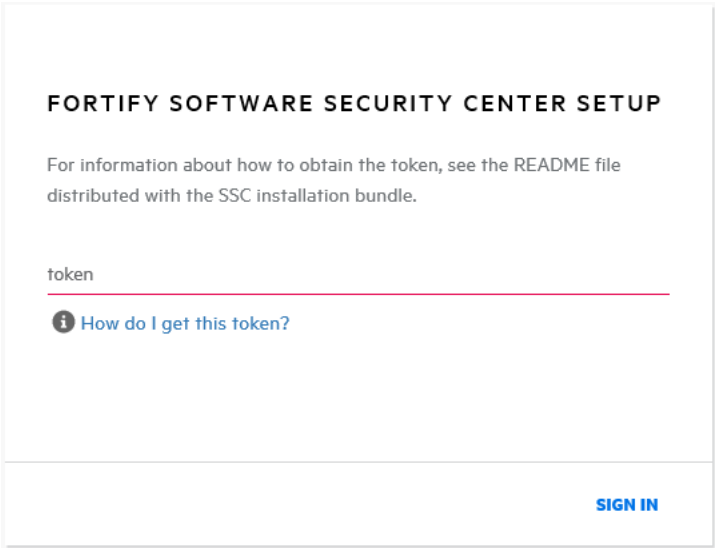
Configuring Fortify Software Security Center After an Upgrade

After you upgrade Fortify Software Security Center and go to your Fortify Software Security Center URL in a browser window, the Setup wizard opens.

Note: The Setup wizard is available to administrators only, and only after the first deployment of Fortify Software Security Center, after an upgrade, or after the server is placed in maintenance mode (see "Placing Fortify Software Security Center in Maintenance Mode" on page 185).

1. After you deploy a new version of the Fortify Software Security Center WAR file in Tomcat Server, open a browser window and type your Fortify Software Security Center server URL.

2. Go to the `<fortify.home>/<app_context>` directory, and open the `init.token` file.
3. Copy the contents of the `init.token` file to the clipboard.
4. In the upper right corner of the Fortify Software Security Center screen, click **ADMINISTRATORS**.



5. Paste the string you copied from the `init.token` file into the text box, and then click **SIGN IN**.
6. If you need to change any configuration settings on the **CONFIGURATION** or **CORE SETTINGS** steps of the Fortify Software Security Center Setup wizard, you can do so using the instructions provided in "Configuring Fortify Software Security Center for the First Time" on page 72.
7. Click **NEXT** until you reach the **DATABASE SETUP** step.

8. On the **DATABASE SETUP** step, do the following:
   a. In the **DATABASE TYPE** box, select the type that matches the Fortify Software Security Center database type.
   b. In the **DATABASE USERNAME** box, type the username for your Fortify Software Security Center database. For more information, see "Database User Account Privileges" on page 63.
   c. In the **DATABASE PASSWORD** box, type the password for your Fortify Software Security Center database.
   d. In the **JDBC URL** box, type the URL for the Fortify Software Security Center database.

      Caution! The database name (including letter case) in the JDBC URL must exactly match your Fortify Software Security Center database name.

      Note: The MariaDB JDBC driver is used to connect to the MySQL database server. Any JDBC URL parameters *must* use MariaDB driver syntax.
      Example of the correct collation parameter syntax:
      `jdbc:mysql://<host>:3306/<database_name>?sessionVariables=collation_connection=<collation_name>`
      (Replace the parameter `connectionCollation=<collation_name>` with `sessionVariables=collation_connection=<collation_name>`.)

   e. To test the connection to your database, click **TEST CONNECTION**.
      If the connection test fails, check the `ssc.log` file (`<fortify.home>/<appcontext>/logs` directory) to determine the cause.
   f. After the Setup wizard indicates that the connection was successful, in the right pane, read the warning and Instructions, and then click **DOWNLOAD SCRIPT**.
   g. Save and run the `ssc-migration.sql` script. (For instructions, see "About the Fortify Software Security Center Database Tables and Schema" on page 69.)

      Note: Depending on the size of the source database, data migration may take several hours to complete.

9. After you run the `ssc-migration.sql` script, click **NEXT**.
10. On the **DATABASE SEEDING** step, do the following:
    a. In the left pane, use **BROWSE** to locate and select your process seed bundle zip file, and then click **SEED DATABASE**.
    b. Use **BROWSE** to locate and select your report seed bundle zip file, and then click **SEED DATABASE**.

c. (Optional) Use **BROWSE** to locate and select your PCI basic seed bundle zip file, and then click **SEED DATABASE**.

11. Click **NEXT**.
12. Click **FINISH**.
13. Restart Tomcat Server.

Tip: If you later find that you need to change any of the configuration settings, you can place Fortify Software Security Center in maintenance mode, and then make any necessary changes. For instructions on how to place Fortify Software Security Center in maintenance mode, see "Placing Fortify Software Security Center in Maintenance Mode" on page 185.

See Also
"Configuring Fortify Software Security Center for the First Time" on page 72

Upgrading Fortify Static Code Analyzer from Fortify Audit Workbench

A Fortify Audit Workbench user can check on the availability of new Fortify Static Code Analyzer and and Fortify Apps and Tools versions from the Fortify Audit Workbench user interface. If a version newer than the one installed is available, the user can download it and upgrade the local instance. A Fortify Audit Workbench user can also configure Fortify Audit Workbench to check for, download, and install new versions automatically at startup.

To enable this functionality for Fortify Audit Workbench users, a Fortify Software Security Center administrator must first set up the auto upgrade capability on the Fortify Software Security Center host machine.

For information about how to upgrade Fortify Static Code Analyzer and its associated tools from Fortify Audit Workbench, see the *Micro Focus Fortify Audit Workbench User Guide*.

See Also

"Enabling Fortify Static Code Analyzer and Fortify Apps and Tools Upgrades from Audit Workbench" below

Enabling Fortify Static Code Analyzer and Fortify Apps and Tools Upgrades from Audit Workbench

To make new Fortify Static Code Analyzer and Fortify Apps and Tools installers available to Audit Workbench users for upgrades:

1. On the Fortify Software Security Center host, navigate to `<ssc_install_dir>/WEB-INF/internal`, and then open the `securityContext.xml` file in a text editor.

2. Locate and uncomment the following line:

```
<!-- <security:intercept-url pattern="/update-site/**"
    access="PERM_ANONYMOUS"/> -->
```

3. Save and close the `securityContext.xml` file.
4. Copy the Fortify_SCA or Fortify_Apps_and_Tools installer files to the *<ssc_install_dir>*`/webapps/ssc/update-site/installers` directory.
5. In the *<ssc_install_dir>*`/webapps/ssc/update-site/installers` directory, create an `update.xml file` for the product that you want to update, as follows:
   a. To enable Fortify Static Code Analyzer updates, use the following XML code:

```
<installerInformation>
  <versionId>####</versionId>
  <version>##.##</version>
  <platformFileList>
    <platformFile>
       <filename>Fortify_SCA_<version>_windows_x64.exe</filename>
       <platform>windows-x64</platform>
    </platformFile>
    <platformFile>
       <filename>Fortify_SCA_<version>_linux_x64.run</filename>
       <platform>linux-x64</platform>
    </platformFile>
    <platformFile>
       <filename>Fortify_SCA_<version>_osx_x64.app.zip</filename>
       <platform>osx</platform>
     </platformFile>
  </platformFileList>
  <downloadLocationList>
    <downloadLocation>
       <url>http://localhost:8080/update-site/installers/</url>
    </downloadLocation>
  </downloadLocationList>
</installerInformation>
```

   b. To enable Fortify Applications and Tools updates, create the `update.xml` file using the following XML code:

```
<installerInformation>
  <versionId>####</versionId>
  <version>##.##</version>
  <platformFileList>
    <platformFile>
       <filename>Fortify_Apps_Tools_<version>_windows_x64.exe</filename>
       <platform>windows-x64</platform>
    </platformFile>
    <platformFile>
```

```
      <filename>Fortify_Apps_Tools_<version>_linux_x64.run</filename>
      <platform>linux-x64</platform>
    </platformFile>
    <platformFile>
      <filename>Fortify_Apps_Tools_<version>_osx_x64.app.zip</filename>
      <platform>osx</platform>
     </platformFile>
  </platformFileList>
  <downloadLocationList>
    <downloadLocation>
      <url>http://localhost:8080/update-site/installers/</url>
    </downloadLocation>
  </downloadLocationList>
</installerInformation>
```

6. Restart Tomcat Server.

Audit Workbench users can now check for and install new Fortify Static Code Analyzer and Fortify Applications and Tools versions.

Note: The BitRock InstallBuilder tool used for the auto upgrade functionality supports only one Windows tag. If you have different versions of Windows, you must have corresponding configuration files for those versions. For information about how to create the additional configuration files, see the `readme.txt` file located in the `<ssc_install_dir>/update-site/installers` directory.

Updating Expired Licenses

For information about how to obtain a Fortify license file, see the *Micro Focus Fortify Software System Requirements* document.

To update an annual license that has expired:

1. Stop Tomcat Server.
2. Place your downloaded `fortify.license` file in the <*fortify.home*> directory.
3. Restart Tomcat Server.

Quarterly Security Content Releases

Micro Focus Fortify notifies you when new security content is available for download. These updates include Rulepacks and external metadata, and can also contain updated seed bundles.

Important! Updated external metadata files can include changes to mapping that reporting depend on. If updated security content includes a new report seed bundle, make sure that you update your rules and mapping *before you run reports*.

See Also

"About Seeding the Fortify Software Security Center Database" on page 70

"About Fortify Software Security Content" on page 189

"Updating Rulepacks from theFortify Update Server" on page 190

Seeding the Database with Report Seed Bundles Delivered with Quarterly Security Content Releases

Micro Focus Fortify notifies you when new security content is available for download. To determine whether this updated content includes a new seed bundle, check under the heading **Micro Focus Security Fortify Premium Content** in your notification document. That section will have information about the existence of a new seed bundle. If a new seed bundle is included, you can use it to re-seed your database. For more information about seed bundles and seeding the database, see "About Seeding the Fortify Software Security Center Database" on page 70.

> **Note:** Seeding the database blocks the creation of new application versions, and the execution of report jobs and FPR processing jobs.

To seed the database with the report seed bundle from a quarterly security content release:

1. Download the updated security content, as follows:
   a. Log on to the Fortify Support Portal (https://www.microfocus.com/support).
   b. In the left column, select **PREMIUM CONTENT**.
   c. On the right, select **FORTIFY EXCHANGE**.
   d. Select and download the latest report seed bundle.
2. Extract the contents of the seed bundle ZIP file.
3. In the left pane, select **Configuration**, and then select **Seed Bundles**.
4. On the **Seed Bundles** page, click **BROWSE**, and then navigate to and select the `ReportBundle.zip` file.
5. Click **SEED BUNDLES**.

Fortify Software Security Center displays a message to let you know the bundle upload was successful.

See Also

"About Seeding the Fortify Software Security Center Database" on page 70

Part I: Using Micro Focus Fortify Software Security Center

The following chapters provide information about how to use Fortify Software Security Center.

Chapter 9: Using Fortify Software Security Center

Fortify Software Security Center is a browser-based product that provides a set of capabilities across the software development life cycle to automate detection of security vulnerabilities in applications. It helps your security and development teams work together to resolve security flaws quickly and accurately by making correlated data from Fortify Static Code Analyzer, Fortify ScanCentral DAST, Fortify ScanCentral SAST, Fortify WebInspect, and third-party tools available through its collaborative online environment.

Topics covered in this section:

About the Central Role of Fortify Software Security Center

Fortify Software Security Center provides a location for collecting, correlating, auditing, and exporting security analysis results. The Fortify Software Security Center server resides in a central location and receives results from different security activities, such as static, dynamic, and real-time analysis.

Fortify Software Security Center is designed to help you:

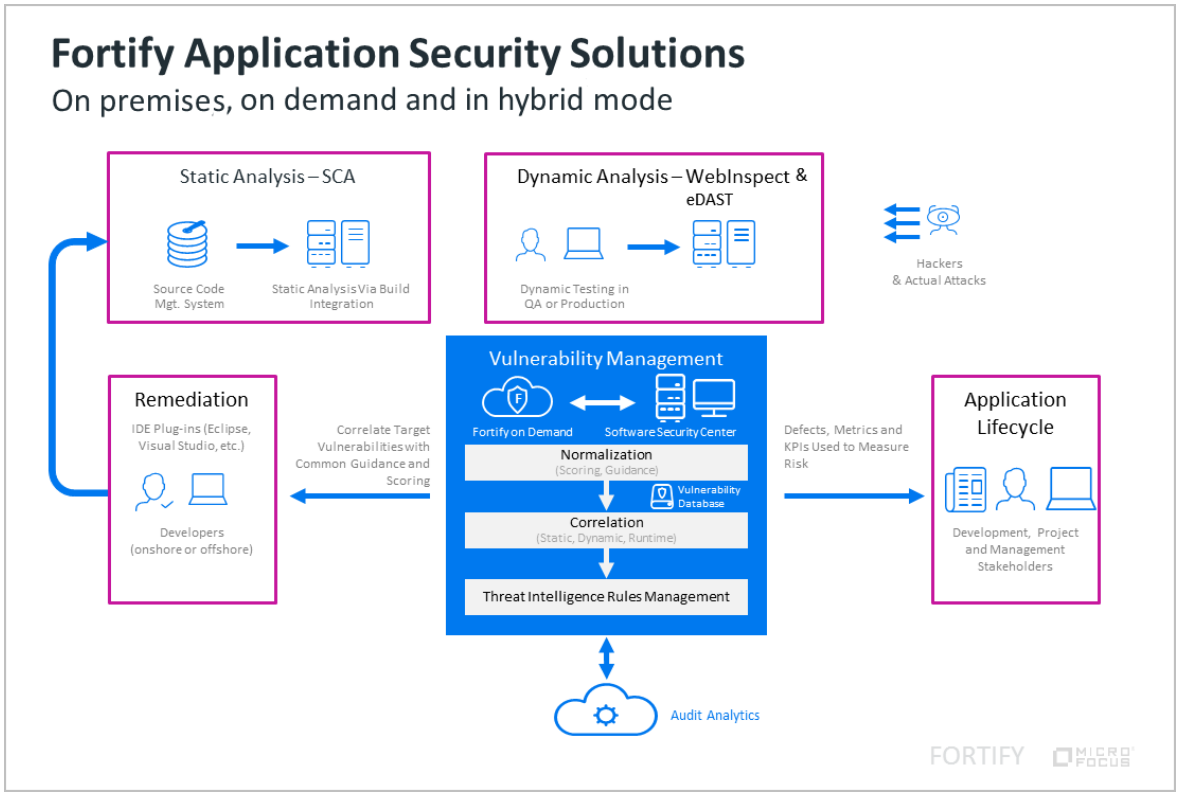
- Identify and prioritize a baseline of existing vulnerabilities
- Prevent new vulnerabilities from being introduced
- Remediate existing vulnerabilities and lower the baseline
- Ensure that your code is in compliance with internal and external security mandates

Fortify Software Security Center works within your organization to answer the following questions:

- How do we drive the adoption of good application security practices?
- How do we get actionable results to development teams?
- Do we measure application teams on a team-by-team basis or as a unit?
- How do we track results over time?

Security Management Workflow

The following figure illustrates the flow of security management processes within Fortify Software Security Center.



As development teams perform scans, they submit periodic scan results from a continuous integration server into Fortify Software Security Center.

Security teams submit periodic results of a dynamic assessment into Fortify Software Security Center.

Fortify Software Security Center correlates and tracks the scan results and assessment results over time, and makes the information available to developers through Audit Workbench, or through IDE plugins such as the Fortify Plugin for Eclipse, the Fortify Extension for Visual Studio, and others.

Users can also push issues into defect tracking systems, including ALM, Jira, Azure DevOps Server, and Bugzilla.

User Accounts and Access

Fortify Software Security Center supports two methods of authentication:

- Local user accounts created within the interface
- Active Directory/LDAP accounts associated with standard corporate authentication (Active Directory/LDAP integration supports user assignment by group or organizational unit)

Topics covered in this section:

Active Directory/LDAP Integration

Active Directory/LDAP integration enables Fortify Software Security Center to authorize users based on their existing corporate credentials. In addition, assignment by group or organizational unit enables Fortify Software Security Center to take advantage of the existing joiners/leavers processes. A new person who joins a group automatically has access to Fortify Software Security Center. A person who leaves a group automatically loses access.

The user who deploys Fortify Software Security Center must configure the integration with the Active Directory/LDAP during installation. For detailed information, see "Configuring LDAP Servers" on page 111.

See Also

"Registering LDAP Entities" on page 123

"Fortify Software Security Center User Account Management" on page 221

Logging in to Fortify Software Security Center for the First Time

To log in to Fortify Software Security Center, your Fortify Software Security Center administrator must provide you with the URL for your instance, a username, and a password.

To log in to Fortify Software Security Center for the first time:

1. To make sure that you access the newest version of the Fortify Software Security Center user interface, clear your web browser's cache.
2. In a web browser, type the URL for your Fortify Software Security Center instance, as follows:
   - If Fortify Software Security Center is configured to use secure HTTP protocol, type the following URL:

     `https://<host_ip>:<port>/ssc/`

     where `<port>` represents the port number that Tomcat Server uses.
   - If Fortify Software Security Center is configured to use insecure HTTP protocol (not recommended), type the following URL:

     `http://<host_ip>:<port>/ssc/`

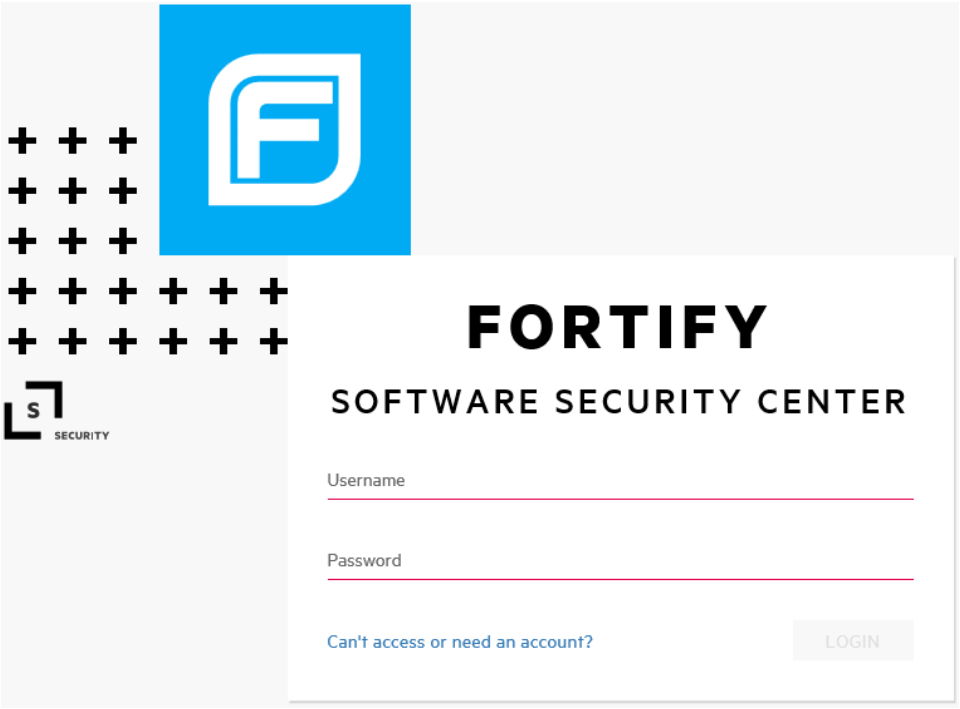
     where `<port>` represents the port number that Tomcat Server uses.
3. In the **Username** and **Password** boxes, type the credentials that your administrator has given you.
4. Click **LOGIN**.
5. If Fortify Software Security Center prompts you to change your password, do so. For instructions, see "Changing Your Password" on page 211.

Requesting Access to Fortify Software Security Center

If you do not yet have a Fortify Software Security Center user account, or if you have forgotten your user name or password, you can request assistance from the login page.

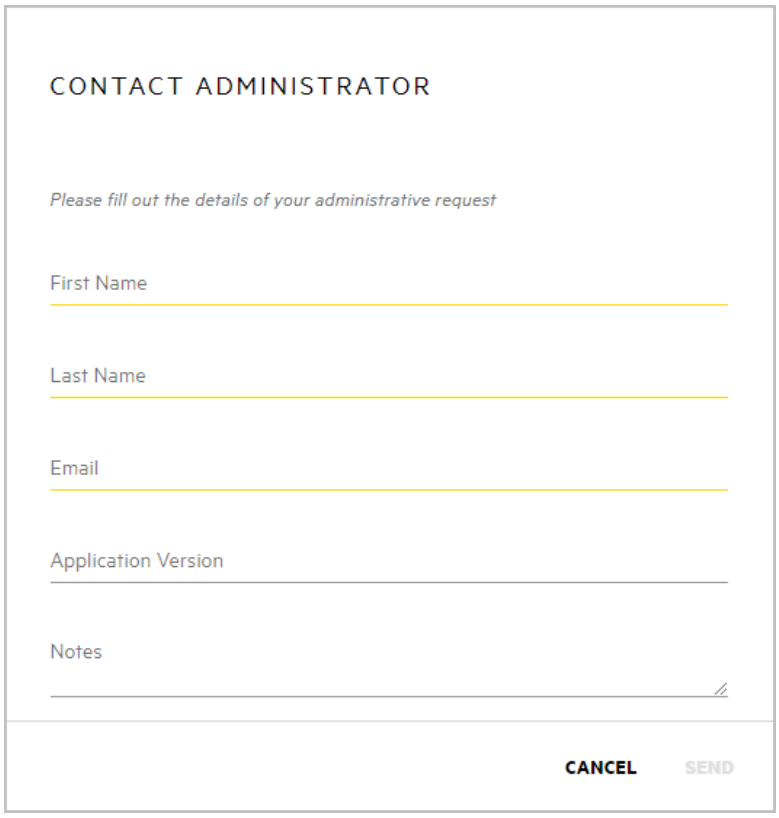
To request access to Fortify Software Security Center:

1. In a web browser, type the URL for your Fortify Software Security Center instance.



2. At the bottom of the Fortify Software Security Center screen, click the **Can't access or need an account?** link.

Note: This link is available only if your Fortify Software Security Center administrator has enabled email notification. (See "Configuring Email Alert Notification Settings" on page 102.)



3. Provide the required information, and then click **SEND**.

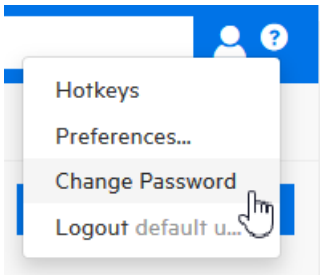
Fortify Software Security Center sends your request to the Fortify Software Security Center administrator.

Changing Your Password

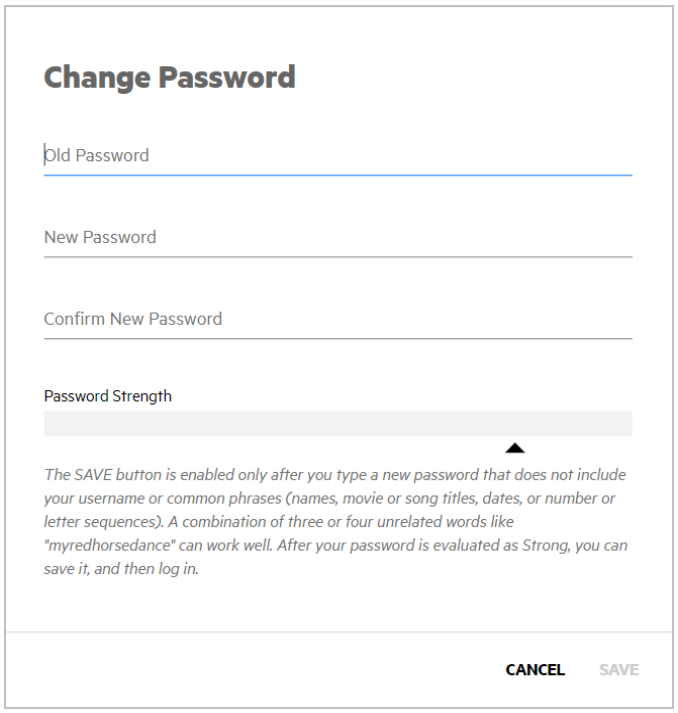
The following procedure describes how to change your password. Note that you can only change your password if you are logged on using a local account.

To change your password:

1. Log in to Fortify Software Security Center.



2. At the right end of the Fortify header, click the user profile icon, and then select **Change Password**.



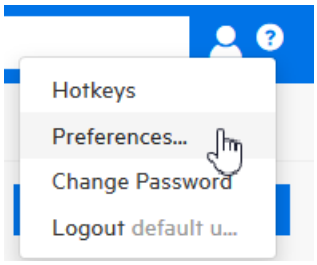
The **SAVE** button in the Change Password dialog box is enabled only after you type a strong new password that does not include your username or common phrases (names, movie or song titles, dates, or number or letter sequences). A combination of three or four unrelated words like "myredhorsedance" can work well. After your password is evaluated as strong, you can save it, and then log in.

3. Provide your old password, type a new one, and then confirm the new one.
4. If the password strength is acceptable, click **SAVE**.

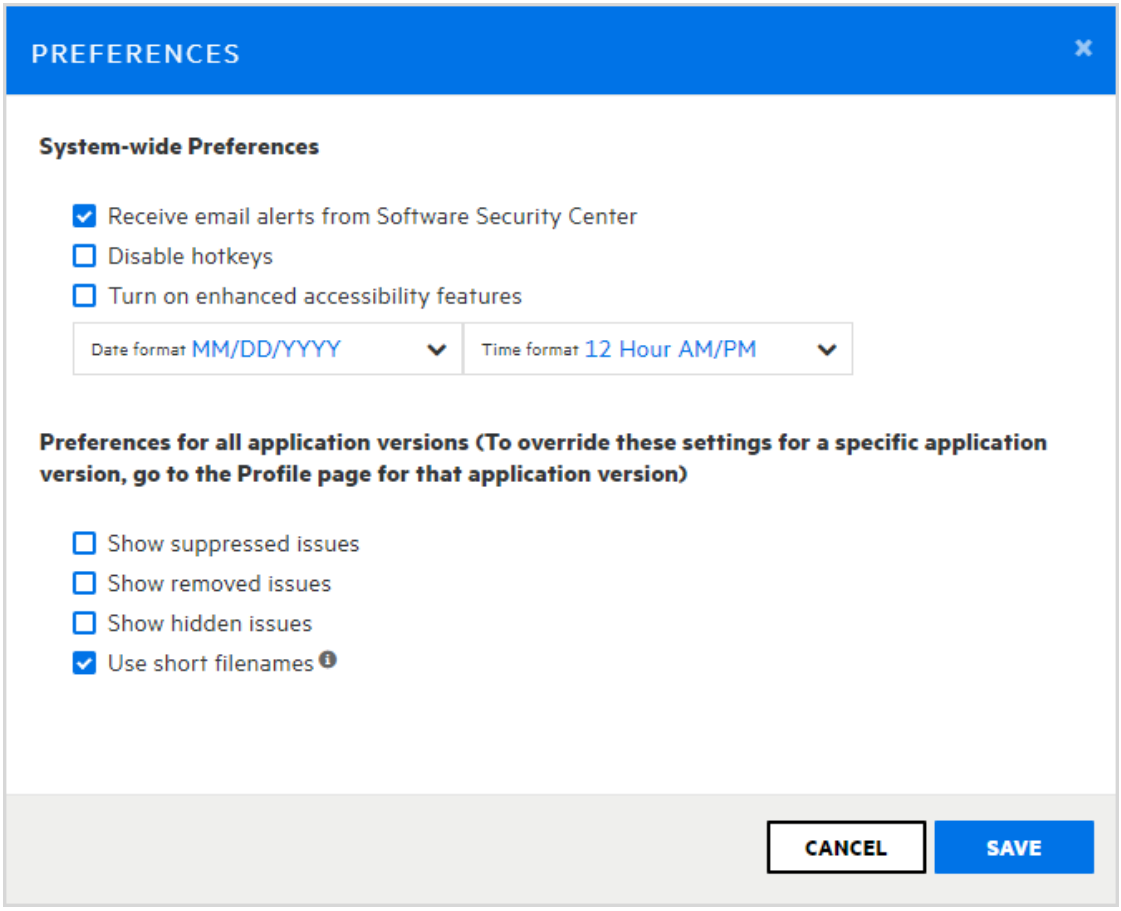
Setting Preferences: System-Wide and Across Application Versions

You can configure preferences for behavior system-wide, and across application versions.

To set system-wide preferences:



1. On the right side of the Fortify header, click the user profile icon, and then select **Preferences**.



2. To set preferences to apply to the entire system, in the PREFERENCES dialog box, under **System-wide Preferences**, do the following:
   a. Select the check boxes for the features you want to enable or disable.
   b. To apply the YYYY/MMDD date format instead of the default MM/DD/YYYY format, select it from the **Date format** list.
   c. To apply the 24 Hour time format instead of the default 12 hour AM/PM format, select it from the **Time format** list.
3. To set preferences for all application versions, do the following:

   Note: To override these settings for a specific application version, go to the APPLICATION PROFILE dialog box for that application version.

   a. To include suppressed issues in the issues list on the AUDIT page, select the **Show suppressed issues** check box.
   b. To include removed issues on the AUDIT page, select the **Show removed issues** check box.
   c. To include hidden issues on the AUDIT page, select the **Show hidden issues** check box.

d. To display short file names in the issues list on the AUDIT page, select the **Use short file names** check box.

4. Click **SAVE**.

About the Fortify Software Security Center Dashboard

After you log in to Fortify Software Security Center, the dashboard displays data for the application versions to which you have access and that pose the highest potential business risk to your organization.

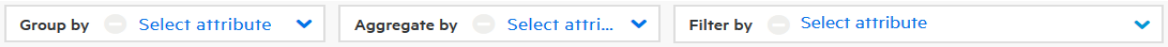
Topics covered in this section:

Issue Stats Page

When you first log in to Fortify Software Security Center, the first thing you see is the ISSUE STATS page of the Dashboard. This page shows summary information about issues for the application versions that you can access, including the number of days that it is taking to review and fix them. To provide a visual cue as to how quickly issues are being handled, the ISSUE STATS page displays colored bars next to the values for the **Average Days to Review** and **Average Days to Remediate**. A green bar indicates that issues are being managed quickly, a red bar indicates that issue management is too slow, and an orange bar indicates that issue management is somewhere between these two extremes.

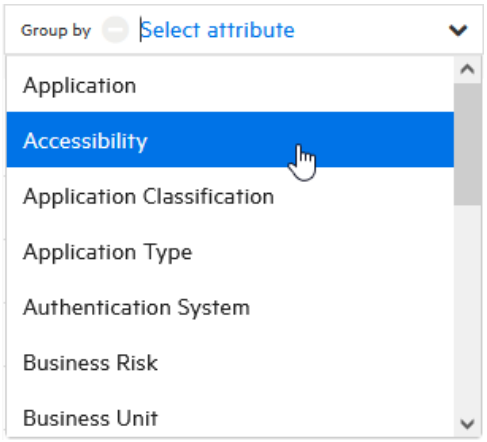
Note: If you are an administrator or security lead, you can set the thresholds that determine what users see when they review information on the Issue Stats page. For details, see "Configuring Issue Stats Thresholds" on page 83.

If you click an application version listed in the table, Fortify Software Security Center takes you directly to the AUDIT page for that application version. No filters are applied to the data.



The Dashboard provides three settings that you can use alone or in combination to refine the summary data displayed.

Selecting a grouping attribute

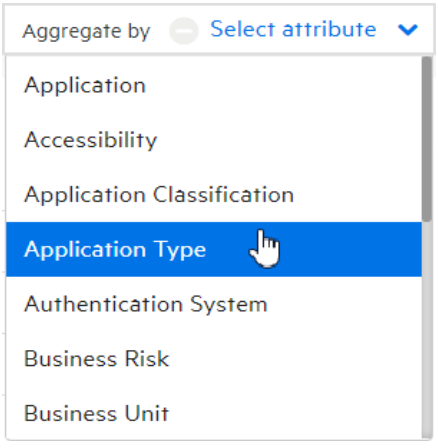


To group your data based on a single application version attribute, select the attribute from the **Group by** list. (The default grouping attribute is the application version.)

In addition to the grouping attribute you selected, the resulting data reflects any attributes you have selected from the **Aggregate by** and **Filter by** lists.

Note: You can achieve finer control over the data displayed if your **Group by** list includes custom attributes (of the single-select type). For instructions on how to create custom attributes, see "Creating Custom Attributes" on page 238.

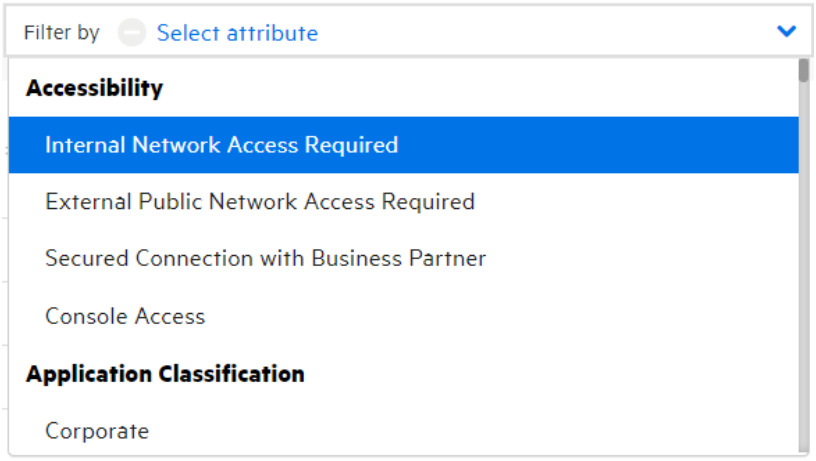
Selecting an aggregating attribute



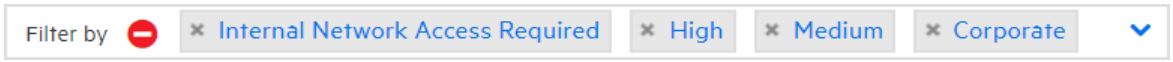
To aggregate the data shown on the Dashboard based on a single application attribute, select the attribute from the **Aggregate by** list. The Dashboard displays your data based on the aggregating attribute, and any attributes you have selected from the **Group by** and **Filter by** lists.

Note: You can achieve finer control over the data displayed if your **Aggregate by** list includes custom attributes (of the single-select type). For instructions on how to create custom attributes, see "Creating Custom Attributes" on page 238.

Selecting one or more filtering attributes

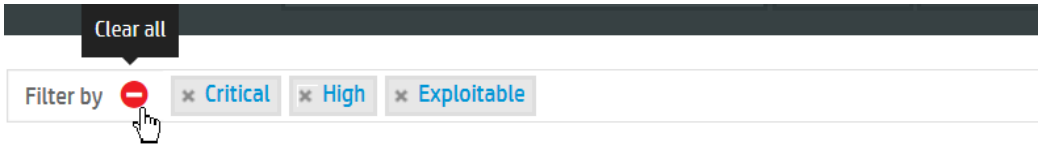


To selectively display data based on an application attributes, select an attribute from the **Filter by** list. You can select multiple attributes, but you must select them one at a time.



The Dashboard displays your data based on the selected filter attributes, and any other attributes you have selected from the **Group by** and **Aggregate by** lists.

Clearing selections from the custom attributes lists



To clear your attribute selection from a list, click the **Clear all** icon .

You can export Fortify Software Security Center data displayed on the ISSUE STATS and AUDIT pages to comma-separated values (CSV) files. For details, see "Exporting Data to Comma-Separated Values Files" below.

Exporting Data to Comma-Separated Values Files

You can export selected data for an application version or data for all Fortify Software Security Center application versions to comma-separated values (CSV)

files.

Exporting the Dashboard Summary Table

To export the summary table displayed on the Dashboard:

1. On the Fortify header, click **DASHBOARD**.
2. On the toolbar, click **EXPORT**.

   Note: A missing **EXPORT** button indicates that your administrator has disabled this functionality.
3. In the EXPORT CSV dialog box, in the **File Name** box, type the name for the file.
4. (Optional) In the **Notes** box, type information about the data you are exporting.
5. Click **SAVE**.
6. To view the exported result:
   a. On the Fortify header, click **REPORTS**.
   b. On the Reports page, click **DATA EXPORTS**.
   c. Specify whether to save or open the file.
   d. In the resulting table, move your cursor to the row for the exported file, and then click the **Download** icon .

To determine how long the system retains your CSV files before they are deleted, see the instructions provided in "Configuring Job Scheduler Settings" on page 135.

Exporting Selected Data for an Application Version to a CSV File

To export data from the ISSUE STATS or AUDIT page to a CSV file:

1. (Optional) If you are exporting data from the Issue Stats page, you can select attributes to aggregate or filter by. On the AUDIT page, you can select attributes to filter by.

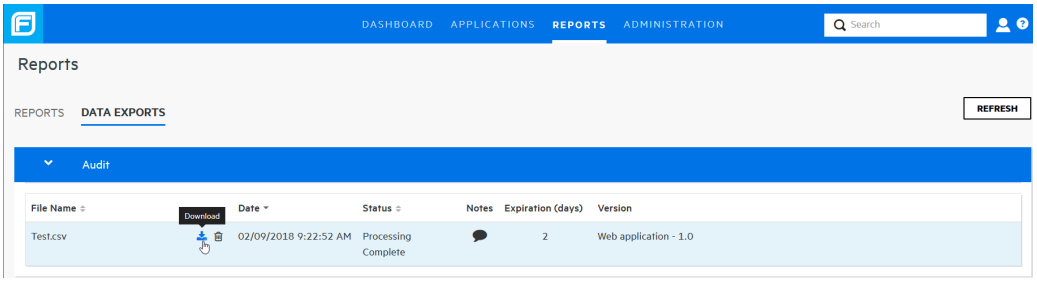
   Note: The **EXPORT** button is removed if you specify an attribute in the **Group by** on either the ISSUE STATS page or the AUDIT page.

2. On the toolbar, click **EXPORT**.

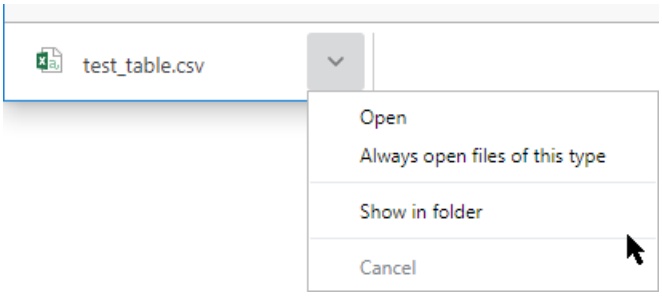
   Note: A missing **EXPORT** button indicates that your administrator has disabled this functionality.
3. In the EXPORT CSV dialog box, in the **File Name** box, type the name for the file.
4. (Optional) In the **Notes** box, type information about the data you are exporting.

5. Click **SAVE**.
6. To view the exported result:
   a. On the Fortify header, click **REPORTS**.
   b. On the Reports page, click **DATA EXPORTS**.



   c. In the resulting table, move your cursor to the row for the exported file, and then click the **Download** icon .

      The CSV file is saved to your **Downloads** folder.



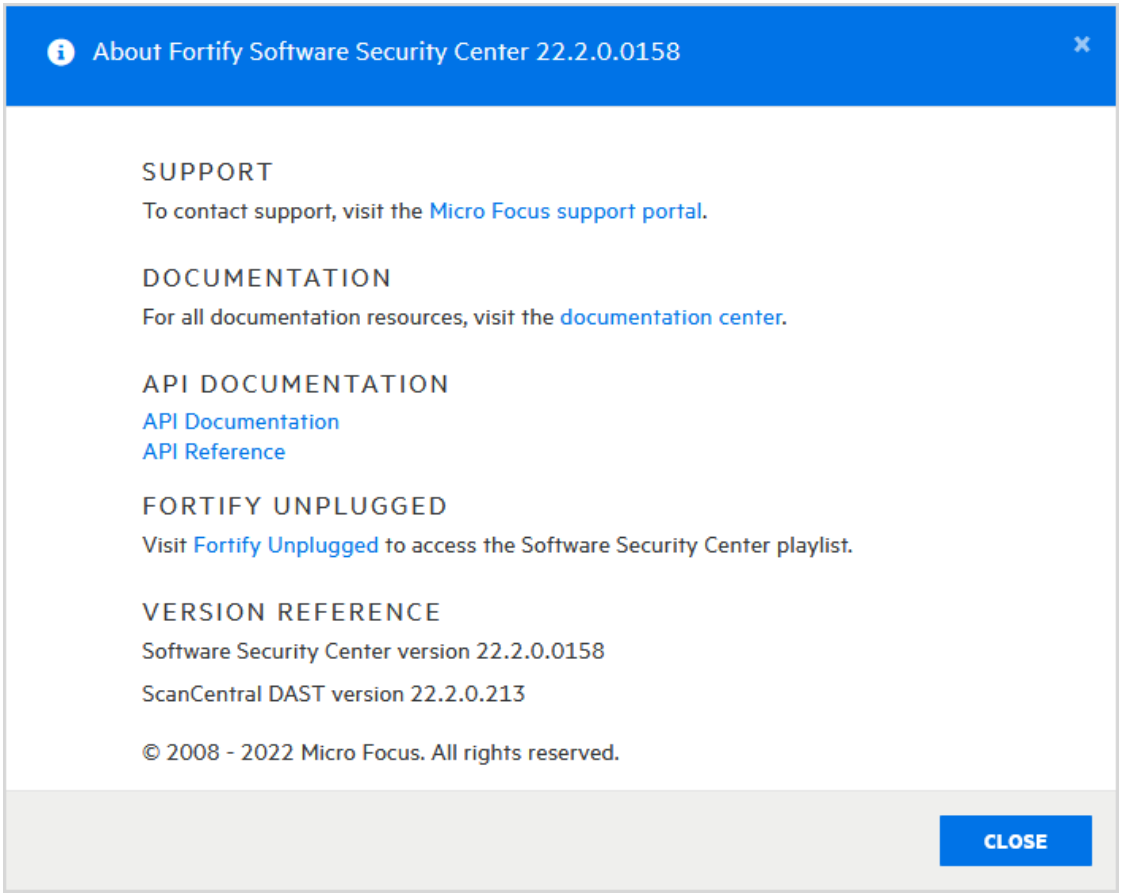
   d. In the status bar, select the arrow next to the CSV file name, and then specify whether to open the file or view it in the **Downloads** folder.

To determine how long the system retains your CSV files before they are deleted, see the instructions provided in "Configuring Job Scheduler Settings" on page 135.

Accessing the Fortify Software Security Center API Documentation

To access the Fortify Software Security Center API Documentation:

1. On the Fortify header, click the help icon .



2. In the About Fortify Software Security Center *<version>* box, click the **API Documentation** link.

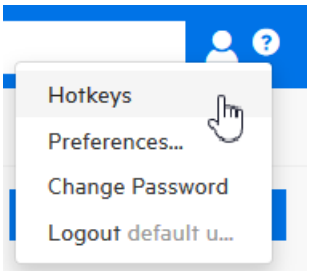
The FORTIFY SOFTWARE SECURITY CENTER API DOCUMENTATION VERSION <*version*> web page opens.

Tip: It is also very useful to leverage a proxy such as the Chrome DevTools to intercept Fortify Software Security Center traffic and determine the appropriate endpoint call(s) to make to perform user interface actions.

Viewing Fortify Software Security Center Keyboard Hotkeys

To view the keyboard hotkeys used to navigate the Fortify Software Security Center user interface:

1. Log in to Fortify Software Security Center.
2. Do one of the following:
   - At the right end of the Fortify header, click the user profile icon, and then select **Hotkeys**.

   - Press the question mark key (?) on your keyboard.

See Also

"Setting Preferences: System-Wide and Across Application Versions" on page 212

Chapter 10: Managing User Accounts

The topics in this chapter provide information about Fortify Software Security Center user accounts and how to work with them.

Fortify Software Security Center User Account Management

As described in the secure deployment guidelines, the primary system administrator of a new Fortify Software Security Center installation creates a non-default Administrator-level account, and then deletes the default admin account. Use the non-default Fortify Software Security Center administrator account to create additional Fortify Software Security Center user accounts.

Fortify Software Security Center supports several default user roles. The following sections provide information about each of these roles.

This section contains information about Fortify Software Security Center roles, user account administration, how to register LDAP entities with Fortify Software Security Center, and how to configure an integration with Microsoft Azure AD.

About Tracking Teams

As an administrator or security lead, you need access to information that enables you to track and monitor your team's progress and ensure that good application security practices are in place and followed. Fortify Software Security Center provides a central point for guiding the adoption of good security practices. By understanding how information is tracked and reported, you can accurately measure development team progress based on application security standards.

About Roles

Roles determine the actions a user can perform in Fortify Software Security Center.

For more fine-grained control over user access to Fortify Software Security Center functionality, you can create custom roles and assign them permissions from the Fortify Software Security Center interface. For instructions on how to create a role, see "Creating Custom Roles" on page 223.

Pre-configured Roles

The following table lists the pre-configured roles you can assign to users in Software Security Center. For information about how to view the permissions associated with

each pre-configured role, see "Viewing Permission Information for Fortify Software Security Center Roles" on page 181.

Role	Description
Administrator	Has full access to the system and all results
Application Security Tester	Performs tasks required to execute dynamic scan requests, including: • View application versions • View and generate reports • Process dynamic scans • Upload scan results • Audit issues
Developer	Developer responsible for producing security results and taking action to triage or remediate security issues
Manager	Responsible for guiding developers to work on results Managers cannot create applications but can grant or revoke access to their team members
Security Lead	Security team member who can create application versions and users
View Only	Can view results, but cannot interfere with the issue triage or the remediation process. Example users: system automation account or temporary auditor
WebInspect Enterprise System	Can connect a WebInspect Enterprise instance to Fortify Software Security Center and retrieve issue audit information. This role is intended for use only by a WebInspect Enterprise instance.

See Also

"About Roles" on the previous page

"Creating Custom Roles" on the next page

Creating Custom Roles

You can define roles of your own and assign them permissions.

To define and configure permissions for a new role:

1. Log in to Fortify Software Security Center as an Administrator, and then, on the Fortify header, click **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION page, select **Users**, and then select **Roles**.
3. On the **Roles** toolbar, click **NEW**.
4. In the CREATE NEW ROLE dialog box, provide the information described in the following table.

   Important! Except for a new line in the **Description** field, **Name** and **Description** field values must not start with the characters =, -, +, or @, and must not include control characters. For a complete list of Unicode characters included in the restricted ranges, see https://www.aivosto.com/articles/control-characters.html.

Field	Description
Name	Role name
Description	(Optional, but recommended) Role description
Universal access	To assign the new role access to all application versions, select this check box. **Note:** Fortify strongly recommends that you select universal access only for administrator-level users.

5. To add permissions (specify the functional areas available to users in this role), click **+ADD PERMISSIONS**.
6. In the ADD PERMISSIONS dialog box, scroll through the table and select the check boxes that correspond to the permissions that you want to grant to the new role.
7. Click **DONE**.

   If any of the permissions you selected requires additional permissions, these are listed next to a warning sign ⚠.
8. To add the listed dependencies to the new role, click **ADD MISSING PERMISSIONS**.

   The CREATE NEW ROLE dialog box now lists the additional permissions (dependencies).
9. Click **SAVE**.

Tip: You can also use the **ADD MISSING PERMISSIONS** to add dependencies when you edit a custom role.

Fortify Software Security Center checks permissions to guard against states that are known to be incompatible. If the role and permissions you selected do not conflict, then you are returned to the **Roles** page, which displays detailed information about the new role.

Deleting Custom Roles

If a custom role listed on the Roles page is assigned to no user accounts, you can delete that role.

To delete a role:

1. Log in to Fortify Software Security Center as an Administrator or Security Lead, and then click **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Users**, and then select **Roles**.
3. In the table, select the check box for the custom roles you want to delete.
4. In the **Roles** toolbar, click **DELETE**.

   Fortify Software Security Center prompts you to confirm that you want to delete the role.
5. Click **OK**.

See Also

"Creating Custom Roles" on the previous page

Fortify Software Security Center Account Administration

Only users who have Administrator accounts can create new user accounts and edit information for existing accounts. Use Administrator accounts to manage the Fortify Software Security Center system. Fortify recommends that you create only the Administrator-level accounts necessary to create and edit local or LDAP Fortify Software Security Center user accounts. The Security Lead and lesser accounts can perform all other application-related activities.

Fortify Software Security Center permits the explicit addition of Administrator-level accounts to application versions. This enables Administrator users to be assigned issues from the AUDIT page.

Topics covered in this section:

Creating Local User Accounts

Fortify Software Security Center Administrator-level users can add new local user accounts to the list of Fortify Software Security Center users.

Important! You cannot create externally managed users from Fortify Software Security Center. These can only be provisioned using the SCIM API.

To create a Fortify Software Security Center user account:

1. Log in to Fortify Software Security Center as an Administrator, and then, in the Fortify header, click **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Users**, and then select **Local Users**.

   The **Local Users** page lists local users.
3. In the **Local Users** toolbar, click **+ADD**.
4. In the CREATE NEW USER dialog box, provide the information listed in the following table.

   Important! Values for fields in the following table marked with an asterisk (*) *must not* start with the characters =, -, +, or @, and must not include control characters.

Field or Check Box	Description
*Username	Username for Fortify Software Security Center logon.
*First Name	(Optional, but strongly recommended) First name of user.
*Last Name	(Optional, but strongly recommended) Last name of user.
*Email	(Optional) Email address of user. **Caution!** Although an email address is not required, the user cannot receive email alerts and notifications unless you provide one.
Password	Password for the new user.

Field or Check Box	Description
	The **Password Strength** indicator displays the relative strength of the password you entered. You can save the user account information only if the password is evaluated as strong or very strong.
Confirm Password	Password for the new user.
User must change password at next login	Leave this check box selected to require the user to change the password at the next login to Fortify Software Security Center.
Password never expires	Select this check box to allow the user to use the originally assigned password until he or she wants to change it. To require the user to change his or her password every thirty days, leave this check box cleared.
Suspended	Select this check box to suspend user access to Fortify Software Security Center.
Roles	(Optional, but strongly recommended) Select the check boxes for all roles to assign to the user. **Caution!** Although this is optional, keep in mind that a user who has no assigned role cannot access Fortify Software Security Center unless that user belongs to a local group that does have an assigned role.
Access	To specify the applications that the new user can access: **Note:** If you have assigned the user the role of Administrator or WebInspect Enterprise System, that user has universal access to all Fortify Software Security Center applications. a. To open the SELECT APPLICATION VERSION dialog, click **ADD**. b. From the **APPLICATION** list, select an application to

Field or Check Box	Description
	which you want the user to have access. The **VERSIONS** list in the center pane displays all active versions of the selected application. c. Select the check boxes for all versions that you want the user to be able to access. To select all versions, select the **Select all** check box. On the right, the **SELECTED VERSIONS** pane lists the versions you selected. d. To add another application version or versions, repeat steps a through c. e. Click **DONE**.

5. Do one of the following:
   - To save your settings and exit the CREATE NEW USER dialog box, click **SAVE**.
   - To save your settings and create another new user, click **SAVE AND ADD ANOTHER**.

Fortify Software Security Center adds the user account to the list of local users.

See Also

"Editing Local User Accounts" below

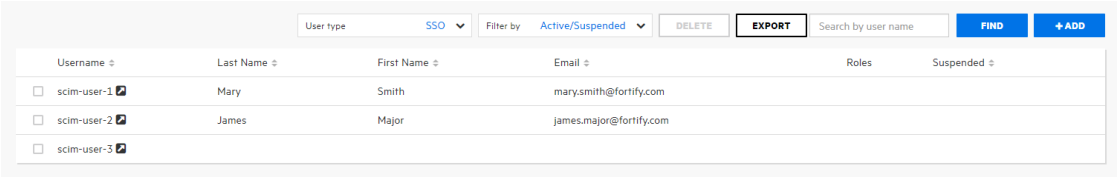
"Unlocking Local User Accounts" on page 229

Editing Local User Accounts

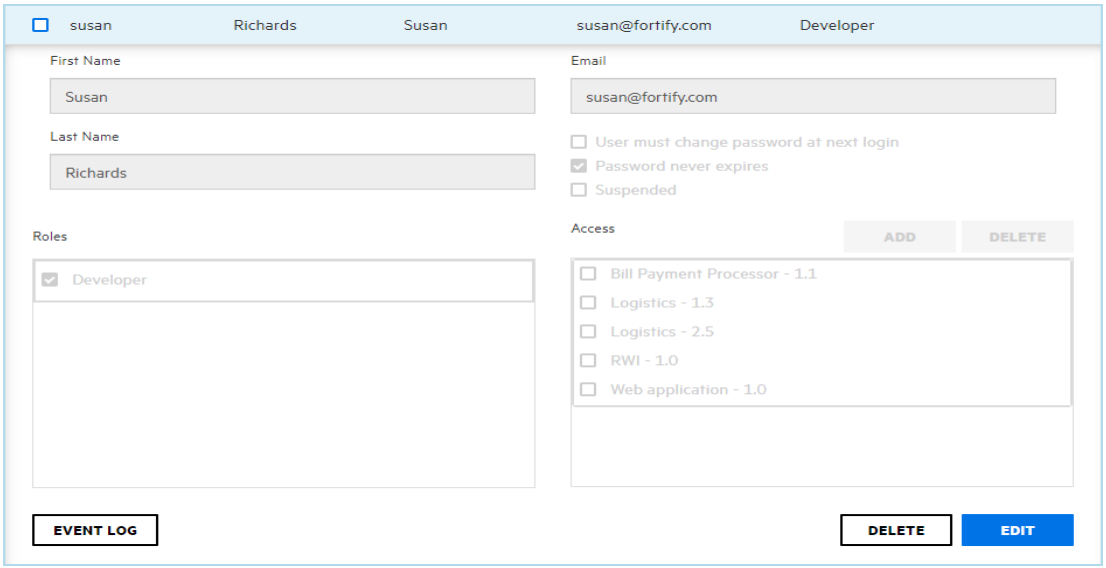
The following procedure describes how to edit the account for local user accounts created from Fortify Software Security Center, as well as user accounts provisioned using the SCIM API.

To edit a local user account:

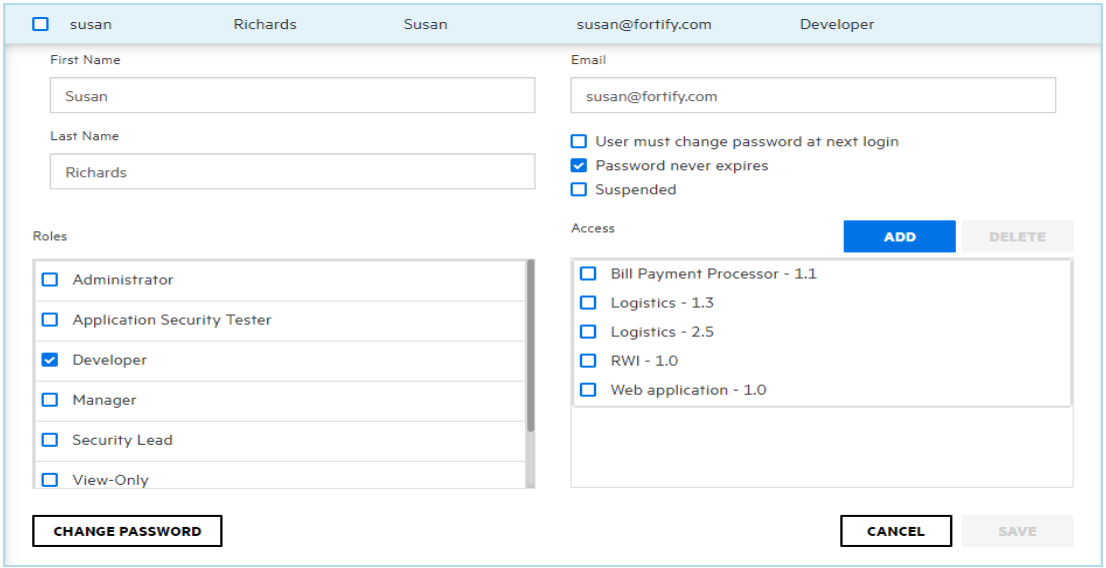
1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Users**, and then click **Local Users**.
3. To selectively view externally managed users (provisioned using the SCIM API), from the **User type** menu, select **SSO**.



4. Locate the user account you want to edit, and then click the row to expand it and view account details.



5. Click **EDIT**.



6. Make any required changes to values in the **First Name**, **Last Name**, and **Email** boxes.

Important! Values for the **First Name**, **Last Name**, and **Email** fields *must not* start with the characters =, -, +, or @, and must not include control characters. For a complete list of Unicode characters included in these restricted ranges, see https://www.aivosto.com/articles/control-characters.html.

Important! From Fortify Software Security Center, the only changes you can make to externally-managed user and group accounts are role and application version assignments. All other configuration (and deletion) must be performed from Azure AD.

7. To change the email address password expiration policy, select or clear the check boxes below the **Email** box, as needed.
8. To change the roles assigned to the user, in the **Roles** section, select or clear the check boxes for available roles.
9. To remove the user from application versions, in the **Access** section, select the check boxes for the application versions, and then click **DELETE**. To assign the user to different application versions, click **ADD**, and then use the SELECT APPLICATION VERSION dialog box to specify the application versions the user is to work on. (For details, see "Creating Local User Accounts" on page 225.)
10. To change the password for the user, click **CHANGE PASSWORD**, and then use the CHANGE PASSWORD dialog box to specify a new password. (If this is an externally managed user, the **CHANGE PASSWORD** button is not available.)
11. Click **SAVE**.

See Also

"Unlocking Local User Accounts" below

"Creating Local User Accounts" on page 225

Unlocking Local User Accounts

After a local user tries unsuccessfully to log in to Fortify Software Security Center three times in a row, Fortify Software Security Center prevents the user from attempting more logins. If email notifications are enabled, the user receives an email to advise the user that he or she is locked out and should notify the Fortify Software Security Center administrator. As an administrator, you can unlock the account for the user.

Note: The locking and unlocking of user accounts does not apply to users provisioned through the SCIM API.

After a user notifies you that they are locked out of their account, unlock the account as follows:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Users**, and then click **Local Users**.
3. Bring up the locked user account, expand the row to display account details, and then click **UNLOCK USER**.
4. Fortify Software Security Center prompts you to confirm that you want to unlock the account.
5. Click **OK**.

See Also

"Creating Local User Accounts" on page 225

"Editing Local User Accounts" on page 227

Viewing Externally Managed Users and Groups

To view externally managed users provisioned using SCIM protocol:

1. Log in to Fortify Software Security Center as a local administrator.
2. On the Fortify header, click **ADMINISTRATION**.
3. In the left pane, select **Users**, and then select **Local Users**.
4. At the top of the Local Users page, from the **User type** list, select **SSO**.

   Fortify Software Security Center lists the users provisioned using SCIM protocol. The **Externally managed user** icon ( ) is displayed next to each username listed in the Local Users table.

To see the groups pushed to Fortify Software Security Center from Azure AD:

1. Log in to Fortify Software Security Center as a local administrator.
2. In the Fortify header, select **ADMINISTRATION**, select **Users**, and then select **Local Groups**.

Assigning Roles to Externally Managed Users and Groups

A user or member of a local group provisioned from an identity management service such as Azure AD cannot access Fortify Software Security Center unless the group has been assigned one or more roles, or the user is assigned a role individually from the Local Users page.

Note: From Fortify Software Security Center, the only changes you can make to externally-managed user and group accounts are role and application version assignments. All other configuration (and deletion) must be performed from Azure AD.

Assign roles to externally managed users and groups just as you would to local users created through the ADMINISTRATION view.

See Also

"Implementation of SCIM 2.0 Protocol" on page 127

"Enabling SCIM for Provisioning of Externally Managed Users and Groups" on page 132

"Using SCIM 2.0 and SAML 2.0 to Configure a Connection to Azure AD for User Provisioning" on page 129

"Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single Sign-On" on page 150

Chapter 11: Applications and Application Versions

To obtain consistent measurement results in Fortify Software Security Center, you define an application for a single code base. Fortify Software Security Center organizes the iterative development and remediation of code bases into *applications* and *application versions*.

- An application is a code base that serves as a container for one or more application versions. If you are working with a new code base, you create a new Fortify Software Security Center application. Fortify Software Security Center automatically creates the first version of that application.
- An application version is an instance of the application or code base that is to eventually be deployed. It contains the data, auditing, and attributes for a particular version of the application code base. If you are working with an existing code base, you create new application *versions* rather than new applications.

An application version is the base unit for team tracking. It provides a destination for security results that is useful for getting information in front of developers and producing reports and performance indicators. Code analysis results for an application version are tracked as shown in the following table.

Existing Analysis Results	+ New Scan Results	= Trending Results
Results of any previous security analysis from Fortify Static Code Analyzer, Fortify WebInspect, or other analyzer	Merge with the existing results (from the same analyzer used to perform this scan) Mark resolved issues Identify new issues Keep unchanged issues	Identify security issues that have been fixed, and issues that remain.

Fortify Software Security Center analysis processing rules verify that the new scan is comparable to the older scan.

This content provides information about applications and application versions. It contains instructions for viewing and creating applications, configuring application attributes, assigning issue templates, and more.

Topics covered in this section:

About Tracking Development Teams

As an administrator or security lead, you need access to information that enables you to track and monitor your team's progress and ensure that good application security practices are in place and followed. Fortify Software Security Center provides a central point for guiding the adoption of good security practices. By understanding how information is tracked and reported through applications and applications versions, you can accurately assess development team progress based on application security standards.

Topics covered in this section:

About the Application Creation Process

After you log in to Fortify Software Security Center and start to add a new application, the CREATE NEW APPLICATION VERSION wizard displays a sequence of steps, each of which presents the team members responsible for creating the application version with one or more strategic choices. After the team agrees upon and makes their selections, the security lead can click **FINISH** to complete the creation process.

Typically, the security team evaluates and decides on all the options before they actually start to create the application version. The following sections describe the options displayed on the wizard screens.

Next

"Application Version Attributes" on page 236

See Also

"Template Selection" on page 245

"Creating the First Version of a New Application" on page 246

"Adding a New Version to an Application" on page 249

Strategies for Creating Application Versions

As a Security Lead, you might choose to create an application version that allows you to track vulnerabilities within deployed applications. Security vulnerabilities often occur in areas of code where different components come together. Although teams may work on different components, it is a good practice to track the entire software component as one piece. As an example, suppose that a text manipulation library is safe on its own, and a file access library is safe on its own. The combination of the text manipulation library and file access library is not necessarily safe, because one may not know the origin of the text being processed.

Strategies for Packaged Software

For software that ships or is deployed as a concrete version, you might use the following strategies:

- If you are creating a brand new application, start a new application version.
- Create a single application version for each release. For example, the Security Lead or Development Manager may deactivate past versions in Software Security Center to archive results and remove them from view. For information about how to deactivate an application version, see "Deactivating Application Versions" on page 287.

  Note: Although a deactivated application version is hidden from view, it still exists in the database. Deleting all versions of an application deletes the application from the database altogether.

- If you are working on an existing application with an evolving code base, create an application version based on an existing version. For example, Application A has several versions. Each new version is initiated based on the results of the previous version. Each successive version is just evolved code (versus a complete rewrite).

Strategies for Continuous Deployment

For applications that use continual deployment, running scans with the `-build-label xxxx` flag enables you to identify which source control checkout was scanned (where `xxxx` represents the ID from your version control system). Relating scans to source control checkout improves your ability to determine when individual issues were introduced and remediated.

About Annotating Application Versions for Reporting

Fortify Software Security Center provides a set of application attributes that you can apply to individual application versions. You can use these attributes to group application versions for reporting, or to associate application versions with external systems.

Administrators can customize the base set of application attributes that Fortify Software Security Center provides. Sample customizations can help organizations track onboarding progress by application ID, line of business, business unit, or regulatory compliance obligations.

Viewing a List of Fortify Software Security Center Applications

To view a list of all Fortify Software Security Center applications:

- On the Fortify header, click **APPLICATIONS**.

See Also

"Searching Applications and Application Versions from the Applications View" on page 254

About Creating Application Versions

You can create a new Fortify Software Security Center application version for an entirely new application or create one for existing application version. The following topics provide instructions for each method:

"About the Application Creation Process" on page 234

"Creating the First Version of a New Application" on page 246

"Adding a New Version to an Application" on page 249

Application Version Attributes

Application versions have business attributes, technical attributes, and organization attributes. These attributes are metadata that Fortify Software Security Center uses to perform cross-application comparisons and reporting.

When you create a new application version, the CREATE NEW VERSION wizard guides you through the selection of required and optional business, technical, and organization application attributes. The application version cannot be finished until you select values for all required attributes. For example, to create an application version, you must specify values for the following attributes:

- Development phase
- Development strategy

- Accessibility

In addition to the default attributes that Fortify Software Security Center provides, Administrators and Security Leads can create custom attributes to assign to application versions. Custom attributes are extremely useful when you need to focus on a highly specific subset of data. For instructions on how to create custom attributes, see "Creating Custom Attributes" on the next page.

The following tables list the default set of attributes for Fortify Software Security Center applications. Note that this list does not include custom attributes that a Fortify Software Security Center administrator may have added to the system. Attributes marked with an asterisk are required.

Technical Attribute	Description
*Development Phase	Current phase of development the application version is in.
*Development Strategy	Staffing strategy used for application development
*Accessibility	Level of access required to use the application
Application Type	Nature of the code base (library, application, or application component)
Target Deployment Platform	Deployment platform for the application
Interfaces	Interfaces used to access the application
Development Languages	Languages used to develop the application
Authentication System	System used to authenticate users who try to access to the application

Organization Attributes	
Business Unit	Business unit for which the application is to be developed or business unit to develop the application
Industry	Industry for which the application is to be developed
Region	Geographical location of the development team

Business Risk Attributes	
Business Risk	Relative risk (high, medium, or low) the application poses to the business goals of the organization
Known Compliance Obligations	All known compliance obligations that the application must meet
Data Classification	Types data to be stored by this application
Application Classification	Direct consumers of the application

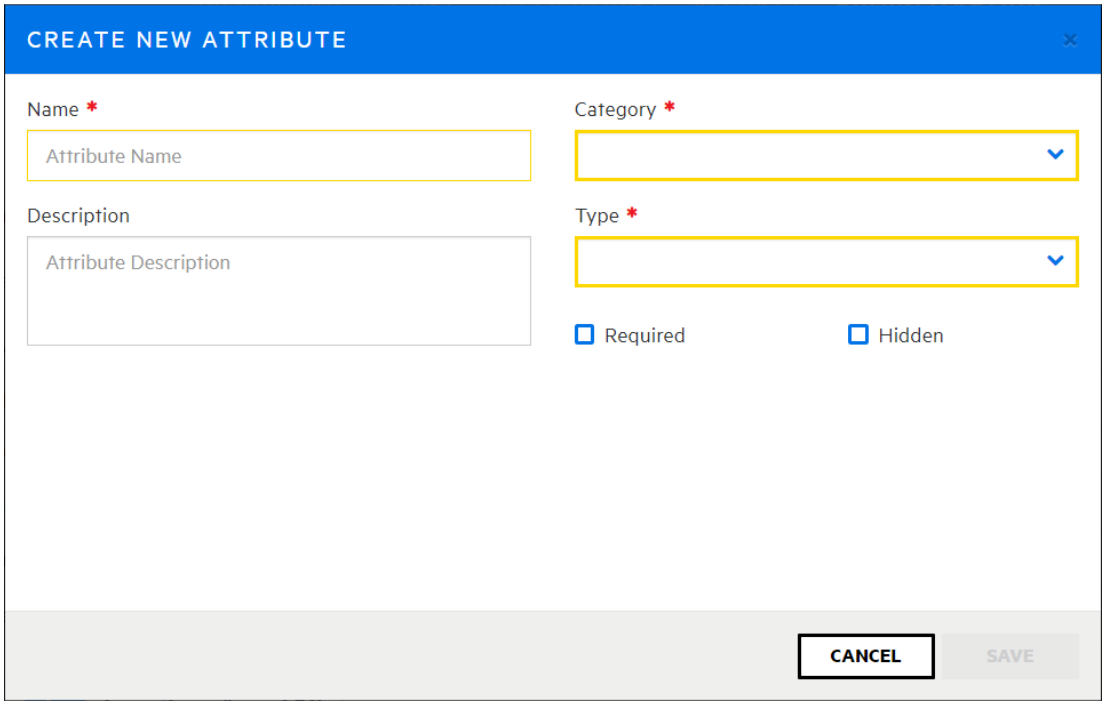
Creating Custom Attributes

Fortify Software Security Center comes with technical, organization, and business attributes that enable administrators and security leads to categorize applications and application versions. As an administrator or a security lead, you can create your own custom attributes that can be set for application versions.

Note: You can create custom attributes only if you have either an Administrator or Security Lead user account.

To create an attribute:

1. Log in to Fortify Software Security Center as an administrator or a security lead.
2. On the Fortify header, click **ADMINISTRATION**.
3. In the left pane, under **Templates**, click **Attributes**.
   The Attributes page lists the attributes on the right.
4. Click **NEW**.



5. In the CREATE NEW ATTRIBUTE dialog box, provide the information described in the following table.

Field	Description
Name	Type a descriptive name for the attribute. **Important!** If you delete an attribute that Fortify Software Security Center uses out-of-the-box, and you then create a new attribute with the same name, database migration may fail.
Description	Type a brief description. The description is displayed under the attribute field in the CREATE NEW APPLICATION VERSION wizard.
Required	Select this check box to require users to set the attribute that you are defining here when they create an application template.
Hidden	Select this check box to prevent the new attribute from being displayed in the CREATE NEW APPLICATION VERSION wizard.

Field	Description
	Caution! If you select **Hidden** to prevent the attribute from showing in the CREATE NEW APPLICATION VERSION wizard, you must also clear the **Required** check box.
Category	Select an attribute type. Depending on the category you select, the attribute is displayed on the **Business Attributes** step, the **Technical Attributes** step, or the **Organization Attributes** step of the CREATE NEW APPLICATION VERSION wizard.
Type	Select one of the following control types: • To create a text field into which a user can type a single line of text, select **Text - Single Line**. • To create a list from which a user can select only a single value for the attribute, select **List of Values - Single Selection**. **Note:** If you create a single-select type attribute, users can select it from the **Group by** and **Aggregate by** lists on the Dashboard to customize the data they view. • To create a list from which a user can select multiple values for the attribute, select **List of Values - Multiple Selection**. • To create a text field into which a user can type multiple lines of text, select **Text - Multiple Lines**. **Note:** If you select one of the **List of Values** types, additional fields are displayed in which you add the values and their descriptions, and specify whether or not they are hidden. • To create a check box for the attribute, select **Boolean**. • To create a field that accepts an integer value, select **Integer**. • To create a calendar selection control for the attribute, select **Date**.

Field	Description
	Note: This type is not available for a Dynamic Scan Request attribute. • To create a file upload field, select **File**. • To create a file upload control in the Dynamic Scan Request dialog box, select **File**.

6. Click **SAVE**.

The new attribute is available the next time a user uses the CREATE NEW APPLICATION VERSION wizard.

For instructions on how to specify custom attributes in existing application versions, see "Specifying New Custom Attributes for Application Versions" on page 243.

Note: By default, an attribute you create through the Fortify Software Security Center user interface is deletable. You can use the Fortify Software Security Center API to define a non-deletable attribute. For information about how to access the API see "Accessing the Fortify Software Security Center API Documentation" on page 219.

See Also

"Deleting Attributes and Attribute Values" below

"Application Version Attributes" on page 236

Deleting Attributes and Attribute Values

If an attribute or attribute value is no longer of use, you can often delete it from the Fortify Software Security Center database, event if it is currently associated with one or more application versions. Doing so removes all traces of the attribute or attribute value from the system.

Deleting Attributes

To delete an attribute from the Fortify Software Security Center database:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, expand the **Templates** section, and then select **Attributes**.

   If an attribute can be deleted, the check box to the left of its name is blue. If it cannot be deleted, the check box to the left of its name is gray, and you cannot select it for deletion.

To see an explanation of why you cannot delete an attribute, move your cursor over the check box. (The attribute is either system-defined and non-deletable, or it is user-defined and has been modified so that it cannot be deleted.)

3. Select the check boxes for the attributes you want to delete, and then click **DELETE**.

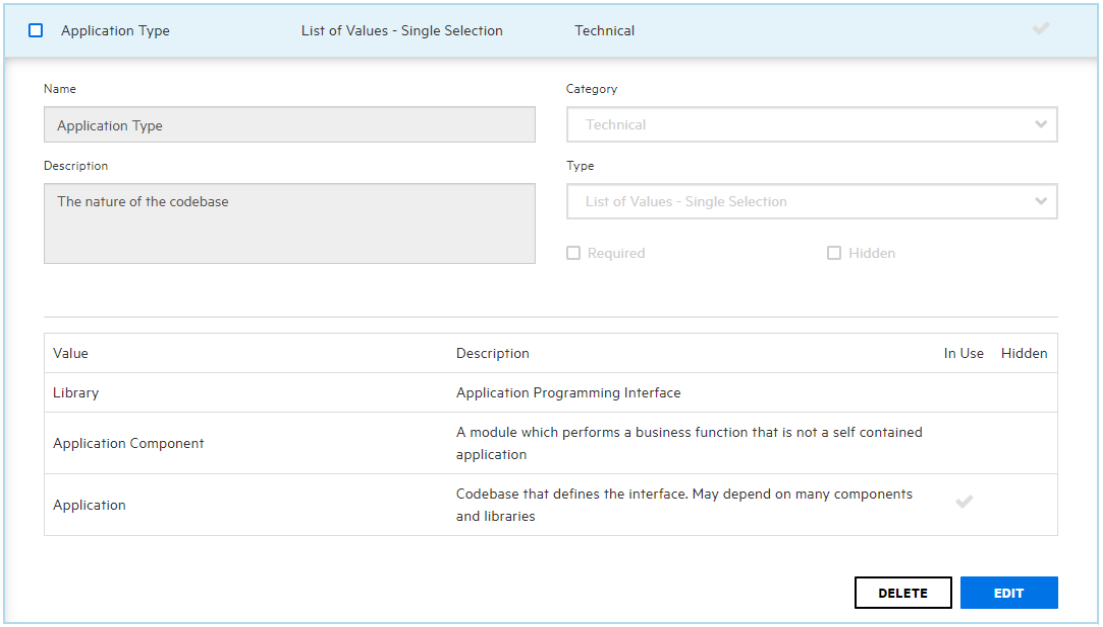
   Fortify Software Security Center alerts you to the fact that the selected attributes will be permanently removed from the system and prompts you to confirm that you want to continue with the deletion.
4. Click **OK**.

Note: By default, an attribute you create through the Fortify Software Security Center user interface is deletable. You can use the Fortify Software Security Center API to define a non-deletable attribute. For information about how to access the API see "Accessing the Fortify Software Security Center API Documentation" on page 219 .

Deleting Attribute Values

To delete an attribute value:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, expand the **Templates** section, and then select **Attributes**.
3. Expand the row for the attribute that has one or more values that you want to delete.

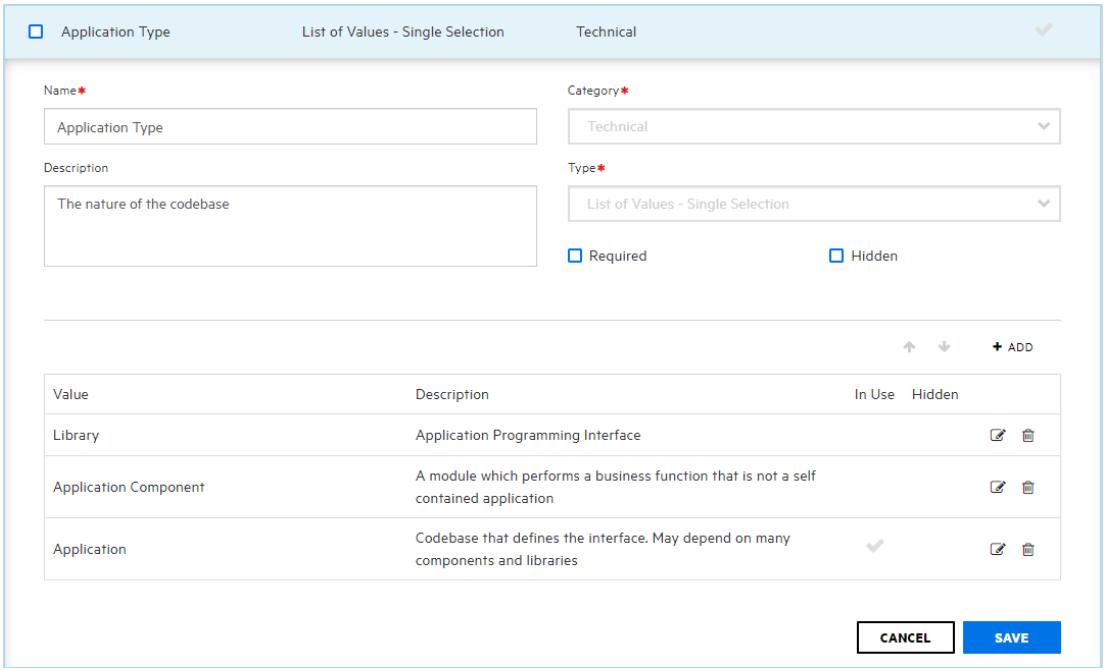


The **In Use** column shows which of the values are currently used with one or more application versions.

4. Click **EDIT**.

Fortify Software Security Center displays a warning to remind you that any changes you make can affect application versions with values based on the attribute, and prompts you to confirm that you want to edit the attribute.

5. Click **OK**.



6. Click the trash icon ( ) to the right of the value you want to delete.

Note: You can delete some attribute values, even if they are currently in use by one or more application versions. However, you cannot delete:

- Values for system-defined list-type attributes that are in use
- Values for system-defined attributes other than list type
- Values that are both in use and that belong to a dynamic scan type attribute
- Values for user-defined attributes designated as non-deletable that are in use

Fortify Software Security Center removes the value without prompting you for confirmation. If you decide that you prefer not to delete the value, just click **CANCEL** to restore it.

See Also

"Creating Custom Attributes" on page 238

Specifying New Custom Attributes for Application Versions

To apply a new custom attribute to an application version:

1. On the Fortify header, select **APPLICATIONS**.
2. In the Applications view, expand the row for the application and then select the version for which you want to specify a new attribute.

   Fortify Software Security Center displays the AUDIT page for that version.
3. On the application version toolbar, click **PROFILE**.

   The APPLICATION PROFILE - <*application_name*> <*application_version*> window opens to the **ADVANCED OPTIONS** section.
4. Click **APPLICATION SETTINGS**.
5. In the **Version Settings** section, click the edit icon.
6. On **Step 1. GENERAL** of the EDIT VERSION wizard, click **NEXT**.
7. On **Step 2. DEFINE ATTRIBUTES AND RISK**, select the attribute category (**Technical Attributes**, **Organization Attributes**, or **Business Risk Attributes**), and then select the value or values for the custom attribute.
8. Navigate to Step 4 of the wizard, and then click **FINISH**.

See Also

"Creating Custom Attributes" on page 238

"Editing Application Version Details" on page 255

About Issue Templates

Applications are defined by *issue templates*, which determine how Fortify Software Security Center configures and prioritizes the issues uncovered in your application source code.

An issue template contains the following settings:

- Folder filters–Controls how issues are sorted into the folders
- Visibility filters–Controls which issues are shown and hidden
- Folder properties–Name, color, and which filter set it is active in
- Custom tags–Specifies which audit fields are displayed and the values for each

Fortify Software Security Center comes with pre-designed issue templates that you can either use as they are, or modify (from Fortify Audit Workbench) to suit your application needs.

To see descriptions of these out-of-the-box issue templates:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Templates**, and then select **Issue**.

The Issue page lists the issue templates and their descriptions.

You can import a Fortify Software Security Center issue template into Fortify Audit Workbench, modify it, save it with a new name, and then import it into Fortify Software Security Center. You can also create a new issue template from scratch in

Fortify Audit Workbench. For instructions on how to modify or create an issue template in Fortify Audit Workbench, see the *Fortify Audit Workbench User Guide*.

Adding Issue Templates to the System

To add an issue template that you created or modified in Fortify Audit Workbench to Fortify Software Security Center:

1. Log in to Fortify Software Security Center as an administrator.
2. On the Fortify header, click **ADMINISTRATION**.
3. In the pane on the left, select **Templates**, and then select **Issue**.
   Fortify Software Security Center lists the system issue templates in a table to the right.
4. Click **NEW**.
5. In the **Name** box in the CREATE NEW ISSUE TEMPLATE dialog box, type the template name.
6. (Optional) in the **Description** box, type a description that lets users know how to use the template.
7. Click **BROWSE**, and then locate and select the new or modified template.
8. Click **SAVE**.

Creating or Modifying Issue Templates

If you use Fortify Audit Workbench to create a new issue template or modify an existing template, you must make sure that the template includes the following filter:

```
<Filter>

  <actionParam>true</actionParam>

  <query>[category]:Insecure Dependency\: Vulnerable Component [analysis type]:SCA</query>

  <action>hide</action>

</Filter>
```

For information about how to create or modify issue templates and upload them to Fortify Software Security Center, see the *Fortify Audit Workbench User Guide*.

Template Selection

Fortify Software Security Center issue templates provide Fortify client and server products an optimal means of categorizing, summarizing, and reporting application data. Issue templates also enable the use of customized application settings at the enterprise level and not just at the application level.

Although you can change the issue template for an application after you finish creating the application, your security team must carefully consider its choice of template before completing the application creation process.

Creating the First Version of a New Application

A Fortify Software Security Center application version consists of the data and attributes for a given variant of the application code base. The following procedure describes how to create the first version of a new application.

To create a new application:

1. Log in to Fortify Software Security Center as either an Administrator or a Security Lead.
2. On the toolbar, click **+ NEW APPLICATION VERSION**.
3. On the **GENERAL** tab of the CREATE NEW APPLICATION VERSION wizard provide the information described in the following table.

Important! Values for fields in the following table marked with an asterisk (*) must not start with the characters =, -, +, or @, and must not include control characters. For a complete list of Unicode characters included in these restricted ranges, see https://www.aivosto.com/articles/control-characters.html.

Field	Description
Application Setup	
*Application name	(Required) Type the application name.
Application description	(Optional)Type a description of the new application.
Version Setup	
*Version name	(Required) Type a name for the version.
Version description	(Optional) Type information about this first version of the application.
Add to existing application	a. To use the settings of an existing application version, select this check box. Otherwise, proceed to step 4. b. To open the SELECT APPLICATION VERSION dialog box, click **BROWSE**. c. Under **APPLICATION**, type a string into the search box, and then click **FIND** to refine the list of applications, and then select the application that has the settings you want to use for the new application.

Field	Description
	The **VERSIONS** pane on the right lists the active versions of the selected application. d. To include inactive versions of the application, select the **Show inactive** check box. e. Select the check box for the version you want, and then click **DONE**. By default, Fortify Software Security Center includes all settings of the selected application version. f. To exclude one or more settings, clear the corresponding check boxes for the settings. g. To copy over all of the issues associated with the selected application version, select the **Application state** check box.

4. Click **NEXT** to advance to the **ATTRIBUTES** settings.
5. On the **TECHNICAL ATTRIBUTES** tab, provide the information described in the following table.

Field	Description
Development Phase	Leave **New** selected.
Development Strategy	Select the strategy used to develop the application version.
Accessibility	Select the value that specifies how the application is to be accessed.
Application Type	Select the application type.
Target Deployment Platform	Select the target deployment platform.
Interfaces	Select the check boxes for the interfaces available to access the application.
Development Languages	Select the check boxes for the languages used to develop the application version.

Field	Description
Authentication System	Select the check boxes for the authentication systems used to access the application.

6. (Optional) Click the **ORGANIZATION ATTRIBUTES** tab, and then make the following selections:
   - From the **Business Unit** list, select the business unit with which to associate the new application.
   - From the **Industry** list, select the industry for which this application is being developed.
   - From the **Region** list, select the region to associate with the application.
7. (Optional) Click the **BUSINESS RISK ATTRIBUTES** tab, and then do the following:
   a. From the **Business Risk** list, select the value that best represents the relative risk that this new application poses to the business goals of your organization.
   b. In the **Known Compliance Obligations** section, select the check boxes for all known compliance obligations that apply to the new application.
   c. In the **Data Classification** section, select the check boxes for all data classifications that this application stores.
   d. In the **Application Classification** section, select the check boxes for all consumer types for which this application is being developed.
8. To advance to the **TEMPLATE** settings, click **NEXT**.
9. Under **Issue Template**, select the check box for a template to set the minimum thresholds for issue detection. To see a description of a template in the pane to the right, select its check box.
10. To advance to the **ACCESS** tab, click **NEXT**.
11. a. To assign a user from the Fortify Software Security Center database, leave **LOCAL** selected.
    b. Select the check box for the team member or members you want to assign.

    Note: To find a specific user, type a user name into the **Search by user name** box, and then click **FIND**.

    Alternatively,

    a. To assign a user from the LDAP directory (if LDAP authentication is configured for your Fortify Software Security Center server), click **LDAP**, and then, from the **View by** list, select the attribute to use to display

LDAP entities.

b. Select the check box for the team member or members to assign.

Note: To find a specific user, type a username into the **Search by user name** box, and then click **FIND**.

12. Click **SAVE**.

    Fortify Software Security Center indicates that the application was successfully created. The new application version is now displayed in the APPLICATIONS view. Once data are uploaded for the application version, it is also displayed in the DASHBOARD view.
13. Click **CLOSE**.

Note: A new application is not listed on the Dashboard until you upload analysis results (artifacts) for it. However, it is listed in the Applications view. For information about how to upload artifacts for an application version, see "Uploading Scan Artifacts" on page 311.

See Also

"Adding a New Version to an Application" below

Adding a New Version to an Application

A version consists of the data and attributes for a given variant of the application code base. The following procedure describes how to create a new version of an existing application.

To create a new version of an existing application:

1. Log in to Fortify Software Security Center as either an Administrator or Security Lead.
2. From the Dashboard, click **+ NEW APPLICATION VERSION**.
3. On the **GENERAL** tab of the CREATE NEW APPLICATION VERSION wizard, under **Application Setup**, do the following:
   a. Select the **Add to existing application** check box.
   b. Click **BROWSE**, and then, in the SELECT APPLICATION dialog box, locate and select the application for which you want to create a new version.
   c. Click **DONE**.

   The **Application name** and **Application description** fields are populated with the name and description of the selected application.
4. In the **Version Setup** section, provide the information described in the following table.

Field	Description
Version name	Type a name for the version or select a version name from the list. **Important!** Values for fields in the following table marked with an asterisk (*) must not start with the characters =, -, +, or @, and must not include control characters. For a complete list of Unicode characters included in these restricted ranges, see https://www.aivosto.com/articles/control-characters.html.
Version description	(Optional) Type descriptive information about this version of the application.
Use existing application version	a. To use the settings of an existing application version, select this check box. Otherwise, click **NEXT** to proceed to the **ATTRIBUTES** tab. b. To open the SELECT APPLICATION VERSION dialog box, click **BROWSE**. c. Locate and select the application that has the settings you want to use for the new version. The VERSIONS pane on the right lists the active versions of the selected application. (To display inactive versions, select the **Show inactive** check box.) d. From the **VERSIONS** list, select the check box for the version you want, and then click **DONE**. By default, Fortify Software Security Center includes all settings of the selected application version. e. To exclude some of the settings, clear one or more of the following check boxes: ◦ **Version attributes** ◦ **Custom tags** ◦ **Analysis processing rules** ◦ **User access settings** ◦ **Bug tracker integration settings** f. To copy over all of the issues associated with the selected

Field	Description
	application version, select the **Application state** check box.

5. To proceed to the **ATTRIBUTES** settings, click **NEXT**.
6. On the **TECHNICAL ATTRIBUTES** tab, provide the information described in the following table.

Field	Description
Development Phase	From this list, select the current development phase of the new version.
Development Strategy	Select the strategy used to develop the new application version.
Accessibility	Select the value that specifies how the application is to be accessed.
Application Type	Select the application type.
Target Deployment Platform	Select the target deployment platform.
Interfaces	Select the check boxes for the interfaces available to access the application.
Development Languages	Select the check boxes for the languages used to develop the application version.
Authentication System	Select the check boxes for the authentication systems used to access the application.

7. (Optional) Select the **ORGANIZATION ATTRIBUTES** tab, and then provide the information described in the following table.

Field	Description
Business Unit	Select the business unit for which the application version is being developed.
Industry	Select the industry sector to which the application

Field	Description
	version applies.
Region	Select the region for which the application version is being developed.

8. (Optional) Select the **BUSINESS RISK ATTRIBUTES** tab.
9. From the **Business Risk** list, select the value that best represents the risk this application version poses to your organization.
10. Provide the information described in the following table.

Field	Description
Known Compliance Obligations	Select the check boxes for all of the known compliance obligations that the application version must meet.
Data Classification	Select the check boxes for all of the data classifications that apply to the application version.
Application Classification	Select the check boxes for all of the application classifications that apply to this application version.

11. To advance to the template setting, click **NEXT**.
12. Under **Issue Template**, select the check box for a template to set the minimum thresholds for issue detection. To see a description of a template displayed in the pane to the right, select its check box.

    Note: The default template is Prioritized High Risk Issue Template.

13. To advance to the **ACCESS** tab, click **NEXT**.
14. Under **TEAM**, do one of the following:

    Note: A user in the administrator role already has full access to all applications. You cannot assign the user to a team unless the user has also been assigned another role. This is true whether the Administrator is a local user or an LDAP user.

    - To assign a user from the Fortify Software Security Center database, select **LOCAL**, and then select the check boxes for the team member or members you want to assign.

Note: To find a specific user, type a user name into the **Search by user name** box, and then click **FIND**.

- Or, if LDAP authentication is configured for your Fortify Software Security Center server:

a. Click **LDAP**, and then, from the **View By** list, select the attribute to use to display LDAP entities.
b. Select the check box for the team member or members you want to assign.

Note: To find a specific user, type a username into the **Search by user name** box, and then click **FIND**.

15. Click **SAVE**.

    Fortify Software Security Center indicates that the version was successfully created and adds the new application version to the application versions list.
16. Click **CLOSE**.

See Also

"Creating the First Version of a New Application" on page 246

Enabling Auto-Apply and Auto-Predict for an Application Version

If your administrator has configured Audit Assistant, enabled auto-apply system-wide, and mapped the appropriate primary tag fields in the Custom Tags section of the ADMINISTRATION view, you can enable auto-apply for a specific application version.

If you enable auto-apply for an application version, then whenever you use Audit Assistant to request a prediction on your static analysis issues, Fortify Software Security Center applies those predictions to your custom tag values.

When Audit Assistant automatically applies custom tag values to issues, the metadata saved for the issue shows that it was audited by Audit Assistant. A gray gavel displayed next to the custom tag name enables users to see that Audit Assistant predicted the issue.

To enable auto-apply for an application version:

1. From the Fortify dashboard, select the link for the application version for which you want to enable auto-apply.

   The AUDIT page lists the issues associated with the application version.
2. On the page header, click **PROFILE**.
3. Select **AUDIT ASSISTANT OPTIONS**.
4. To have Audit Assistant automatically send unaudited issues to Fortify Scan Analytics for assessment, select the **Enable auto-predict** check box. (For information on auto-prediction, see "About Audit Assistant Auto-Prediction" on

page 92.)

5. Select the **Enable auto-apply** check box.

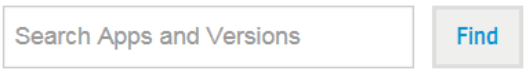
   If your primary tag values are not mapped to Audit Assistant, Fortify Software Security Center displays a warning to that effect and advises you to contact your administrator.
6. Click **APPLY**.
7. Fortify Software Security Center prompts you to confirm that you want to save your settings.
8. Click **OK**.
9. Click **CLOSE**.

See Also

"Configuring Audit Assistant" on page 90

Searching Applications and Application Versions from the Applications View

To search for a specific application or application version from the Applications view:



1. In the **Search Apps and Versions** box above the **Applications** table, type at least part of the application name or version name for the application or version you want to find.
2. Click **Find**.

   The **Applications** table lists all application versions that match your search string.
3. To return to the complete **Applications** table, clear the text in the search box.

See Also

"Searching Globally in Fortify Software Security Center" on page 365

Updating the Application Overview Page

If an application version has pending audit information, its **Overview** page heading displays the "more information" icon .

To recalculate the metrics for the application:

- Click the icon, and then, in the Refresh application metrics dialog, click **Refresh now**.

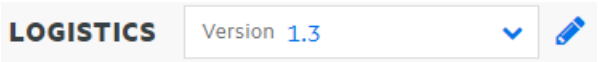
The metrics refresh may take some time, depending on current system activity. After the refresh is complete, the **Overview** page displays the latest data for the application.

Note: Metrics are also refreshed automatically according to the system schedule.

Editing Application Version Details

To edit the details of an application version:

1. On the Fortify header, click **APPLICATIONS**.
2. In the **Applications** table, select the application version to edit.



3. To the right of the application name on the AUDIT page, click the edit icon .
4. In the EDIT VERSION: <*version*> window, click a tab to edit values in any of the fields described in "Adding a New Version to an Application" on page 249.
5. After you make your changes, click **SAVE**.

See Also

"Changing the Template Associated with an Application Version" on page 264

Using Bug Tracking Systems to Help Manage Security Vulnerabilities

Developers fixing software defects often use a bug tracking system to help manage their workload. Security vulnerabilities are a type of bug, and getting vulnerability information into the bug tracking system helps developers take appropriate remediation measures, in line with other development activities. The result is more security awareness and faster remediation of security issues.

From Software Security Center, you can map to any of several bug tracking systems, so that your development team can file bugs into the bug tracking system you already use.

When a developer files a bug, Software Security Center populates bug tickets with the following basic vulnerability information:

- Details that describe the type of issue uncovered
- Remediation guidance, with instructions on the action to take
- A link back to Software Security Center for complete issue details

Topics covered in this section:

Bug Tracker Configuration

To enable a team to access and use a bug tracking system from Fortify Software Security Center, a security lead or development manager must configure Fortify Software Security Center to connect to a bug tracker instance. Either the developer or security lead can then submit bugs to address important security issues.

If you are a security lead or development manager, you can enable team access to your bug tracking system as follows:

1. Edit the application version details.
2. Configure the bug tracker.

See Also

"Velocity Templates for Bug Filing" below

"Managing Bug Tracker Plugins" on page 171

"Authoring Bug Tracker Plugins" on page 423

Velocity Templates for Bug Filing

Text-based fields for filing bugs in Fortify Software Security Center can be associated with Apache Velocity templates that reference issue data. When you submit a bug for one or more issues, the content for the mapped fields is generated using the corresponding template and data from the issues.

Fortify Software Security Center provides pre-defined templates for the summary and description fields of the supported bug tracker plugins that ship with Fortify Software Security Center. You can edit these pre-defined templates or add templates that map other text-based fields that the plugin provides.

This section contains the following topics:

"Adding Velocity Templates to Bug Tracker Plugins" on the next page

"Customizing Velocity Templates for Bug Tracker Plugins" on page 258

"Deleting Velocity Templates" on page 259

Adding Velocity Templates to Bug Tracker Plugins

Fortify Software Security Center provides pre-defined templates for the summary and description fields of the supported bug tracker plugins that ship with Fortify Software Security Center. You can edit these templates or add templates that map other text-based fields that the plugin provides.

Important! Before you add a new template or edit an existing one, make sure that you review the pre-defined templates carefully to understand how to correctly reference variables within the template.

As you create (or edit) a template, keep the following in mind:

- To avoid runtime errors, Fortify strongly recommends that you validate variables in your template before you render them. (See the pre-defined templates for examples of how to use a macro.)
- Use conditionals if you want to render content differently for a single-issue bug (as opposed to a bug that includes multiple issues).

To add a Velocity template to a bug tracker plugin:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Templates**, and then select **Bug Filing**.

   The Bug Filing page lists the template groups for supported bug trackers.
3. In the table, click the row that shows the template group for your bug tracker plugin.

   The row expands to display details for the pre-defined templates mapped to the description and summary fields for the plugin.
4. Click **EDIT**.
5. Click **+ ADD FIELD**.
6. In the **Mapped field** box in the ADD TEMPLATE dialog box, type the name of the field to map, as it appears in the bug tracker plugin dialog box. (Note that you can map only text-based fields.)
7. In the **Template** box, type your Velocity Template Language (VTL) statement for the mapping.

   For information about format the VTL statement, click the **Editing tips** link. To access full instructions on how to write the statement, click the **Velocity User Guide** link. This takes you to the Apache Velocity Project website. To see a list of all available variables, click **SHOW VARIABLES**.)

   Note: Not all variables are available for all issues. In particular, verbose content such as “ATTRIBUTE_COMMENTS,” “ISSUE_DETAIL,” and “ISSUE_RECOMMENDATION” is available only if you are filing a bug for a single issue.

8. Click **APPLY**.
9. To add another template, repeat steps 5 through 8.
10. Click **SAVE**.

On the Bug Filing page, the details for the bug tracking plugin now include your new template.

See Also

"Velocity Templates for Bug Filing" on page 256

"Customizing Velocity Templates for Bug Tracker Plugins" below

"Bug Tracker Configuration" on page 256

"Deleting Velocity Templates" on the next page

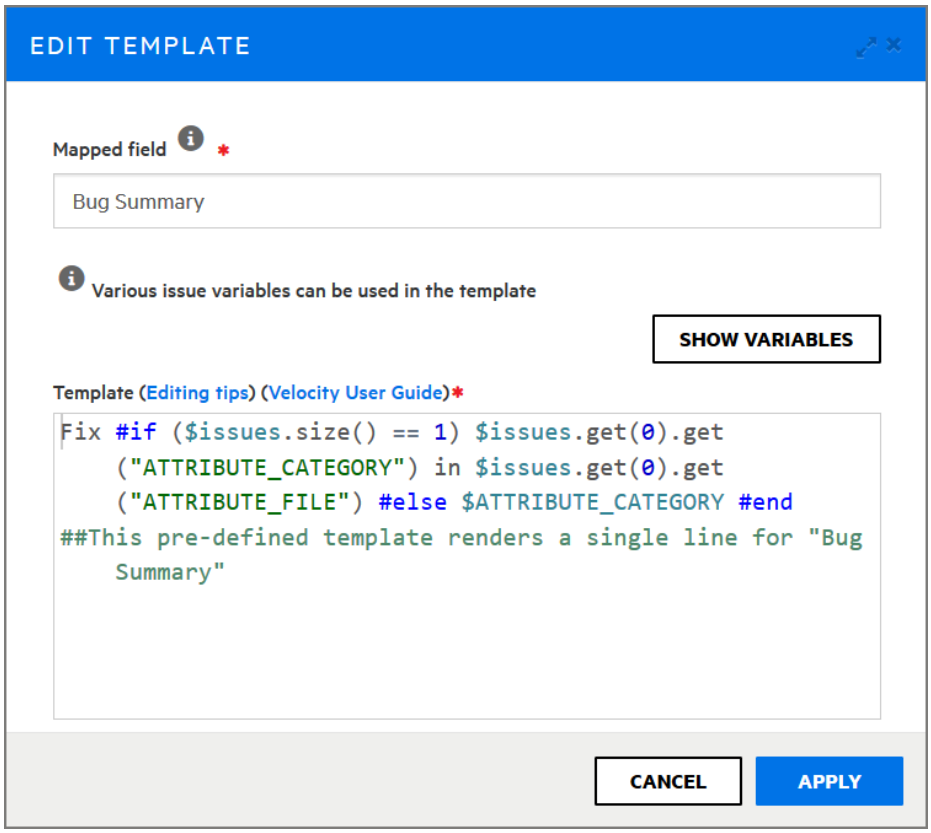
Customizing Velocity Templates for Bug Tracker Plugins

To customize the Velocity template for a bug tracker plugin:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION page, select **Templates**, and then select **Bug Filing Templates**.
3. In the table on the right, click the template group for the bug tracker plugin you use.

   The row expands to display details for the pre-configured Velocity templates that are mapped to the description and summary fields that the plugin provides.
4. Click **EDIT**.

5. To the right of the mapped field you want to modify, click the **Edit field** icon.



6. To see useful tips on how to edit the template, click **Editing tips**. To access detailed instructions on how to modify the template, click the **Velocity User Guide** link. This takes you to the Apache Velocity Project website. To see a list of all available variables, click **SHOW VARIABLES**.
7. Make any necessary changes to the content in the **Mapped field** and **Template** boxes.
8. Click **APPLY**.
9. Click **SAVE**.

The details displayed for the bug tracker plugin now include your changes.

See Also

"Deleting Velocity Templates" below

"Velocity Templates for Bug Filing" on page 256

"Adding Velocity Templates to Bug Tracker Plugins" on page 257

Deleting Velocity Templates

If a bug tracker plugin is not associated with any application versions, you can delete its associated template group.

To delete the templates group associated with a bug tracker plugin:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane of the Bug Filing page, select **Templates**, and then select **Bug Filing**.
3. In the list of template groups , click the name of your bug tracker plugin.

   The row expands to display details for the pre-configured templates mapped to the description and summary fields that the plugin provides.
4. Click **DELETE**.

   Fortify Software Security Center prompts you to confirm that you want to delete the template group.

   Caution! Fortify strongly recommends that you not delete the pre-defined template groups.
5. To continue with the deletion click **OK**.

The Bug Filing page no longer lists the velocity templates for the bug tracker plugin.

See Also

"Velocity Templates for Bug Filing" on page 256

"Adding Velocity Templates to Bug Tracker Plugins" on page 257

"Customizing Velocity Templates for Bug Tracker Plugins" on page 258

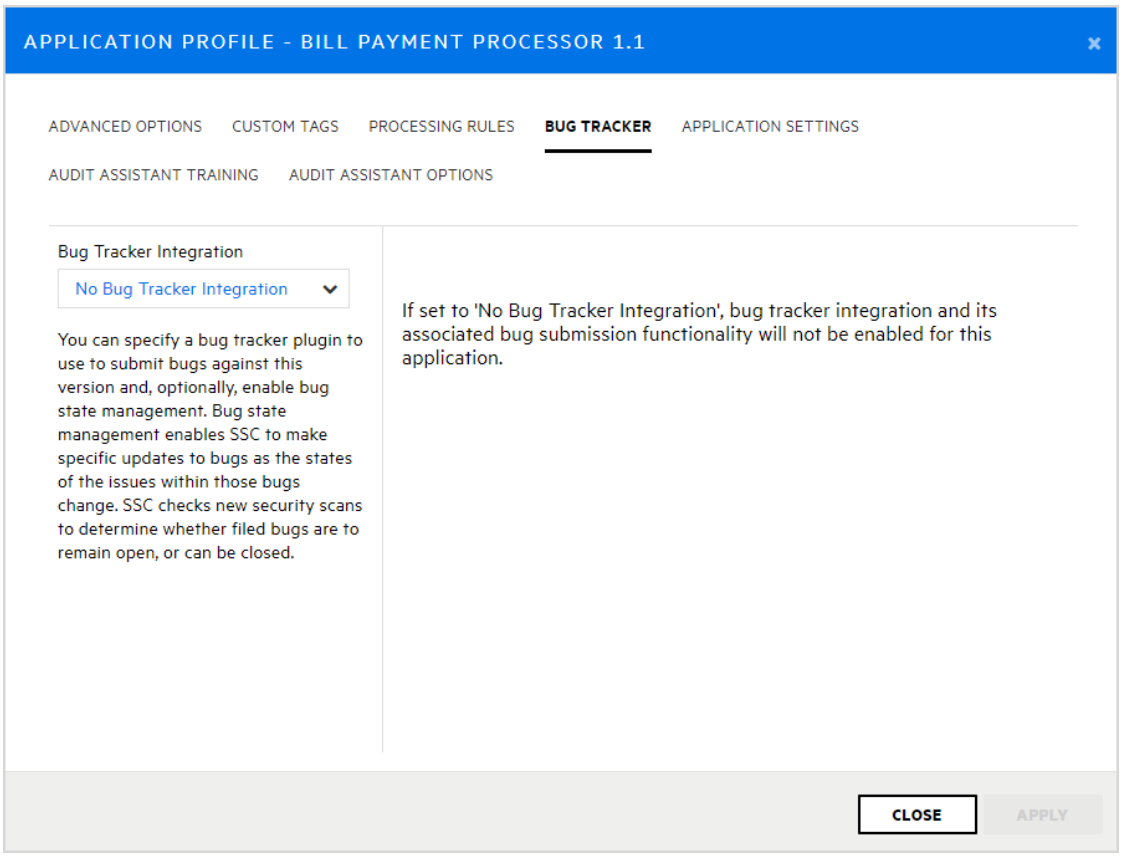
Assigning a Bug Tracking System to an Application Version

Use the following procedure to assign a bug tracking system to an application version. Before you can do this, the bug tracker plugin must already be in the system. For information about how to add a bug tracker to Fortify Software Security Center, see "Managing Bug Tracker Plugins" on page 171.

To integrate with a bug tracking system:

1. On the Fortify header, click **APPLICATIONS**.
2. In the **Applications** table, click the application version to which you want to assign a bug tracker.

   The AUDIT page for the selected application version lists the issues with the version.
3. At the upper right, click **PROFILE**.
4. In the APPLICATION PROFILE - <*Application_Name*><*Application_Version*> dialog box, click the **BUG TRACKER** tab.



5. From the **Bug Tracker Integration** list, select the application to use for tracking bugs for this application version.
6. Complete the required fields, and then click **VALIDATE CONNECTION**.
7. In the TEST BUG TRACKER PLUGIN CONFIGURATION dialog box, type your bug tracker authentication credentials, and then click **TEST**.

   After Fortify Software Security Center verifies your connection to your bug tracker, it displays a message to indicate that the test was successful.
8. Click **OK**.

   You can enable bug state management for the application version. With bug state management enabled, Fortify Software Security Center can update bugs as the states of the issues within those bugs change.
9. (Optional) To enable bug state management, select the **Bug state management** check box.
10. In the **Username** and **Password** boxes, provide the credentials for your bug tracker, and then click **APPLY**.

    The SUCCESS dialog box advises you that bug configuration was successful.
11. Click **OK**.
12. Click **CLOSE**.

See Also

"About Bug Tracker Integration" on page 169

"Managing Bug Tracker Plugins" on page 171

"Submitting a Bug for Multiple Issues" on the next page

"Authoring Bug Tracker Plugins" on page 423

Submitting a Bug for a Single Issue

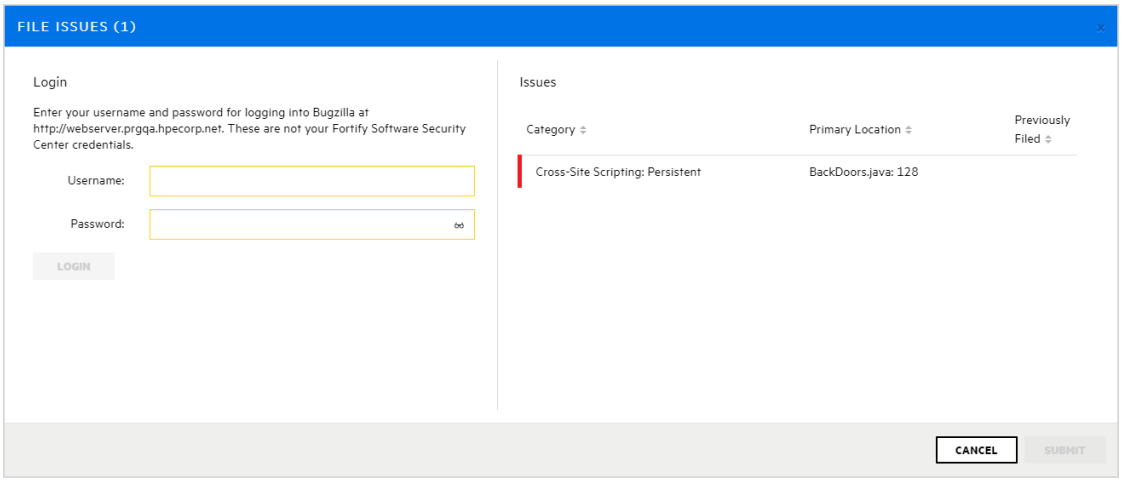
If a bug tracking plugin is specified for an application version (see "Assigning a Bug Tracking System to an Application Version" on page 260), you can use that bug tracker to submit bugs that cover one or multiple issues.

To submit a bug for a single issue:

1. From the AUDIT page for an application version, expand the row for an issue for which you want to submit a bug.
2. Click **FILE BUG**.

   Note: If the **FILE BUG** button is not available, a bug tracker may not have been assigned to the application version. (To address this, see "Managing Bug Tracker Plugins" on page 171 and "Assigning a Bug Tracking System to an Application Version" on page 260.)

   Note too, that if a bug is already submitted for the issue, you cannot submit a new bug against it.



3. In the FILE ISSUES (1) dialog box, under **Login**, provide the username and password for the bug tracker associated with this application version, and then click **LOGIN**.

   Fortify Software Security Center retains your credentials for the duration of your work session so you do not have to provide them to file additional bugs during that session.

   The **Login** section displays the fields for the bug tracker specified for the application version.
4. Provide input for all fields required for the bug tracker, and then click **SUBMIT**.

After a successful submission, a bug icon is displayed for the issue in the **Bug submitted** column of the issues table.

See Also

"Submitting a Bug for Multiple Issues" below

"Viewing Bugs Submitted for Issues" on page 358

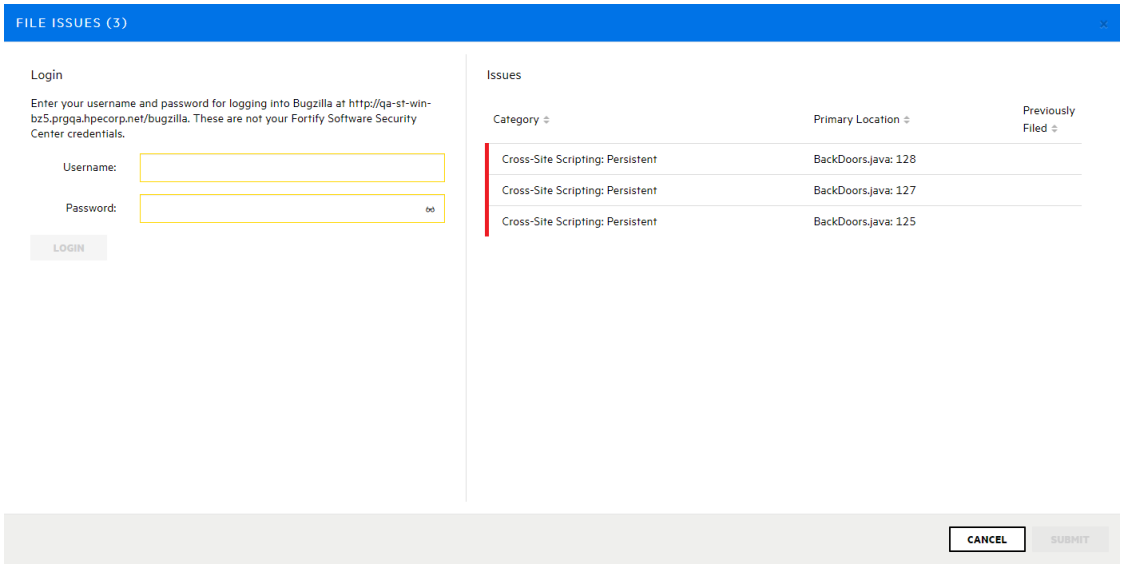
Submitting a Bug for Multiple Issues

If a bug tracking plugin has been specified for an application version (see "Assigning a Bug Tracking System to an Application Version" on page 260), you can submit bugs that cover one or multiple issues. (For information about how to file a bug for just one issue, see "Submitting a Bug for a Single Issue" on the previous page.)

To submit a single bug that covers multiple issues:

1. From the AUDIT page for an application version, select the check boxes for all issues that you want to include in a bug, and then, above the issues table, click the **File Bug** icon .

   Note: If, after you select check boxes, the **File Bug** icon is not visible, you first need to set up a bug tracker for the application version. (See "Assigning a Bug Tracking System to an Application Version" on page 260.)



   Note: If a bug was previously submitted for a selected issue, you cannot submit a new bug against that issue. The FILE ISSUES dialog box displays the message, "Some selected issues have already been filed and will be ignored," and displays a bug icon for the issue in the **Previously Filed** column.

2. In the FILE ISSUES dialog box , under **Login**, provide the username and password for the bug tracker associated with this application version, and then click **LOGIN**.

   Fortify Software Security Center retains your credentials for the duration of your work session so you do not have to provide them to file additional bugs during that session.

   The **Login** section displays the fields for the bug tracker specified for the application version.
3. Provide input for all required fields, and then click **SUBMIT**.

After a successful submission, a bug icon is displayed for the selected issues in the **Bug submitted** column of the issues table.

See Also

"Submitting a Bug for a Single Issue" on page 262

"Viewing Bugs Submitted for Issues" on page 358

Bug State Management

Bug state management enables Fortify Software Security Center to make specific updates to bugs as the states of the issues within those bugs change. Fortify Software Security Center checks new security scans to determine whether filed bugs are to remain open, or can be closed.

If scan results indicate that one of more security issues associated with a previously submitted bug persist (and match the selection criteria), Fortify Software Security Center checks the bug tracking system to ensure that the bug is in a valid open state and, if necessary, reopens the bug.

If all issues associated with a bug are removed (either because the issues were remediated or no longer match the selection criteria), Fortify Software Security Center updates the bug to indicate that stakeholders may resolve or close this ticket. To enable auditing and traceability, Fortify Software Security Center does not automatically resolve or close bugs.

For instructions on how to enable bug state management for an application version, see "Assigning a Bug Tracking System to an Application Version" on page 260.

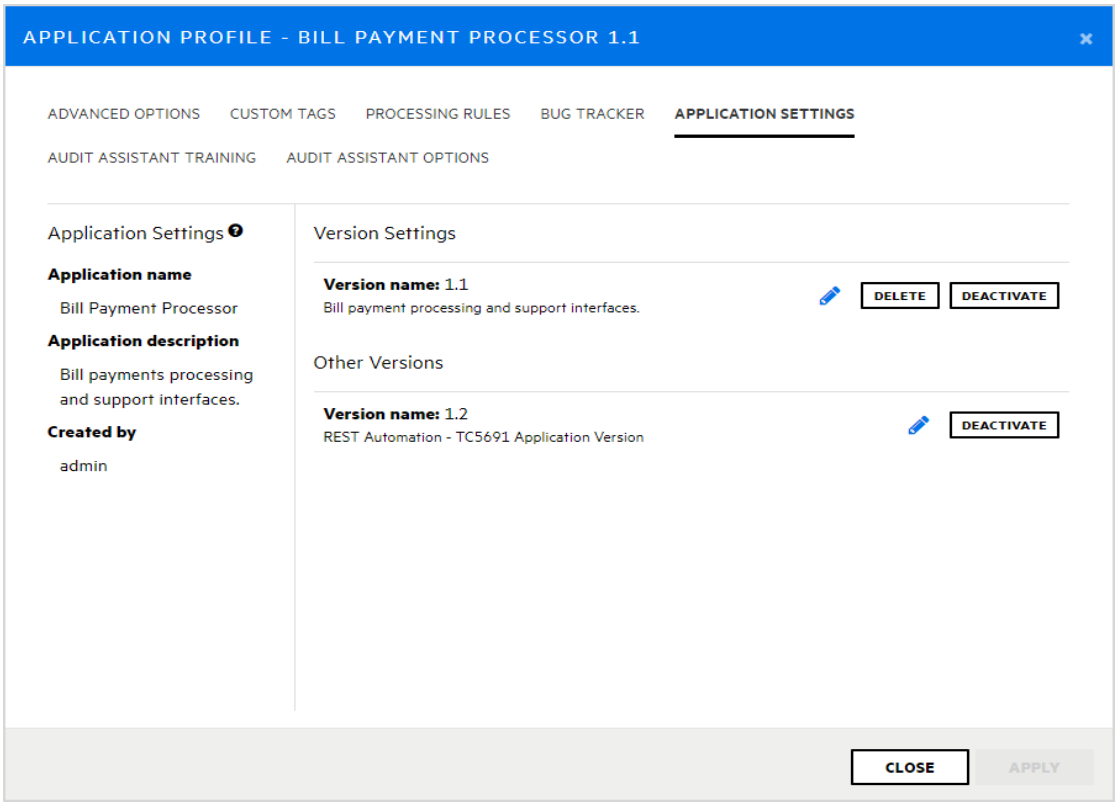
Changing the Template Associated with an Application Version

You can modify many settings for an existing application version, including its issue template. However, keep in mind that assigning a different issue template to an application version or updating an issue template on the server results in loss of synchronization between the database cache and existing audit sessions.

Caution! Fortify recommends that you change the template associated with an application version only if no results have yet been processed for that application version. If you change the issue template for an application version for which results have already been processed, Fortify Software Security Center does not recalculate the issue metrics and metrics generated based on the previously assigned template are unavailable and cannot be deleted.

To change the template associated with an application version:

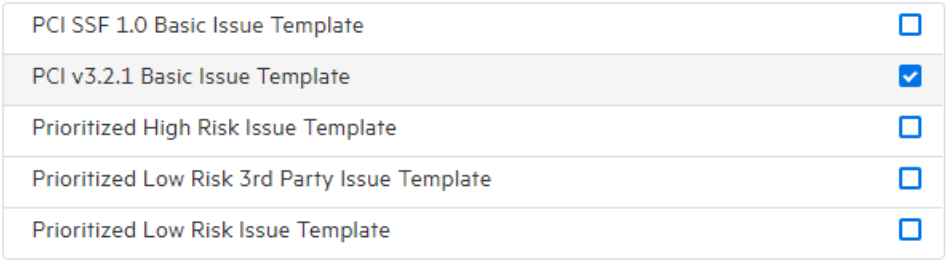
1. Log in to Fortify Software Security Center as either an Administrator or Security Lead.
2. From the Dashboard ISSUE STATS page, click the name of the application version you want to modify.
3. On the application version toolbar of the AUDIT page, click **PROFILE**.
4. In the APPLICATION PROFILE <*application_version*> dialog box, click **APPLICATION SETTINGS**.



5. Under **Version Settings**, click the edit icon .

   Caution! Changing the template can alter the metrics calculated for the application version. Existing metrics will not be recalculated.

6. In the EDIT VERSION dialog box, click the **TEMPLATE** tab.



In the list of templates, the currently assigned template is marked as selected.

7. Select the check box for the template you prefer to use for the application version.
8. Click **SAVE**.

After you change the template, Fortify Software Security Center invalidates any auditing session of the affected application version (for example, by a different user) and displays an error message to advise you that the application version audit session must be restarted.

Note: A Fortify Audit Workbench user auditing the affected application version does not see this information.

Setting Analysis Results Processing Rules for Application Versions

Analysis results processing rules enable management approval and oversight of code scans. You can specify the rules to be followed when analysis results for an application version are processed during scan artifact uploads.

To configure the analysis results processing rules for an application version:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Dashboard, click the link for the application version for which you want to configure the processing rules for analysis results.
2. On the application version toolbar of the AUDIT page, click **PROFILE**.
3. In the APPLICATION PROFILE - <*Application_Version*> dialog box, select the **PROCESSING RULES** tab, and then review the listed processing rules.
4. Select or clear the check boxes for the processing rules you want to apply to the application version. These rules are described in the following table.

Rule	Description
Require approval if the Build Project is different between scans	Fortify Software Security Center compares the Build Project for the

Rule	Description
	scan and the scan that preceded it. If the Build Projects differ, management approval is required before the scan can be uploaded.
Check external metadata file versions in scan against versions on server	If a user attempts to upload an FPR file, Fortify Software Security Center compares the external metadata version for the file with the external metadata version on the Fortify Software Security Center server. If the external metadata version for the FPR file is later (higher) than the external metadata file version on the server, Fortify Software Security Center requires approval for the file upload. If the external metadata version for the FPR file is earlier (lower) than, or the same as, the external metadata file version on the server, then Fortify Software Security Center allows the FPR file upload.
Require approval if file count differs by more than 10%	Fortify Software Security Center compares the file count for the scan and the scan that preceded it. If the count differs by more than ten percent, management approval is required before the scan can be uploaded.
Perform Force Instance ID migration on upload	A newer version of Fortify Static Code Analyzer or of a Rulepack can change an instance ID from one created in a previous scan by an older version of Fortify Static Code Analyzer (or a Rulepack). Both instance IDs identify the same issue. When enabled, this

Rule	Description
	rule migrates old instance IDs to the corresponding new instance IDs, even if the Fortify Static Code Analyzer version (or Rulepack) versions are the same. For detailed information about how this rule works, see "About Processing Rules that Affect Instance ID Migration" on page 271.
Require approval if result has Fortify Java Annotations	Fortify Software Security Center checks the results to determine whether they include Fortify Java annotations. If Fortify Software Security Center finds any of the annotations, management approval is required before the scan can be uploaded.
Require approval if line count differs by more than 10%	Fortify Software Security Center compares the line count for the scan and the scan that preceded it. If the count differs by more than ten percent, management approval is required before the scan can be uploaded.
Automatically perform Instance ID migration on upload	A newer version of Fortify Static Code Analyzer or of a Rulepack can change an instance ID from one that was created in a previous scan by an older version of Fortify Static Code Analyzer or a Rulepack. Both instance IDs identify the same issue. When enabled, this rule automatically migrates old instance IDs to the corresponding new instance IDs to preserve the history of the issues. (It is sometimes useful to disable this

Rule	Description
	rule as a troubleshooting measure for customer support.) For detailed information about how this rule works, see "About Processing Rules that Affect Instance ID Migration" on page 271.
Require approval if the engine version of a scan is newer than the engine version of the previous scan	Fortify Software Security Center checks to determine whether any scan engine (Fortify Static Code Analyzer, Fortify WebInspect, Fortify WebInspect Agent) version is newer than the one already used in the application. If it detects newer versions, it flags the upload for management approval.
Ignore SCA quick scan results and SCA speed dial results performed with a setting of less than four.	Blocks the processing of Fortify Static Code Analyzer scans done in quick can mode, which searches for high-confidence, high-severity issues. This rule also prevents the upload of speed dial analysis results performed at a level of less than four. To enable the uploading speed dial analysis results, clear this check box. **Caution!** After you choose between uploading a full scan or uploading speed dial analysis results, Fortify recommends that future scan results uploaded for the application version be of the same type.
Require approval if the Rulepacks used in the scan do not match the Rulepacks used in the previous scan	Fortify Software Security Center checks to determine whether you have added or removed a

Rule	Description
	Rulepack, and whether a Rulepack version has changed. If it detects that a Rulepack has been added, removed, or updated, it flags the upload for management approval.
Require approval if Fortify SCA or Fortify WebInspect Agent scan does not have valid certification	Fortify Software Security Center checks to see that a Fortify Static Code Analyzer or WebInspect Agent scan has valid certification. If the certification is not valid, then someone may have tampered with the results in the upload. If the certification is missing, it is not possible to detect tampering. If certification is missing or is not valid, the rule requires management approval.
Require approval if result has analysis warnings	Fortify Software Security Center checks to see whether a Fortify Static Code Analyzer or Fortify WebInspect Agent scan contains analysis warnings. If it detects analysis warnings, the rule requires management approval. **Note:** This rule applies only to the first upload of a given results file, and does not apply to subsequent uploads of the file. For example, if audit Information is added to a previously-uploaded FPR file that contains analysis warnings, Fortify Software Security Center does not require management approval when the changed file is again uploaded.

Rule	Description
Warn if audit information includes unknown custom tag	If audit information includes an unknown custom tag, the rule requires management approval.
Require the issue audit permission to upload audited analysis files	If a user attempts to upload audited analysis files, but does not have the permissions required to audit issues (edit custom tag values for issues, add comments to issues, and suppress and unsuppress issues), this rule blocks the upload.
Disallow upload of analysis results if there is one pending approval	If an analysis result still requires approval, this rule blocks its upload.
Disallow approval for processing if an earlier artifact requires approval	If an earlier scan artifact requires approval, and was not approved, this rule blocks the user from approving the current scan artifact. If this processing rule is *not* selected, then when a user approves the current FPR, all previous FPRs are automatically approved.

Fortify Software Security Center prompts you to confirm that you want to save the settings for analysis result processing rules.

5. Click **APPLY**.

About Processing Rules that Affect Instance ID Migration

Two processing rules affect instance ID migration; Perform Force Instance ID migration on upload, and Automatically perform Instance ID migration on upload. It is useful to understand how these are used.

An issue instance ID can mutate for any one of the following reasons:

- The IID-generation algorithm changes with a new Fortify Static Code Analyzer version
- Use of a new Rulepack versions
- Changes to scan settings (For example, using extra rules are specified for a scan.)

- Vulnerable code is duplicated (For example, the same vulnerable code is copied and pasted multiple times in an application version. In this case, Fortify Static Code Analyzer generates a unique instance ID for the first duplicate fragment, and then increments this generated instance ID for all remaining duplicated fragments. So, two separate scans can produce different instance IDs for the same code fragments, depending on the order in which the two scans uncover them.)

The **Automatically perform Instance ID migration on upload** rule addresses issue instance ID mutation that results either from an IID-generation algorithm change with a new Fortify Static Code Analyzer version, or from a change in Rulepack version. For example, Fortify Software Security Center detects that the Fortify Static Code Analyzer version used in the latest scan is newer than the version used for previous scans. With "Automatically perform Instance ID migration on upload" selected, Fortify Software Security Center runs the migration. If Fortify Software Security Center detects no changes in the Fortify Static Code Analyzer version used, it does not run the migration (even if "Automatically perform Instance ID migration on upload" is selected).

The **Perform Force Instance ID migration on upload** rule addresses instance ID mutation that results from changes in scan settings or from vulnerable code duplication. Fortify Software Security Center can easily determine whether the Fortify Static Code Analyzer version or Rulepack version has changed. If Fortify Software Security Center detects such a change, it performs the migration automatically. However, in other cases (duplicate code, scan settings), Fortify Software Security Center cannot make this determination. You can use this processing rule to force Fortify Software Security Center to perform the migration in such cases.

If you suspect that the issue instance ID changed as a result of either changes in scan settings or vulnerable code duplication, Fortify recommends that you select the **Perform Force Instance ID migration on upload** processing rule.

Note: Instance ID migration takes a noticeable amount of time, which is why these two rules exist. Because you may not really want to run IID migration every time, these rules let you determine whether or not to run instance ID migration after each scan upload.

See Also

"Uploading Scan Artifacts" on page 311

"Approving Analysis Results for an Application Version" on page 316

Configuring Audit Assistant Options for an Application Version

To configure Audit Assistant options for an application version:

1. Check to make sure that Fortify Software Security Center has been configured to use Audit Assistant with your applications. (See "Configuring Audit Assistant" on page 90.)
2. From the Dashboard, select the application version for which you want to configure Audit Assistant options.
3. On the AUDIT page, click **PROFILE**.

   The APPLICATION PROFILE - <*application_name*> <*application_version*> window opens to the **ADVANCED OPTIONS** section.
4. Click **AUDIT ASSISTANT OPTIONS**.
5. From the **Application version prediction policy** list, select the prediction policy that you want Audit Assistant to apply to this application version.

   Note: You can specify an application version prediction policy only if the **Enable specific application version policies** option is enabled system-wide. (See "Configuring Audit Assistant" on page 90.) Otherwise, Audit Assistant uses the default prediction policy.

   If you choose not to specify a prediction policy for the application version, Audit Assistant uses the default prediction policy.
6. To have Audit Assistant automatically send unaudited issues for this application version to the Fortify Scan Analytics server for assessment, select the **Enable auto-prediction** check box.

   Note: The **Enable auto-prediction** and **Enable auto-apply** check boxes are available only if those audit settings are enabled system-wide. (See "Configuring Audit Assistant" on page 90.)
7. To have Audit Assistant automatically assign predicted values from the Scan Analytics server to the mapped custom tag values, select the **Enable auto-apply** check box.
8. Click **APPLY**.

See Also

"Configuring Audit Assistant" on page 90

Custom Tags

To audit code in Fortify Software Security Center, the security team examines analysis results and assigns values to “tags” that are associated with application

issues. The development team can then use these tag values to determine which issues to address and in what order.

Fortify Software Security Center provides a single default tag named “Analysis” to enable application auditing out of the box. Valid values for the Analysis tag are Exploitable, Not an Issue, Suspicious, Reliability Issue, and Bad Practice. You can modify the Analysis tag attributes, revise the tag values, or add new tag values based on your auditing needs.

To refine your auditing process, you can define your own custom tags. Like the Analysis tag, your custom tag definitions are stored in an issue template that you can associate with an application version. For example, you could create a custom tag used track the sign-off process for an issue. After a developer audits the issues to which he or she is assigned, a security expert can review those issues and mark each as “approved” or “not approved.”

Note: Fortify Audit Workbench users can add custom tags to their projects as they audit them. However, if these custom tags are not defined in Fortify Software Security Center for the issue template associated with the corresponding application version, then the new custom tags are lost after the Audit Workbench user uploads an FPR file to Fortify Software Security Center.

Topics covered in this section:

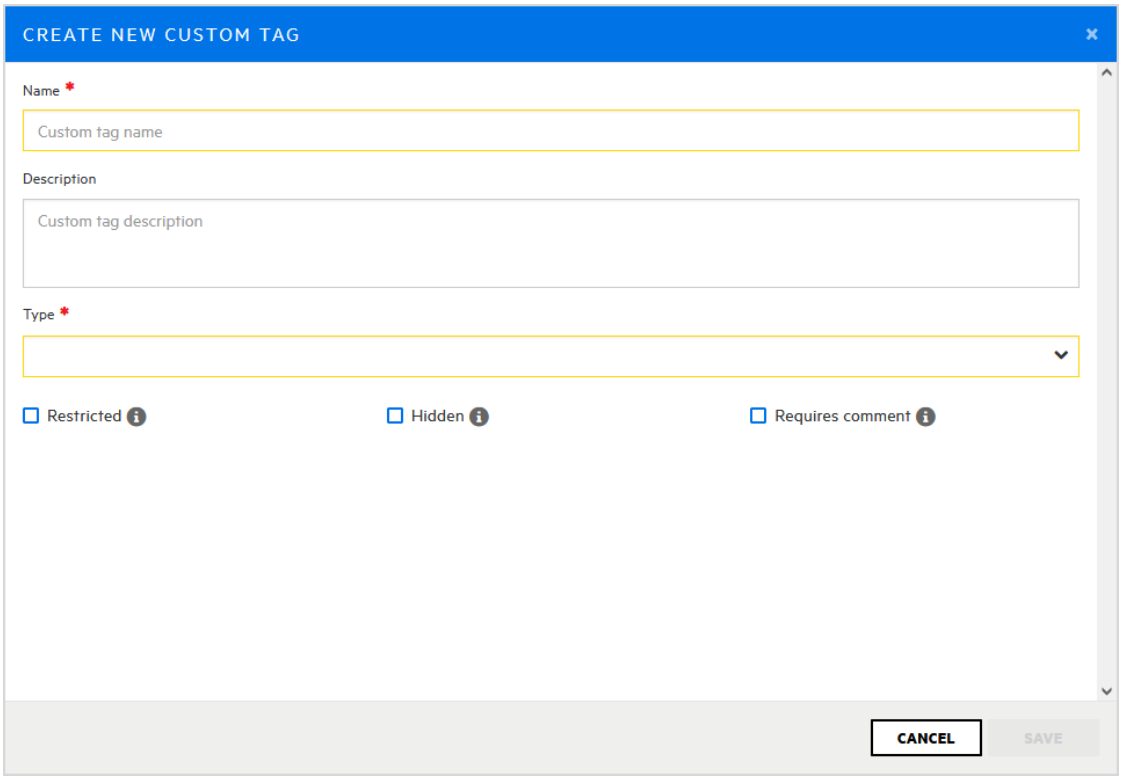
Adding Custom Tags to the System

If you are a Fortify Software Security Center administrator, you can add custom tags to the system. The following topics describe how to add each of the supported custom tag types to Fortify Software Security Center.

Note: You can filter issues based on the values for custom tags you create and assign to an application version. For information, see "Filtering Issues for Display on the OVERVIEW and AUDIT Pages" on page 332.

To add a custom tag:

1. On the Fortify header, click **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, select **Templates**, and then select **Custom Tags**.
3. On the Custom Tags page header, click **NEW**.



4. In the CREATE NEW CUSTOM TAG dialog box, type a name for the new tag in the **Name** box.

   Important! Make sure that the name you specify for a custom tag *is not* a database reserved word.

5. (Optional) In the **Description** box, type content that describes how to use the custom tag.
6. From the **Type** list, select one of the tag types listed in the following table.

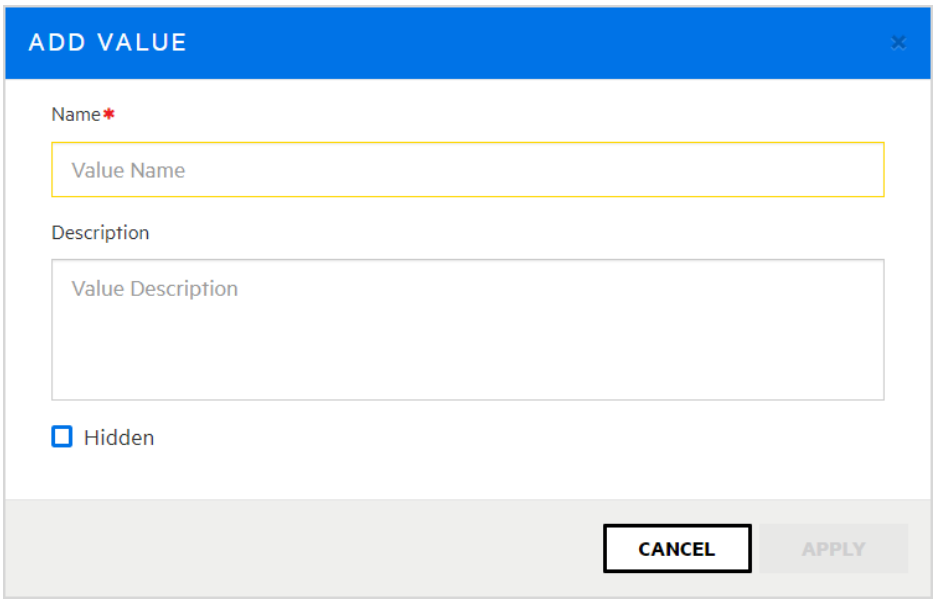
Type	Values Accepted
Date	Calendar date in the format specified in the

Type	Values Accepted
	PREFERENCES dialog box (see "Setting Preferences: System-Wide and Across Application Versions" on page 212).
Decimal	Number with a precision of up to 18 (up to 9 decimal places)
List	Selection from the list of values that you specify for the tag
Text	String with up to 500 characters (HTML/XML tags and newlines are not allowed)

7. (Optional) Select any or all of the following optional tag features:
   - To allow only users with specific permission (managers, security leads, administrators) to modify the tag, select the **Restricted** check box.
   - (List-type only) A list-type custom tag can be *extensible*, which means that auditors can add values to it as they audit issues. To enable users to add new values to the list tag during audits, select the **Extensible** check box.
   - To prevent the display of the tag in the ASSIGN dialog box or in Audit Workbench, select the **Hidden** check box.
   - To require users to leave a comment whenever the value of this custom tag changes, select the **Requires comment** check box. If a custom tag that requires a comment is changed, the system automatically adds a comment to indicate the changes made to the tag.

     Note: If the new custom tag that requires a comment is a date-type tag, the date users select for the tag while auditing is always in the format specified in the PREFERENCES dialog box.
8. If your new custom tag is a date-, decimal-, or text-type tag, click **SAVE**. If your new custom tag is a list-type tag, continue to the next step.

9. (Required) To specify a value for the new tag:
   a. Click **+ ADD**.

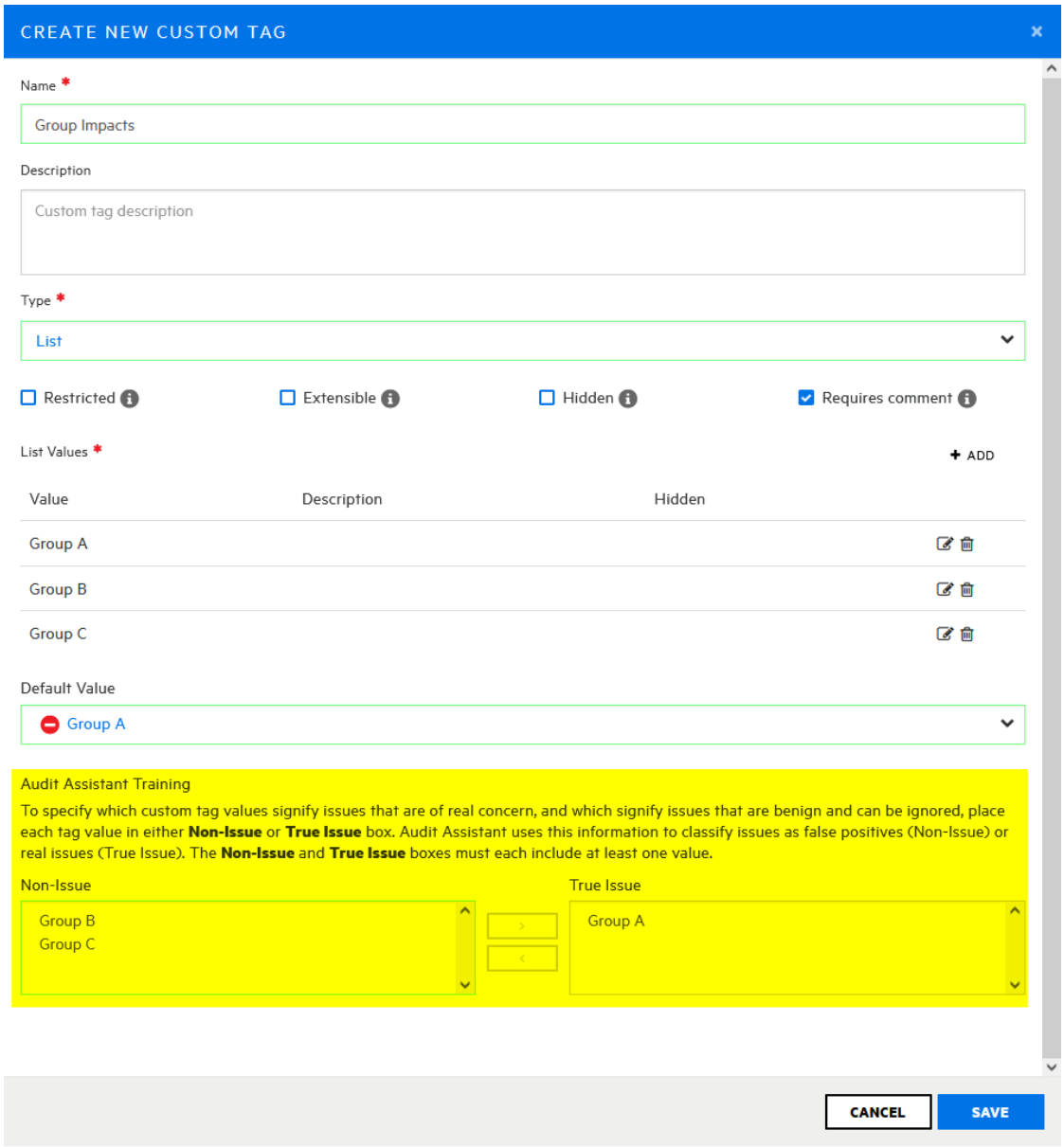


   b. In the ADD VALUE dialog box, type a value in the **Name** box.

      A value can be a discrete attribute for the issue that this tag addresses. For example, you might specify that this custom tag addresses a due date or server quality issue.
   c. (Optional) In the **Description** box, type a description of what the value represents.
   d. To prevent the tag from being displayed in the Assign dialog box and in Audit Workbench, select the **Hidden** check box.
   e. Click **APPLY**.
   f. Repeat these steps (a through f) until you have defined all of the values you need for the new custom tag.
10. (Optional) From the **Default Value** list, select the default value for this tag. (If the custom tag has a default value, then issues with no value set for the tag acquire that default value. If no default value is defined, then the tag value is empty.)

    Note: You can designate a list-type tag as the *primary tag* for auditing an application version after you assign it to an application version. For instructions on how to assign a tag to an application version, see "Assigning Custom Tags to Application Versions" on page 284.
11. If Fortify Software Security Center is integrated with Audit Assistant, it is important that you provide Audit Assistant with information that it can use to distinguish list tag values that signify true issues from those that signify non issues (true positives versus false positives). You do this in the **Audit Assistant**

Training section of the CREATE NEW CUSTOM TAG dialog box, where the **Non-Issue** list initially contains all values you added for the new tag.



12. (For a Fortify Software Security Center instance integrated with Audit Assistant only) From the **Non-Issue** list, select at least one tag value which, if selected, indicates a true vulnerability (use the **Ctrl** and **Shift** keys to select multiple values) and use the right-pointing arrow to move the selection to the **True Issue** list.

    Important! The **Non-Issue** list and the **True Issue** list must each contain at least one value.

13. Click **SAVE**.

Note: To use a new custom tag to audit application version issues, you must first assign the tag to the application version. For instructions, see "Assigning Custom Tags to Application Versions" on page 284.

See Also

"Mapping Audit Assistant Analysis Tag Values to Fortify Software Security Center Custom Tag Values" on page 93

"Globally Hiding Custom Tags" below

"Deleting Custom Tags" on the next page

"Custom Tags" on page 273

"Editing Custom Tags" on page 282

"Associating Custom Tags with Issue Templates" on page 283

"Managing Custom Tags Through Issue Templates" on page 286

"Managing Custom Tags Through an Issue Template in an FPR File" on page 287

Modifying Custom Tag Attributes

To modify the attributes of a custom tag:

1. From the left pane of the ADMINISTRATION page, click **Templates**, and then click **Custom Tags**.
2. On the **Custom Tags** page, click the row that displays the tag you want to modify.

   The row expands to reveal the details.
3. Click **EDIT**.
4. Modify the tag attributes, and then save your changes.

   Caution! Make sure that the name you specify for a custom tag *is not* a database reserved word.

See Also

"Adding Custom Tag Values" on the next page

"Adding Custom Tags to the System" on page 274

Globally Hiding Custom Tags

To globally hide a custom tag:

1. From the left pane in the ADMINISTRATION view, click **Templates**, and then select **Custom Tags**.

The Custom Tags page lists all existing custom tags.

2. Click the row for the tag you want to hide.
   The row expands to display the details for the tag.
3. Click **EDIT**.
4. Select the **Hidden** check box.
5. Click **SAVE**.

The custom tag no longer appears on the AUDIT page or in Fortify Audit Workbench.

Deleting Custom Tags

If you are an Administrator or a Security Lead, you can delete custom tags.

Note: You cannot delete a custom tag if:

- It is set as the primary tag.
- It has been used in auditing issues.
- It is currently associated with an application version or issue template. For information on how to remove a custom tag from an application version, see "" on page 286. For information on how to remove a custom tag from an issue template, see "Removing Custom Tags from Issue Templates" on page 283.

You can never delete the Analysis tag.

To delete custom tags:

1. From the left pane in the **ADMINISTRATION** page, select **Templates**, and then select **Custom Tags**.
   The Custom Tags page opens. Existing custom tags are listed on the right.
2. Select the check boxes for the custom tags you want to delete.
3. In the Custom Tags toolbar, click **DELETE**.
4. When prompted to confirm that you want to delete the tag (or tags), click **OK**.

See Also

"Custom Tags" on page 273

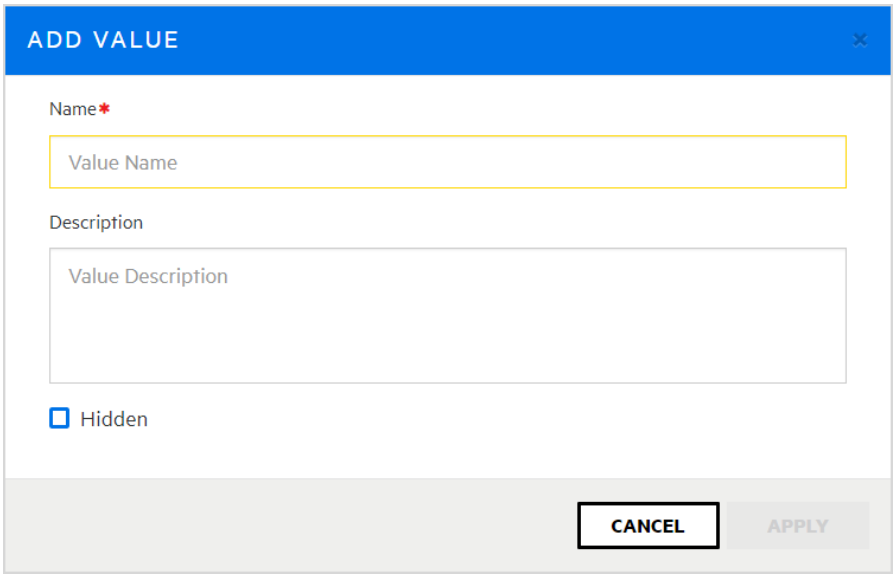
Adding Custom Tag Values

If you are a Fortify Software Security Center administrator, you can add values to the list-type custom tags in the system.

Note: If a custom tag is assigned the extensible attribute, then you can add values to it as you audit issues.

To add a value to a list-type custom tag:

1. On the Fortify header, click **ADMINISTRATION**.
2. In the left pane, click **Templates**, and then click **Custom Tags**.
   The Custom Tags page lists the custom tags in the system.
3. Click the row for the tag to which you want to add a value.
   The row expands to display the details for the tag.
4. Below the table of values, click **EDIT**.
5. Above the table of values, click **+ ADD**.



6. In the ADD VALUE dialog box, type a name and, optionally, a description for the new value.
   If Fortify Software Security Center is configured to use Audit Assistant and if auto-apply is enabled, you must map an Audit Assistant tag to the new tag value.
7. To map an Audit Assistant tag to the new tag value, under **AA Custom Tags**, select the check box for the Audit Assistant tag that corresponds to your new tag value. (If necessary, you can change the mapping later.)
8. To prevent the tag from being displayed in the Assign dialog box or in Audit Workbench, select the **Hidden** check box.
9. Click **APPLY**.
10. On the Custom Tags page, under **Audit Assistant Training**, the new value is listed in the **Non-Issue** list. If it is not a real issue, leave it as is. If the value does, in fact, apply to real issues, then select it and move it to the **True Issue** list.

    Note: Both the **Non-Issue** list and the **True Issue** list must each contain at least one value.

11. Click **SAVE**.

See Also

"Editing Custom Tags" below

"Deleting Custom Tag Values" below

"Adding Custom Tags to the System" on page 274

"Assigning Custom Tags to Application Versions" on page 284

Editing Custom Tags

If you are an Administrator-level user, you can modify custom tags in the system.

To edit a custom tag:

1. From the left pane in the ADMINISTRATION view, click **Templates**, and then select **Custom Tags**.
   The Custom Tags page lists all custom tags in the system.
2. Click the row for the tag you want to edit to expand it and display the details.
3. Below the table of values, click **EDIT**.
4. Edit the values for any of the displayed fields, and then click **SAVE**.
   For information about the displayed fields, see "Adding Custom Tags to the System" on page 274.

See Also

"Deleting Custom Tag Values" below

"Assigning Custom Tags to Application Versions" on page 284

Deleting Custom Tag Values

If you are an administrator or a security lead, you can delete custom tag values.

To delete a value for a custom tag:

Note: You cannot delete a custom tag value that is currently associated with an application version, issue template, or if an issue is audited using the value.

1. From the left pane in the ADMINISTRATION view, select **Templates**, and then select **Custom Tags**.
   The Custom Tags page lists all custom tags in the system.
2. Click the row for the tag from which you want to delete a value.
   The row expands to display the details for the tag.
3. Below the table of values, click **EDIT**.
4. In the table of values, click the **Remove value** icon in the row for the value

you want to delete.

5. Click **SAVE**.

See Also

"Editing Custom Tags" on the previous page

"Adding Custom Tags to the System" on page 274

"Adding Custom Tag Values" on page 280

Associating Custom Tags with Issue Templates

After you first create an issue template and upload an issue template file, the custom tags defined in that issue template file are the custom tags that are initially associated with the issue template. Updates to existing custom tags are ignored because tags are designed to be updated using the procedures described in previous sections, but newly-defined custom tags in that issue template file are added to the system and associated with the issue template.

Note: The custom tags associated with an issue template are the default tag set assigned to an application version when it is first created using that issue template.

To associate a custom tag with an issue template:

1. On the Fortify header, click **ADMINISTRATION**.
2. In the left pane, select **Templates**, and then select **Issue**.
3. Click the row that displays the issue template that you want to associate with the custom tag.

   The row expands to reveal the template details.
4. Click **EDIT**.
5. In the **CUSTOM TAGS** section, click **+ ADD CUSTOM TAG**.
6. In the ADD CUSTOM TAG dialog box, select the check box for the custom tag to associate with the issue template, and then click **+ADD**.

   The **CUSTOM TAGS** table now lists the tag you added.
7. Click **SAVE**.

See Also

"Disassociating a Custom Tag from an Application Version" on page 286

Removing Custom Tags from Issue Templates

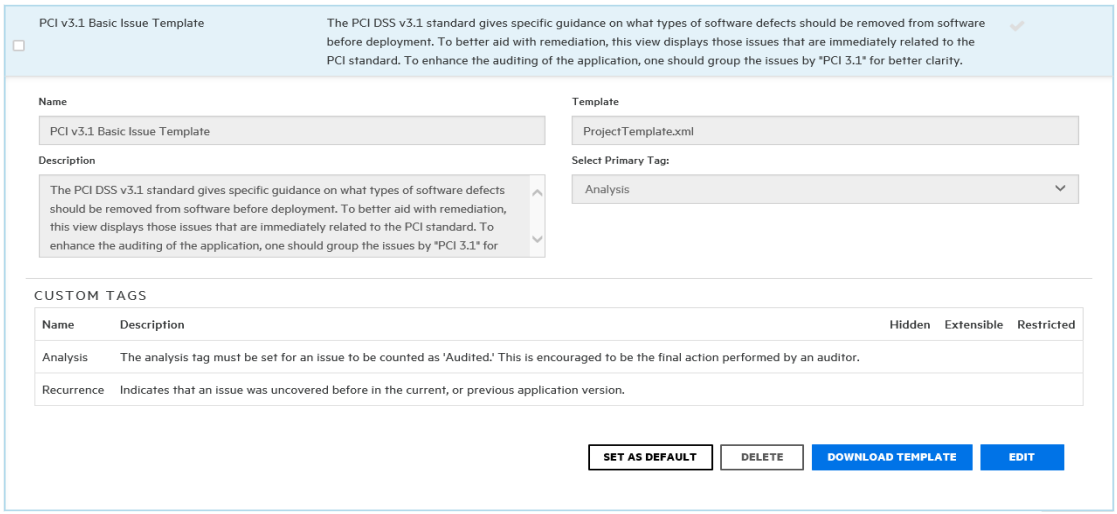
To remove a custom tag from an issue template:

1. From the left pane in the ADMINISTRATION page, select **Templates**, and then select **Issue**.

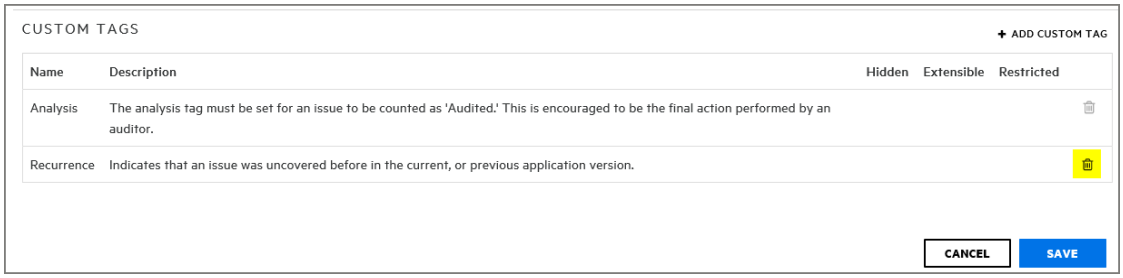
The table on the right lists all of the issue templates in the system.

2. Click the row that displays the issue template associated with the custom tag you want to remove.

   The row expands to reveal the issue template details. The **CUSTOM TAGS** section lists the custom tags currently associated with the template.



3. At the bottom of the expanded row, click **EDIT**.



4. In the last column, click the remove icon for the custom tag that you want to remove from the template.

   Note: You cannot remove the designated primary tag from an issue template.

5. Click **SAVE**.

See Also

"Custom Tags" on page 273

Assigning Custom Tags to Application Versions

To use a new custom tag to audit application version issues, you must first assign the tag to the application version.

To assign a custom tag to an application version:

1. From the Applications view, expand the row for the application, and then select the name of the version you plan to audit.
2. On the application version toolbar of the AUDIT page, click **PROFILE**.
3. In the APPLICATION PROFILE dialog box, select the **CUSTOM TAGS** tab.
4. Click **ASSIGN/ REMOVE**.

   The **CUSTOM TAGS** tab lists all of the tags available for auditing issues.
5. Select the check box for the custom tag you want to assign to the application version (you can select multiple tags), and then click **DONE**.

   The selected tag is now listed as an assigned tag.

   To successfully complete the audit of an issue in Fortify Software Security Center, you must specify a value for the custom tag that is designated as the *primary tag*. By default, the Analysis tag is the primary tag.

   During an audit, the primary tag is listed first. If list-type custom tags other than Analysis exist in your Fortify Software Security Center instance and are assigned to the application version, you can select one of these (instead of Analysis) as the primary tag.
6. (Optional) To assign a tag other than the current primary tag as primary:

   Note: You can only assign list-type custom tags as primary tags.

   a. Click **SELECT PRIMARY**.
   b. From the **Select Primary Tag** list in the SELECT PRIMARY TAG dialog box, select the tag to set as the primary custom tag.

      Note: If you use Audit Assistant, and you have not provided Audit Assistant guidance information, make sure that you edit the tag to include that information. For information about how to provide Audit Assistant guidance, see "Adding Custom Tags to the System" on page 274. For information about how to edit a custom tag, see "Editing Custom Tags" on page 282.

   c. Click **DONE**.
7. Click **CLOSE**.

The assigned custom tag will be available the next time a team member audits issues for the application version.

See Also

"Disassociating a Custom Tag from an Application Version" on the next page

Disassociating a Custom Tag from an Application Version

You can disassociate a custom tag from an application version if it has not been used in auditing that application version.

To disassociate a custom tag from an application version:

1. On the Fortify header, click **APPLICATIONS**.
2. Click the application version name to which the custom tag is assigned.
3. On the application version toolbar of the AUDIT page, click **PROFILE**.
4. In the APPLICATION PROFILE window, select the **CUSTOM TAGS** tab.
5. Click **ASSIGN/REMOVE**.

   The **CUSTOM TAGS** tab lists all custom tags in the system. The check boxes for tags associated with the application version are selected.
6. Clear the check box for the custom tag that you want to remove, and then click **DONE**.
7. Click **CLOSE**.

The **AUDIT** tab in the issue details on the AUDIT page for this application version no longer lists the custom tag.

After you remove the custom tag from all application versions and issue templates to which it has been assigned, you can delete the tag.

See Also

"Removing Custom Tags from Issue Templates" on page 283

"Adding Custom Tags to the System" on page 274

"Assigning Custom Tags to Application Versions" on page 284

Managing Custom Tags Through Issue Templates

Custom tags defined in an issue template file are assigned to that specific issue template. You cannot update existing custom tags through direct issue template upload. If Fortify Software Security Center detects an updated custom tag, it displays a warning and prompts you to confirm that you want to continue.

You must update existing custom tags through the custom tag administration section of Fortify Software Security Center, as follows:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION page, select **Templates**, and then select **Custom Tags**.
3. Complete the update.

You can add a new custom tag through an issue template upload. This could, for example, allow a member of a security team who is not part of a software audit to define the issue template and the custom tags in the issue template.

Managing Custom Tags Through an Issue Template in an FPR File

FPR files typically contain an issue template. If an FPR file uploaded to Fortify Software Security Center contains an issue template with a custom tag that has been set as editable, you can add a value to the tag.

About Deleting Application Versions

You cannot directly delete an application in Fortify Software Security Center. Fortify Software Security Center removes an application automatically after all of its versions are deleted.

If you are assigned the Administrator role in Fortify Software Security Center, you can delete any application version. If you are in the Security Lead or Manager role, then you can delete any application version to which you are assigned.

If you would rather not delete a version, but prefer instead to remove it from display on the DASHBOARD and Applications pages, you can *deactivate* it. For instructions on how to deactivate an application version, see "Deactivating Application Versions" below.

See Also

"Deleting an Application Version " on page 289

Deactivating Application Versions

Deactivating an application version hides that version in the Applications view. Note that deleting all versions of an application deletes the application altogether.

To deactivate an application version:

1. From the Applications view, expand the row for the application and then select the version you want to deactivate.
2. On the AUDIT page for the selected version, click **PROFILE**.
3. In the APPLICATION PROFILE dialog box, click **APPLICATION SETTINGS**.
4. In the **Version Settings** pane, click **DEACTIVATE**.

   Fortify Software Security Center prompts you to confirm that you want to deactivate the version.
5. Click **OK**.

   The **DEACTIVATE** button is now the **ACTIVATE** button. If you need to, you can re-activate the version later.
6. Close the APPLICATION PROFILE dialog box.

See Also

"Reactivating Application Versions" below

"Deleting an Application Version " on the next page

Reactivating Application Versions

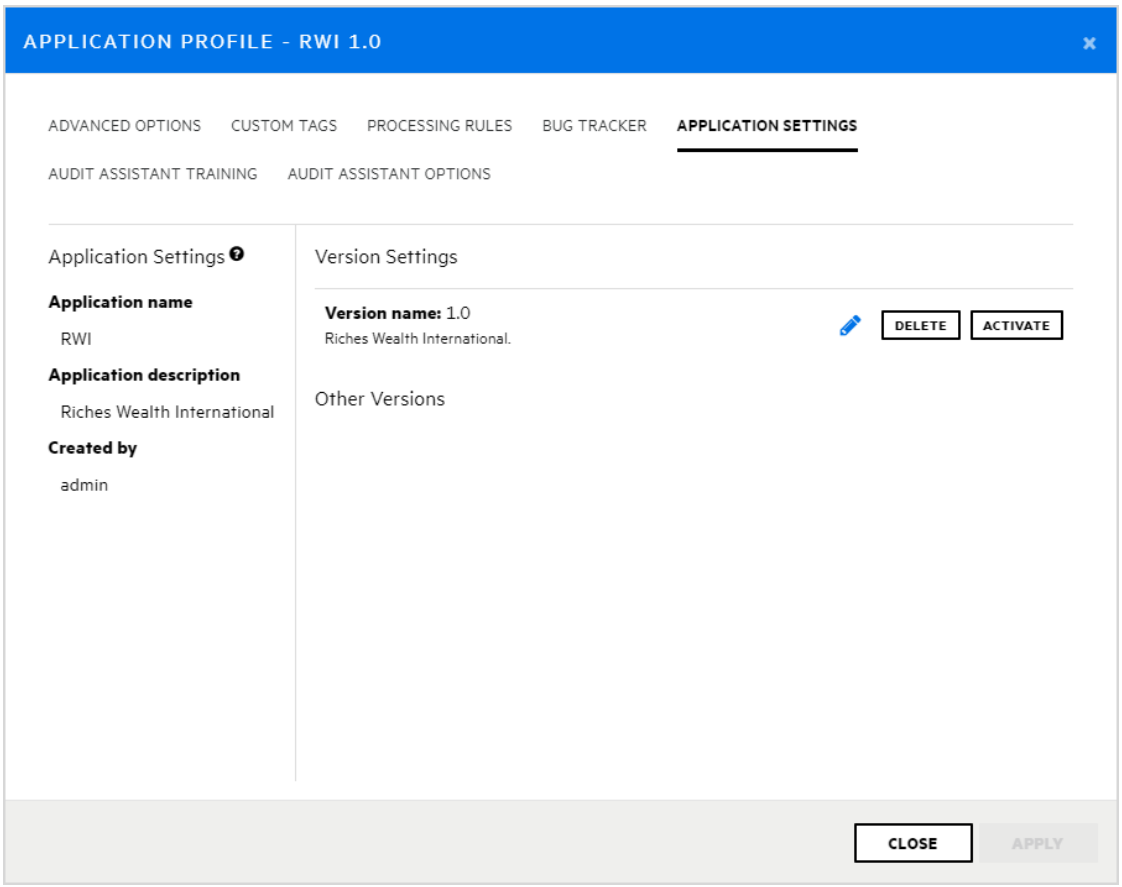
If a specific application version has been deactivated and is not listed on the DASHBOARD or in the Applications view, you can reactivate it to make it visible again.

If the deactivated application version was the only version of the application that exists, you can do the following to access and reactivate it:

- Create a new version of the deactivated application, and then follow the procedure described below.

To reactivate an application version when another version of the application exists:

1. On the Fortify header, click **APPLICATIONS**.
2. In the Applications view, select the **Show inactive versions** check box.
3. In the table, click the deactivated application version number.
4. On the application version toolbar of the AUDIT page, click **PROFILE**.
5. In the APPLICATION PROFILE - *<application_version>* dialog box, select the **APPLICATION SETTINGS** tab.



6. Click **ACTIVATE**.
   Fortify Software Security Center prompts you to confirm the activation.
7. Click **OK**.
8. Click **CLOSE**.

The application version is again displayed on the Fortify Software Security Center Dashboard and in the Applications view.

Deleting an Application Version

If you would rather not delete an application version, but prefer instead to remove it from display on the Fortify Software Security Center Dashboard and in the Applications view, see "Deactivating Application Versions" on page 287

Important! If you delete all versions of an application, Fortify Software Security Center automatically deletes the application.

To delete a Fortify Software Security Center application version:

1. From the Applications view, select the name of the application version you want to delete.

Fortify Software Security Center opens the OVERVIEW page for the selected version.

2. On the application version toolbar, click **PROFILE**.
3. In the APPLICATION PROFILE dialog box, click **APPLICATION SETTINGS**.
4. In the **Version Settings** pane, click **DELETE**.

   Fortify Software Security Center prompts you to confirm that you want to delete the version.
5. Click **OK**.

Fortify Software Security Center removes the version from the database.

Chapter 12: About Webhooks

You can create webhooks to update external systems about events that occur in Fortify Software Security Center.

Topics covered in this section:

Webhooks Permissions

The following table shows which Fortify Software Security Center roles have permission to perform which webhook-related tasks.

Roles	Permissions
Administrator	User can create, view, and manage webhooks to monitor any kind of event.
Security Lead	• User can view webhooks. Application versions that webhooks monitor will be filtered to include only those for which the user has explicit view permission. • User can create and manage webhooks monitoring events only on entities for which the user has explicit view permission. A Security Lead cannot create or manage the following: • Webhooks with the **Send me everything!** option selected • Webhooks with the **Monitor All Application Versions** option selected • Webhooks set to monitor any events that require universal access

To see all of the actions each Fortify Software Security Center role can perform:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Users**, and then select **Roles**.

   The **Roles** table lists all of the roles to which you can assign users.
3. To see all of the actions a user in a given role can perform, click the row for the role.

Creating Webhooks

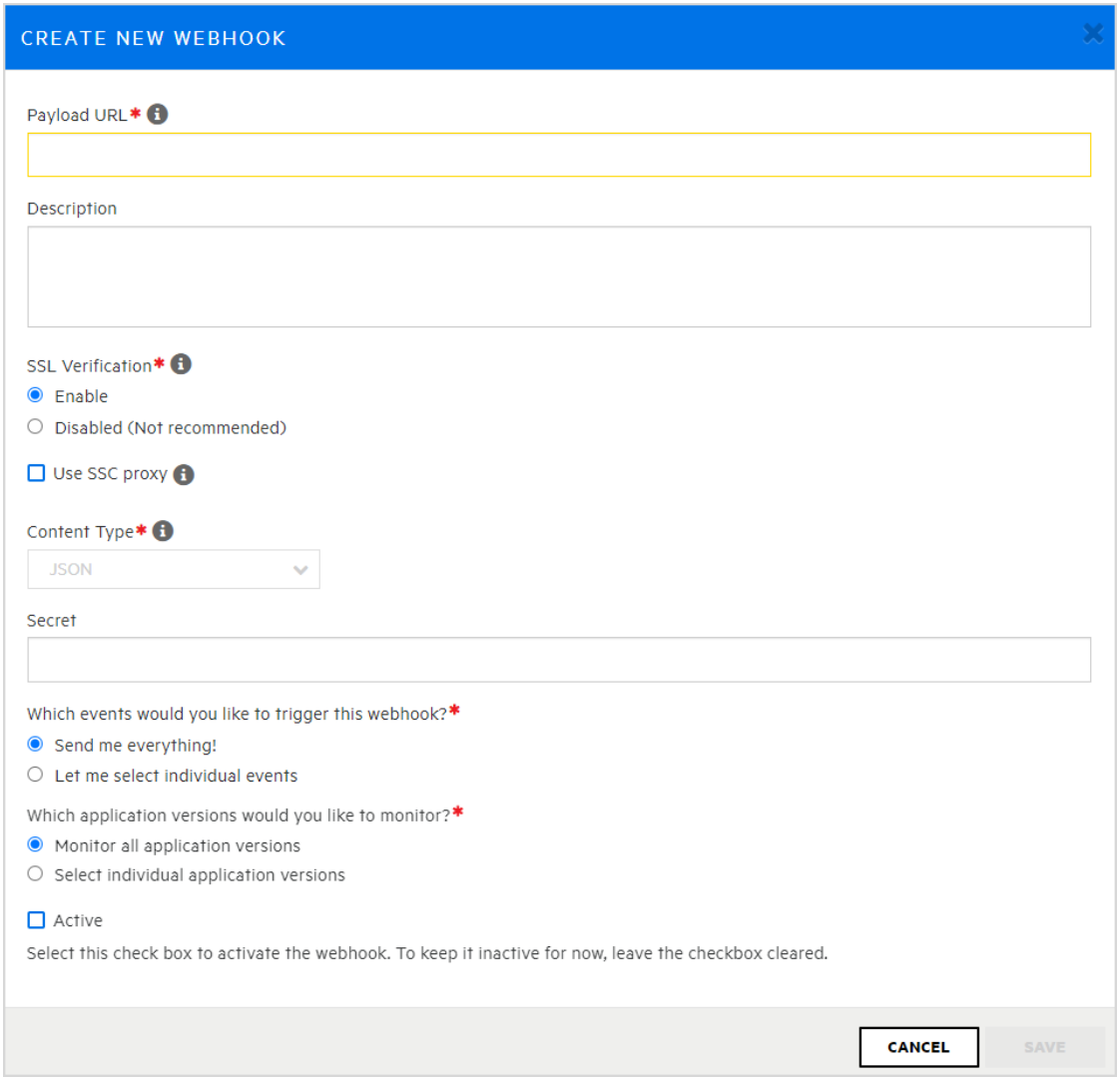
If you are an Administrator, you can create webhooks to monitor any kind of event, whether global or application version-specific. If you are a Security Lead, you can create webhooks that monitor events on the entities that you have permission to view.

Note: For information on which roles have which permissions to work with webhooks, see "Webhooks Permissions" on the previous page.

To create a new webhook:

1. Log in to Fortify Software Security Center as an Administrator or Security Lead, and then, on the Fortify header, click **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION page, select **Configuration**, and then select **Webhooks**.

   The Webhooks page lists any webhooks already configured.
3. On the Webhooks page, click **NEW**.



4. In the CREATE NEW WEBHOOK dialog box, provide the information described in the following table.

Field	Description
Payload URL	In this box, specify the URL to which you want the requested payload sent.
Description	(Optional) Provide a description of the webhook and its payload.
SSL Verification	Specify whether SSL certificate verification is required to invoke the webhook based on the specified URL.

Field	Description
Use SSC proxy	(Optional) If you have set up a proxy for Fortify Software Security Center integrations, you can select this check box to use it for webhooks. For information about how to configure a proxy for Fortify Software Security Center integrations, see "Configuring a Proxy for Fortify Software Security Center Integrations" on page 132.
Content Type	Displays the format used for the payload to be delivered. **Note:** For this release, JSON is the only content type supported.
Secret	(Optional) Enter a webhook secret to be used to verify the data integrity and authenticity of POST requests. The secret is used to calculate a hash-based message authentication code (HMAC), which is communicated to the payload destination via the "X-SSC-Signature" header. The code is calculated using the HMAC-SHA256 algorithm. The secret is used as a key and the payload body (with HTTP "Date" header value appended) is used as a message. The HMAC value is then encoded as a hexadecimal number with the prefix `sha256=`.
Which events would you like to trigger this webhook?	Do one of the following: • To have the following events included in the payload, select **Send me everything!** (This applies to all current and future events.) • To include a focused subset of events in the payload, select **Let me select individual events**, and then, in the **Global Events** and **Application version events** lists, (described below) select the check boxes for the events to include in the payload.
Global events (system-wide)	

Field	Description
USER_CREATED: A new local user, local group, or LDAP entity was added to Fortify Software Security Center. **USER_DELETED**: A local user, local group, or LDAP entity was deleted from Fortify Software Security Center. **USER_UPDATED**: A local user, local group, or LDAP entity was updated. **LOCAL_USER_ACCOUNT_LOCKED:** A local user was locked out of Fortify Software Security Center as a result of too many login attempts with invalid credentials. **APP_VERSION_CREATED:** A new application version was created in SSC. **APP_VERSION_DELETED:** An application version was deleted from Fortify Software Security Center. **REPORT_GENERATION_COMPLETE**: A new requested report is available for viewing and download. **REPORT_GENERATION_REQUESTED:** A new report was requested. **Application Version Events (application version-specific)** **ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS:** An uploaded artifact was successfully processed to Fortify Software Security Center, and its data are available. **ANALYSIS_RESULT_UPLOAD_FAILURE:** An uploaded artifact was not successfully processed. **ANALYSIS_RESULT_UPLOAD_REQUIRES_APPROVAL:** An uploaded scan artifact requires approval before it can be processed. **ANALYSIS_RESULT_INDEXING_COMPLETED:** Indexing of data for global searches after Fortify Software Security Center finished processing an uploaded FPR was completed. **ANALYSIS_RESULT_UPLOAD_APPROVE:** An artifact was approved for uploading. **APP_VERSION_UPDATED:** An application version was updated from the APPLICATION PROFILE dialog box.	
Application version events **ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS:** Analysis results were successfully uploaded. **ANALYSIS_RESULT_UPLOAD_FAILURE:** An analysis results upload	

Field	Description
failed. **ANALYSIS_RESULT_UPLOAD_REQUIRES_APPROVAL:** An analysis upload requires approval. **ANALYSIS_RESULT_INDEXING_COMPLETED:** Indexing of an analysis result was completed. **ANALYSIS_RESULT_UPLOAD_APPROVED:** Analysis upload results were approved. **APP_VERSION_UPDATED:** An application version was updated.	
Which application versions would you like to monitor?	Do one of the following: • To monitor all application versions (existing application versions and application versions to be created in the future), select the **Monitor All Application Versions** option. • To monitor just a subset of application versions: i. Select the **Select Individual Application Versions** option. ii. Click **ADD**. iii. In the SELECT APPLICATION VERSION dialog box, from the **APPLICATION** list, select an application to monitor. iv. To select all versions, select the **Select All** check box. Otherwise select the check boxes for the versions. v. Click **DONE**. vi. To add another application version or versions, repeat these steps.
Active	Select this check box to make the webhook active. To leave the webhook inactive for now, leave the check box cleared.

5. After you finish configuring the webhook, click **SAVE**.

See Also

"Viewing Webhook Payloads" on the next page

"Deleting Webhooks" on page 301

Editing Webhooks

To edit a webhook:

1. Log in to Fortify Software Security Center as an Administrator or Security Lead, and then, on the Fortify header, click **ADMINISTRATION**.

   Note: If you are a Security Lead, you can only edit webhooks that monitor the entities for which you have explicit view permission.

2. In the left pane of the ADMINISTRATION page, select **Configuration**, and then select **Webhooks**.

   The Webhooks page lists any webhooks already configured.
3. Select the row to see the details for the webhook you want to edit.
4. Change any values for the fields described in "Creating Webhooks" on page 292.
5. (Optional) To request redelivery of a payload after you finish making changes, under **Recent deliveries**, select the row for the payload you want redelivered, and then click **REDELIVER**.
6. Click **SAVE**.

See Also

"Viewing Webhook Payloads" below

"Creating Webhooks" on page 292

Viewing Webhook Payloads

If you are an Administrator, you can view all webhook payloads. If you are a Security Lead, you can view only webhook payloads for application versions that you have explicit permission to view.

To view webhook payloads:

1. Log in to Fortify Software Security Center as an Administrator or Security Lead, and then, on the Fortify header, click **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION page, select **Configuration**, and then select **Webhooks**.

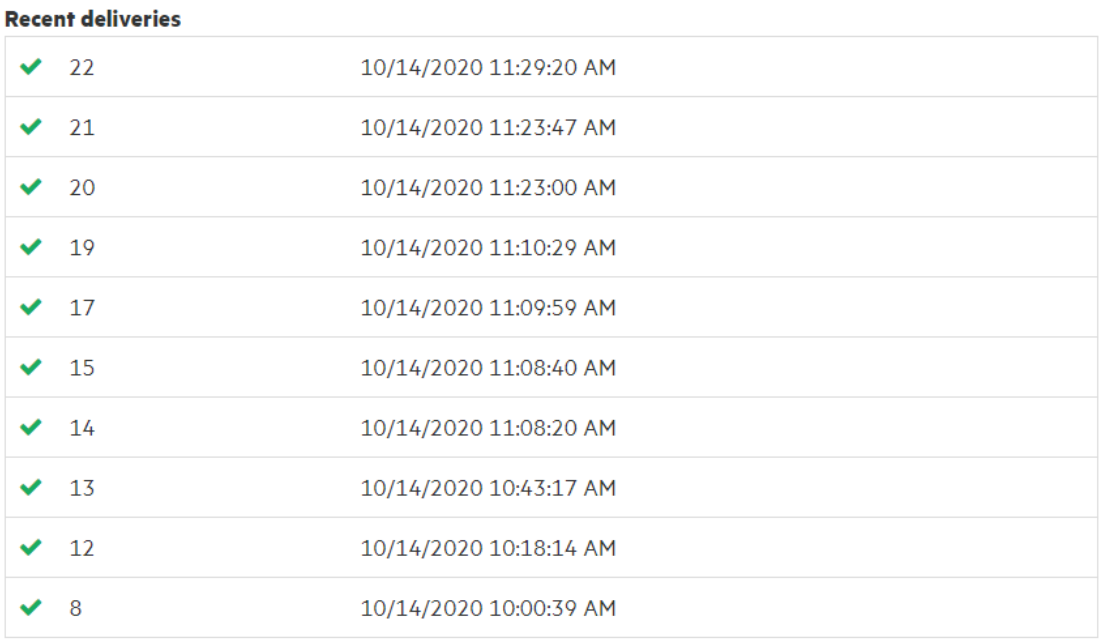
   The Webhooks table lists all existing webhooks and displays the status of each, as follows:

   ✓ A green check mark indicates that the last payload request was successful.

   ✕ A red x indicates that the webhook is active but could not deliver the last payload requested.

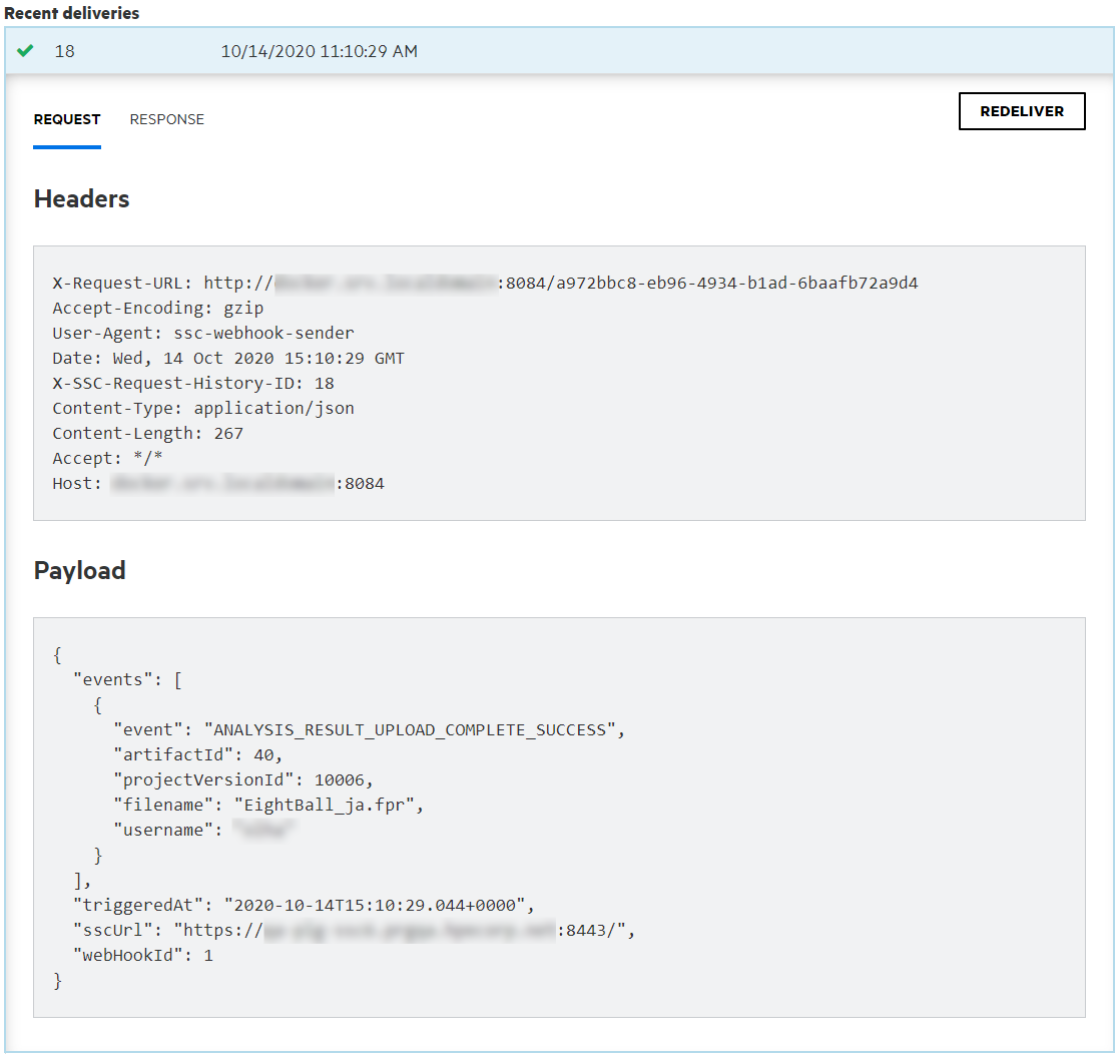
Note: If the **Status** field for a listed webhook displays no icon, in the Webhooks table, expand its row and check to make sure that the **Active** check box, located above the **Recent deliveries** table, is selected.

3. In the Webhooks table, select a webhook to expand its details and examine its recently-delivered payloads (up to ten), if any.

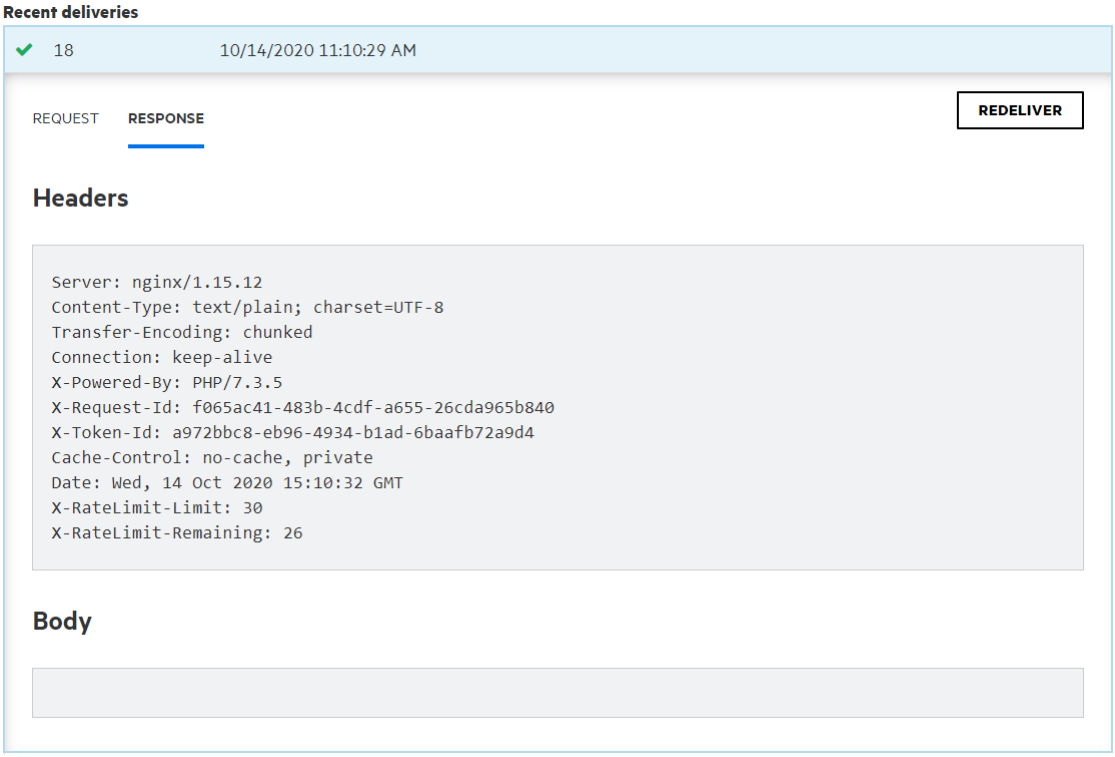


The **Recent deliveries** section lists the payloads (up to ten) most recently delivered.

4. Click the row for the payload you want to examine.



5. To see body or header details for the response, select the **RESPONSE** tab.



For details about the content of delivered payloads, see "Webhook Payloads" on page 438.

See Also

"Deleting Webhooks" on the next page

"Creating Webhooks" on page 292

"Editing Webhooks" on page 297

Redelivering Webhook Payloads

If changes are made that affect the payload delivered to the payload URL for a webhook. you can request that the payload be redelivered.

To request redelivery of a webhook payload:

1. Log in to Fortify Software Security Center as an Administrator or Security Lead, and then, on the Fortify header, click **ADMINISTRATION**.

   Note: If you are a Security Lead, you can only edit webhooks that monitor the entities for which you have explicit view permission.

2. In the left pane of the ADMINISTRATION page, select **Configuration**, and then select **Webhooks**.

   The Webhooks page lists any webhooks configured.

3. Select the row for the webhook for which you want a payload redelivered.
4. Under **Recent deliveries**, select the row for the payload you want redelivered, and then click **REDELIVER**.

See Also

"Creating Webhooks" on page 292

"Editing Webhooks" on page 297

"Viewing Webhook Payloads" on page 297

Deleting Webhooks

To delete a webhook:

1. Log in to Fortify Software Security Center as an Administrator or Security Lead, and then, on the Fortify header, click **ADMINISTRATION**.
2. In the left pane, select **Configuration**, and then select **Webhooks**.

   The Webhooks page lists all existing webhooks and their current status.
3. In the table, select the check box for the webhook you want to delete, and then click **DELETE**.

See Also

"Creating Webhooks" on page 292

"Editing Webhooks" on page 297

Chapter 13: Variables, Performance Indicators, and Alerts

Fortify Software Security Center lets you store measured values and event conditions for application versions as variables. A Fortify Software Security Center variable is a definition of a metric that is to be evaluated periodically for each application version. Variables count issues, conditions, and other categories of numeric data.

Performance indicators combine variables into metrics that are normalized across application version boundaries, and that can represent complex higher-level abstractions such as monetary costs. Fortify Software Security Center variables and performance indicators provide the building blocks that you can use to create customized metrics, which you can then incorporate into customized alert definitions.

You can use the values of variables to trigger alerts, which Fortify Software Security Center then displays on the dashboards of users specified as recipients in alert definitions. Fortify Software Security Center can also email alert notifications to members of an application version team.

Topics covered in this section:

Working with Variables

If you are a Security Lead or an Administrator, you can define variables for your applications. The following topics provide information about Fortify Software Security Center variable syntax and search strings, and include instructions on how to create variables.

Creating Variables

To create a Fortify Software Security Center variable:

1. Log in as a Security Lead or an Administrator, and then click **ADMINISTRATION**.

   Note: Users who have Developer accounts cannot create Fortify Software Security Center variables.

2. In the pane on the left, under **Metrics & Tracking**, select **Variables**.
3. In the Variables toolbar, click **NEW**.
4. In the CREATE NEW VARIABLE dialog box, provide the information described in the following table.

Field	Description
Name	Type a variable name that begins with a letter (a-z, A-Z), and that contains only letters, numerals (0-9), and the underscore character (_).
Description	(Optional) Type a description so that other users can understand how to use the variable.
Search String	Type a valid Fortify Software Security Center variable search string. (For information about how to construct search strings, select the **Syntax Guide** link below the **Search String** box, or see "Variable Syntax" below.)
Folder	From this list, select a folder from the default filter set to associate with the variable. The **Folder** list displays the unique folder names associated with all available issue templates. The variable value is calculated if the folder name is associated with the issue template for the application version.

5. After Fortify Software Security Center validates the variable, click **SAVE**.

The **Variables** table now lists your new variable.

Variable Syntax

The Fortify Software Security Center variable format is `modifier:searchstring`.

Example: `[Fortify Priority Order]:critical audited:false`

To search for an exact match of the string, enclose the string in quotation marks (""). To search for a string without qualifications, type the string without quotation marks.

The following table lists the Fortify Software Security Center relational operators.

Relational Operator	Description	Example
Number range	A comma-separated pair of numbers used to specify the beginning and end of a range of numbers. Use a left or right bracket (“[ ]”) to specify that the range includes the adjoining number. Use a begin or end parenthesis (“( )”) to specify that the range excludes (is greater than or less than) the adjoining number.	`(2,4]` Indicates a range of greater than two, and less than or equal to four
`!` (not equal)	Negate a modifier with an exclamation character (`!`).	`file:!Main.java` Returns all issues that are not in `Main.java`.

Performance Indicators

Fortify Software Security Center performance indicators enable you to combine variables into metrics that are normalized across application version boundaries, and that can represent complex, high-level abstractions such as monetary costs. This section provides information about performance indicator syntax and instructions on how to create performance indicators.

The general format for a Fortify Software Security Center performance indicator formula is as follows:

```
Variable[operator]Variable
```

where `operator` is a standard mathematical operator (`+`, `-`, `*`, `/`).

For instructions on how to create performance indicators, see "Creating Performance Indicators" on the next page.

Creating Performance Indicators

To create a Fortify Software Security Center performance indicator:

1. Log in to Fortify Software Security Center as a Security Lead, and then click the **ADMINISTRATION** tab.

   Note: Users who are assigned the Manager or Developer role cannot create Fortify Software Security Center performance indicators.

2. In the pane on the left, under **Metrics & Tracking**, select **Performance Indicators**.

   The table to the right lists existing performance indicators.
3. Click **NEW**.
4. In the CREATE NEW PERFORMANCE INDICATOR dialog box, provide the information described in the following table.

Field	Description
Name	Type a performance indicator name.
Description	(Optional) Type a description of this performance indicator.
Equation	Type a valid Fortify Software Security Center performance indicator equation. The format for a performance indicator formula is as follows: `Variable[operator]Variable` where operator is a standard mathematical operator (`+`, `-`, `*`, `/`).
Return Type	From this list, select the value type to return.

5. After you configure and successfully validate the new performance indicator, click **SAVE**.

The **Performance Indicators** table lists your new indicator.

Alert Definitions

Alert definitions can include variables or performance indicators to determine when Fortify Software Security Center is to generate an alert notification in the **Todo List** pane of the Dashboard.

Note: This functionality is available only if a Fortify Software Security Center administrator has enabled email notifications.

You can configure alert notifications to send email messages about one or more alert notifications to users assigned to a given application version.

Next

"Creating Alerts" below

See Also

"Configuring Email Alert Notification Settings" on page 102

"Enabling and Disabling Receipt of Email Alerts" on page 104

"Deleting Alerts" on page 309

Creating Alerts

You can define alerts for any application versions to which you have been granted access.

To create a Fortify Software Security Center alert:

1. On the Fortify header, click **ADMINISTRATION**.
2. In the pane on the left, click **Templates**, and then select **Alerts**.
   The Alerts page displays any alerts defined to date.
3. In the Alerts toolbar, click **NEW**.
4. In the CREATE NEW ALERT dialog box, in the **Name** box, type a name for the alert.
5. (Optional) In the **Description** box, type text that describes what the alert is for.
6. To create the alert without enabling it, clear the **Enable Alert** check box. To enable this alert, leave the check box selected.
7. Next to **Type**, select the type of alert you want to create.

   Note: Only administrators can create *scheduled* alerts.

8. Next to **Recipients**, do one of the following:
   - To have the alert sent only to you, leave the **Me only** option selected.
   - To have the alert sent to users assigned to application version assignees, select the **Version assignees** option.
   - (For scheduled alerts only) To have the alert sent to all Fortify Software Security Center users, select **All system users**.

   Note: Regardless of the option you select, you will receive the notification.

9. Provide the information for the alert type you selected, as shown in one of the following tables.

Performance indicator
a. From the **Alert when** list, select a performance indicator. b. From the list of operators, select an operator. c. Type a numeric value. The type of performance indicator selected determines whether the value represents an integer or a percentage. By default, performance indicator alerts are triggered just once, when the performance indicator value meets the criterion set for **Alert when**. For example, an alert with the trigger criterion set to Critical Exposure Issues < 50 is triggered only once, even if many new critical issues are uncovered in subsequent scans. d. To have Fortify Software Security Center reset your alert after each new artifact upload, select the **Reset after triggering** check box.
Variable
a. From the **Alert when** list, select a variable. b. From the list of operators, select the appropriate operator. c. Type a numeric value. The type of variable you selected determines whether the value represents an integer or a percentage. By default, variable alerts are triggered just once, when the variable value meets the criterion set for **Alert when**. For example, an alert with the trigger criterion set to NEWIssues = 0 is triggered only once, even if new issues are uncovered in subsequent scans. d. To have Fortify Software Security Center reset your alert after each new artifact upload, select the **Reset after triggering** check box.
System event
• From the **Alert when** list, select the Fortify Software Security Center system event to trigger the alert.
Scheduled alert (Administrators only)
Under **Alert when**, do the following: a. Use the calendar control to specify the date on which Fortify Software Security Center is to send the alert.

b. In the two boxes to the right, type the hour and minute (hh:mm) at which to send the alert.
c. Toggle between **AM** and **PM** to determine whether the alert is sent in the morning or afternoon.
d. From the list of countries and regions, select the country or region to which your time and date settings apply.
e. From the time zone list, select the time zone to which your time and date settings apply.

10. If you are creating a performance indicator alert or variable alert, do the following to specify the application versions for which you want to use the alert:
    a. Click **ADD**.
    b. In the SELECT APPLICATION VERSION dialog box, from the **APPLICATION** list, select an application for which you want to use the alert.

       The **VERSIONS** pane (center) lists the active versions of the selected application.
    c. To include inactive versions of the application in the **VERSIONS** list, select the **Show inactive** check box.
    d. To use the alert for all application versions, select the **Select all** check box. Otherwise, in the **VERSIONS** list, select the check boxes for the versions for which you want to use the alert.

       The pane on the right lists the application versions you selected to receive the new alert.
    e. To select versions of another application, repeat steps b through d.
    f. Click **DONE**.
11. In the **Message** box, type a message to tell recipients why they have received the alert.

    Note: If you are creating a scheduled alert, *message text is required*.
12. Click **SAVE**.

    If you selected **Version assignees** as recipients, Fortify Software Security Center displays the following alert:

    "Are you sure you want to notify all application versions users? This could potentially notify a large amount of users every time the alert triggers."
13. To proceed, click **OK**. Otherwise, click **CANCEL**, and then select **Me Only** as the recipient.

Fortify Software Security Center displays the details for your new alert.

See Also

"Deleting Alerts" on the next page

"Configuring Email Alert Notification Settings" on page 102

"Enabling and Disabling Receipt of Email Alerts" on page 104

"Alert Definitions" on page 305

Editing Alerts

To edit a Fortify Software Security Center alert:

1. Log in to Fortify Software Security Center as an Administrator, and then, on the Fortify header, click **ADMINISTRATION**.
2. In the pane on the left, click **Templates**, and then select **Alerts**.
   The Alerts page displays all alerts you have defined.
3. In the **Alerts** table, locate and select the row for the alert you want to edit.
   The row expands to reveal the alert settings.
4. At the bottom right of the alert settings, click **EDIT**.
5. Make the necessary changes and then click **SAVE**.

Deleting Alerts

To delete a Fortify Software Security Center alert:

1. Log in to Fortify Software Security Center as an Administrator, and then click the **ADMINISTRATION** tab.
2. In the pane on the left, select **Templates**, and then select **Alerts**.
   The Alerts page displays all alerts you have defined.
3. In the **Alerts** table, select the check box to the left of the alerts you want to delete.
4. In the **Alerts** toolbar, click **DELETE**.
   Fortify Software Security Center prompts you to confirm that you want to proceed with the deletion.
5. Click **OK**.

See Also

"Configuring Email Alert Notification Settings" on page 102

"Alert Definitions" on page 305

"Creating Alerts" on page 306

Viewing and Marking Alerts

Fortify Software Security Center flags any unread alerts that either you or another user has set up for you to receive. These flags are visible in the collapsible pane on

the right of the Dashboard, and on the right end of the Fortify header in every view.

To view your unread alerts, do one of the following:

- At the right end of the Fortify header, click the red circle that shows the number of unread alerts.
- On the Dashboard, in the **Todo List** section of the collapsible pane, click the red circle that shows the number of unread alerts.

The ALERTS window opens and lists any unread alerts.

To mark an alert as having been read:

- In the ALERTS window, select the check box to the left of the alert name, and then click **MARK AS READ**.

To mark an alert as unread:

- In the ALERTS window, select the check box to the left of the alert name, and then click **MARK AS UNREAD**.

To view alerts that you have already read:

- From the **View** list, select **Read**.

To view unread alerts:

- From the **View** list, select **Unread**.

To view all of your alerts (read and unread):

- From the **View** list, select **All**.

If you have marked all of your alerts as read, the read alert flag is no longer displayed. To see these alerts, go to the Dashboard and, in the **Todo List** section of the collapsible pane, click **Show all alert notifications**.

Chapter 14: About Working with Scan Artifacts

The following sections describe all of the various aspects of working with scan artifacts.

Uploading Scan Artifacts

The following procedure describes how to upload your scan artifacts to the Fortify Software Security Center database. For information about how to submit training metadata to Fortify Audit Assistant, see "Submitting Training Data to Audit Assistant" on page 363.

Note: As it inserts data into the database, Fortify Software Security Center truncates HTTP responses that contain more than 100,000 characters. Such responses are either cut off at the end, or contain `\n\n...\n\n` elsewhere in the response. This does not affect downloaded scans. It affects only the data displayed on the Fortify Software Security Center AUDIT page.

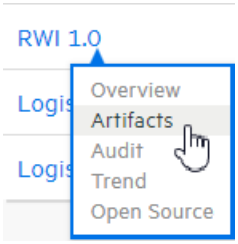
Important! The files you upload to Fortify Software Security Center must not exceed 2 GB.

Important! To upload third-party artifacts, you must have the correct parser configured. For information, see "Adding and Managing Parser Plugins" on page 175.

Also note that any raw scan file that contains third-party data must be packed into a ZIP file along with a `scan.info` metadata file. The `scan.info` property file must provide a value for the `engineType` property to identify the scanning engine that produced the results. That engine type must match the engine type registered by the parser plugin configured. The `scan.info` file can also provide a `scanDate` property value in ISO-8601 format. You can obtain the `scan.info` contents from https://github.com/fortify/sample-parser.

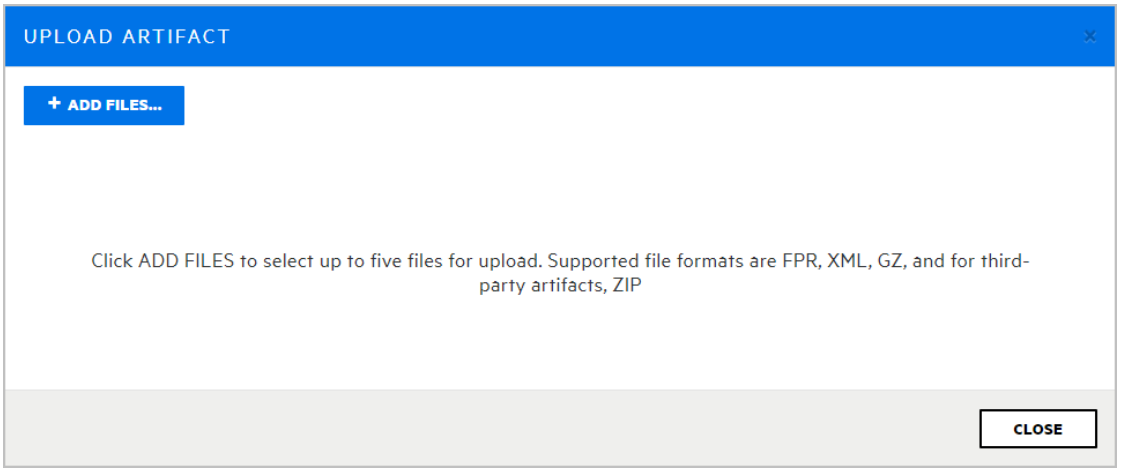
To upload a scan artifact to the Fortify Software Security Center database:

1. On the Dashboard or, for new applications, the Applications view, move your cursor to the application version for which you want to upload an artifact, and then select **Artifacts** from the shortcut menu.



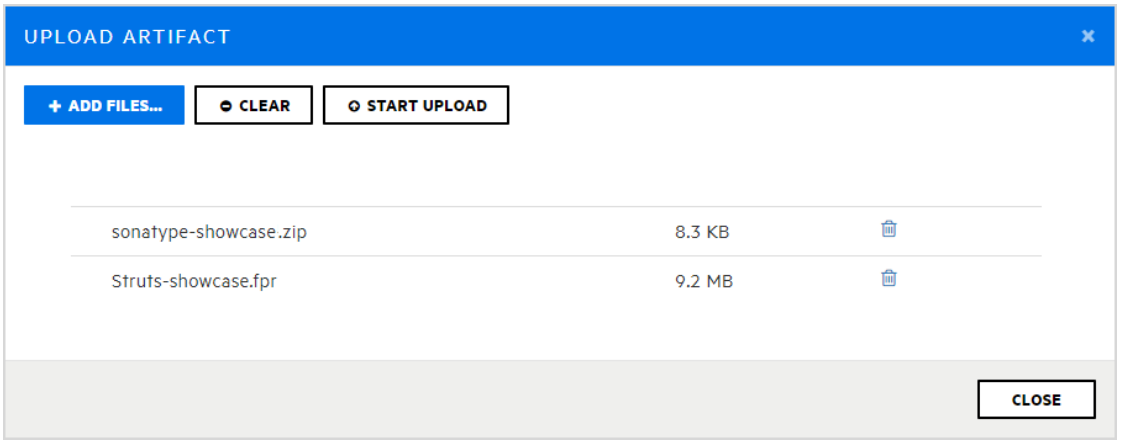
2. The **ARTIFACT HISTORY** table lists any and all scan artifacts uploaded for the application version.

3. Click **ARTIFACT**.



4. In the UPLOAD ARTIFACT dialog box, click **+ ADD FILES**.
5. Navigate to and select one or more (up to five) artifact files to upload.

   Formats supported for artifact upload are FPR, XML, GZ, and, for third-party artifacts, ZIP.



   The UPLOAD ARTIFACT dialog box lists the selected files.

6. To remove a file from the list, click the trash icon for that file. To remove all of the listed files, click **CLEAR**.
7. Click **START UPLOAD**.
   The dialog box displays a progress bar as each file is uploaded.
8. After your files are successfully uploaded, click **CLOSE**.

Note: If a scan artifact requires approval based on analysis result processing rules, it must be approved before Fortify Software Security Center can process it. For information, see "Approving Analysis Results for an Application Version" on page 316.

Viewing File Processing Errors

If there was an error in processing an uploaded artifact, the **Status** column of the **ARTIFACT HISTORY** table displays **Error Processing**, along with a circled number that indicates the number of processing rules violated.

To view information about the processing rules violated:

- Click the circled number.

The Artifact Processing Messages box opens to display details about problems encountered during the upload.

See Also

"Downloading Scan Artifacts" on page 315

"Setting Analysis Results Processing Rules for Application Versions" on page 266

"Using an Application Identifier to Upload FPR Files" on page 417

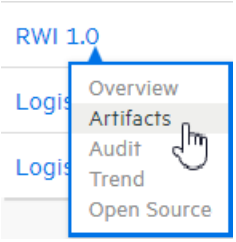
"Using an Application Name and Version to Upload FPR Files" on page 418

Viewing Scan Artifact Details

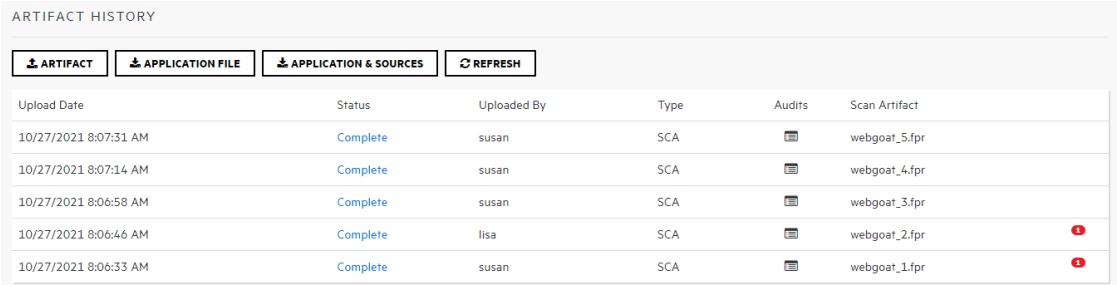
The following procedure describes the details available for uploaded scan artifacts. (For information about how to upload scan artifacts, see "Uploading Scan Artifacts" on page 311.)

To upload a scan artifact to the Fortify Software Security Center database:

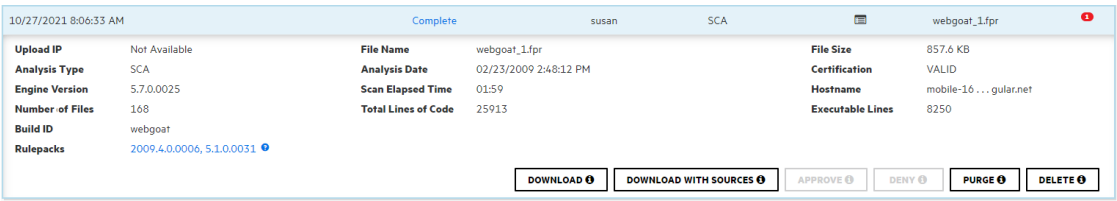
1. On the Dashboard or Applications view, move your cursor to the application version for which you want to view artifact details, and then select **Artifacts** from the shortcut menu.



The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the application version.



2. To view details for one of the listed artifacts, click the corresponding row.



The details shown include the analysis engine version, number of files and lines of code scanned, the analysis date, and more.

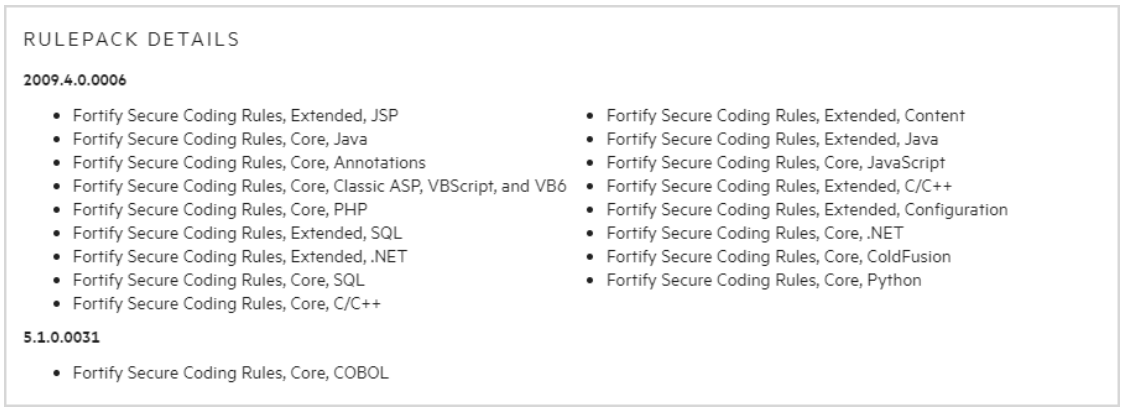
If an error occurred in processing the uploaded artifact, the **Status** column of the **ARTIFACT HISTORY** table displays **Error Processing**. A number on the right indicates the number of processing rules violated.

3. To view the line(s) of code associated with any processing errors for the scan, click the circled number (1).

   The SCAN WARNING box displays the line of code where processing rules were violated, along with a description of the violation.

   The field displays the Rulepack versions used in generating the scan.

4. To view a list of the coding rules applied during the scan, grouped by Rulepack version, click the **Rulepacks** link.


RULEPACK DETAILS

2009.4.0.0006

- Fortify Secure Coding Rules, Extended, JSP
- Fortify Secure Coding Rules, Core, Java
- Fortify Secure Coding Rules, Core, Annotations
- Fortify Secure Coding Rules, Core, Classic ASP, VBScript, and VB6
- Fortify Secure Coding Rules, Core, PHP
- Fortify Secure Coding Rules, Extended, SQL
- Fortify Secure Coding Rules, Extended, .NET
- Fortify Secure Coding Rules, Core, SQL
- Fortify Secure Coding Rules, Core, C/C++
- Fortify Secure Coding Rules, Extended, Content
- Fortify Secure Coding Rules, Extended, Java
- Fortify Secure Coding Rules, Core, JavaScript
- Fortify Secure Coding Rules, Extended, C/C++
- Fortify Secure Coding Rules, Extended, Configuration
- Fortify Secure Coding Rules, Core, .NET
- Fortify Secure Coding Rules, Core, ColdFusion
- Fortify Secure Coding Rules, Core, Python

5.1.0.0031

- Fortify Secure Coding Rules, Core, COBOL

Note: If a scan artifact requires approval based on analysis result processing rules, it must be approved before Fortify Software Security Center can process it. For information, see "Approving Analysis Results for an Application Version" on the next page.

See Also

"Downloading Scan Artifacts" below

"Purging Scan Artifacts" on page 323

"Setting Analysis Results Processing Rules for Application Versions" on page 266

"Using an Application Identifier to Upload FPR Files" on page 417

"Using an Application Name and Version to Upload FPR Files" on page 418

Downloading Scan Artifacts

From the ARTIFACT HISTORY page, you can download the latest merged FPR file for an application version, or you can download FPR files that result from individual scans.

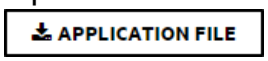
Downloading the Merged FPR File for an Application Version

To download the latest merged scan results for an application version in FPR format:

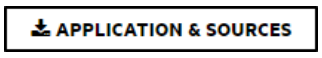
1. On the Fortify header, click **APPLICATIONS**.
2. In the Applications view, expand the row for the application and then select the version you are interested in.
3. On the application version toolbar, click **ARTIFACTS**.

   The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the application version.
4. Do one of the following:

- To download the latest merged scan results for an application version, at the top of the ARTIFACT HISTORY table, click **APPLICATION FILE**.

- To download the current merged application scan results in FPR format with sources, at the top of the ARTIFACT HISTORY table, click **APPLICATION & SOURCES**.

5. To open the scan results in Fortify Audit Workbench, in your **Downloads** folder, double-click the downloaded FPR file.

Downloading Individual Scan Results

To download results for a given processed scan:

1. On the Fortify header, click **APPLICATIONS**.
2. In the Applications view, expand the row for the application and then select the version you are interested in.
3. On the application version toolbar, click **ARTIFACTS**.

   The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the application version.
4. Click the row for the artifact you want to download to expand it and see the artifact details.
5. To download the artifact, click **DOWNLOAD**.

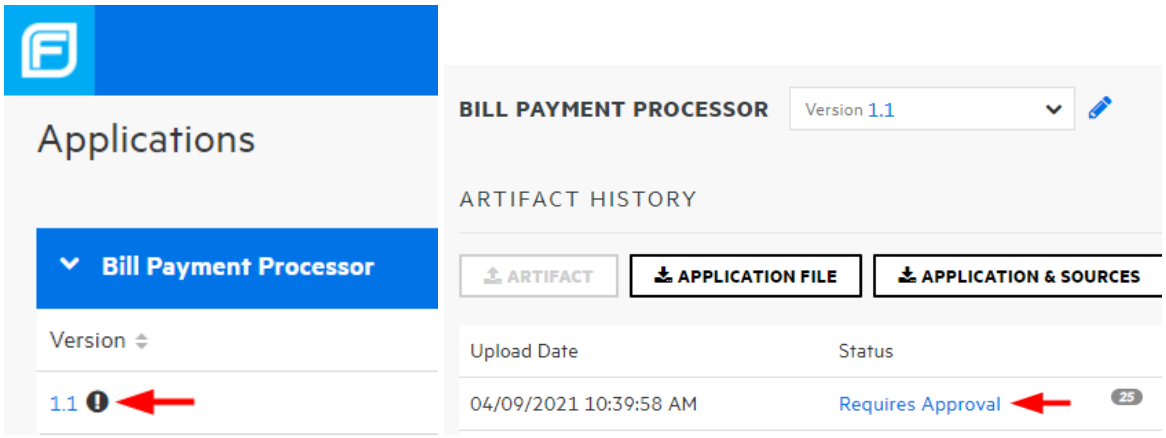
See Also

"Uploading Scan Artifacts" on page 311

"Deleting Artifacts" on page 324

Approving Analysis Results for an Application Version

Depending on the processing rules configured for an application version, and whether the Rulepack used in processing a scan was outdated (older than the server Rulepacks), analysis results may require approval. (See "Setting Analysis Results Processing Rules for Application Versions" on page 266.) If analysis results require approval, this is indicated by an alert icon () next to the version name in the Applications view and by the **Requires Approval** value in the **Status** column of the **ARTIFACT HISTORY** table.



Note: If an artifact was uploaded by mistake or, for some other reason, you do not want Fortify Software Security Center to process the artifact, follow the steps described in "Denying Processing Approval" below.

To approve analysis results for an application version so that Fortify Software Security Center can process the artifact:

1. In the Applications view, expand the application row, move your cursor to the version number, and then select **Artifacts** from the shortcut menu.

   The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the selected application version.
2. Expand a row with the value **Requires Approval** in the **Status** column.
3. At the bottom of the expanded section, click **APPROVE**.

   The APPROVE UPLOAD OF ANALYSIS RESULTS dialog box opens. The **Processing Messages** section shows an explanation of what, specifically, triggered the approval requirement.
4. In the **Approval Comment** box, type a comment to indicate why you are approving these results.
5. Click **APPROVE**.

Fortify Software Security Center proceeds to process the artifact.

Denying Processing Approval

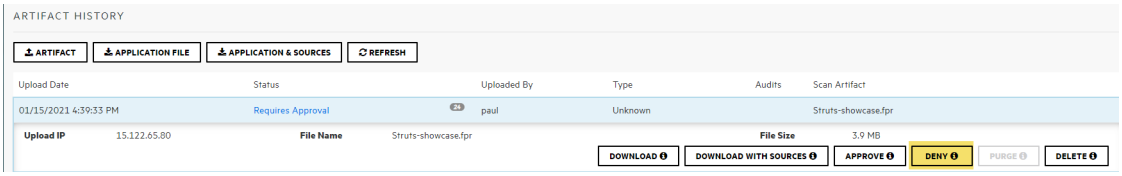
If an artifact was uploaded by mistake or, for some other reason, you do not want Fortify Software Security Center to process the artifact, you can either delete it, or, if you want to retain a record of the artifact upload, you can deny approval.

To deny approval of an artifact:

1. In the Applications view, expand the application row, move your cursor to the version number, and then select **Artifacts** from the shortcut menu.

The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the selected application version.

2. Expand the row for the artifact that requires approval, and which you do not want Fortify Software Security Center to process.



3. At the bottom of the expanded details section, click **DENY**.

   The DENY UPLOAD OF ANALYSIS RESULTS dialog box opens. The **Processing Messages** section lists explanations of what, specifically, triggered the approval requirement.

4. In the **Comment** box, type a comment to indicate why you want to deny approval of these results.
5. Click **DENY**.

The **Status** value for the artifact changes to **Approval Denied**.

Viewing High-Level Summary Results

Fortify Software Security Center offers several ways to view high-level summary results for application versions from the Fortify Software Security Center Dashboard or from the Overview page.

Viewing Summary Metrics on the Issue Stats Page

To view summary metrics for application versions (individually and collectively) from the Issue Stats page:

- On the Fortify header, select **DASHBOARD**.

The following three portlets on the Issue Stats page (the default Dashboard view in Fortify Software Security Center) displays consolidated metrics for all of the applications to which you have access:

- The **Issues Remediated** portlet shows the total number of issues remediated to date, the average number of days it took to review them, and the average number of days required to remediate them.
- The **Issues Pending Review** portlet shows the total number of open issues, and the number of these that have been reviewed.
- The **Application Versions** portlet shows the total number of application versions to which you have access the number of files scanned and the number of lines of code scanned for those application versions.

The table on the Issue Stats page displays summary metrics for each of the application versions to which you have access. If you click an application version listed in the table, Fortify Software Security Center takes you directly to the AUDIT page for that application version.

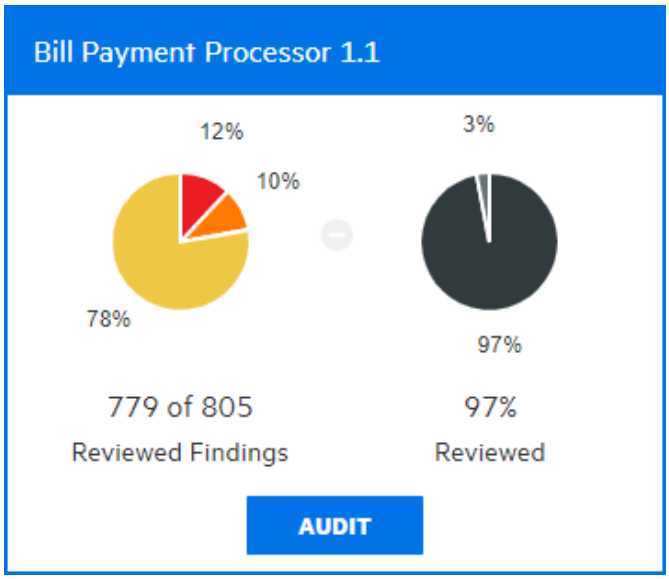
Together, the portlets and table enable you to see how quickly issues are being reviewed and remediated.

Viewing Summary Metrics on the CHART Page

You can view a graphical representation of summary metrics for individual application versions from the CHART page.

To view summary metrics for application versions from the Chart page:

1. On the Dashboard toolbar, click **CHART**.
   Fortify Software Security Center opens to the **REVIEWED** tab.
2. In the list of application versions, move your cursor to a colored bar for an application version.

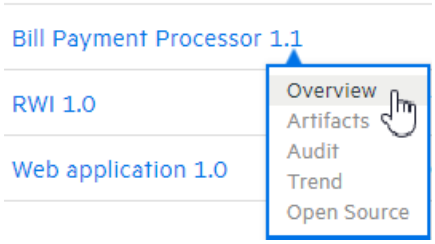


Fortify Software Security Center shows the summary findings for the version. In the example shown here, the pie chart of the left shows the security ratings for the 97% of findings (779 of 805) that have been audited to date for this application version. The chart on the right shows the percentage of findings audited (97) and the percentage of the total that has yet to be audited (3).

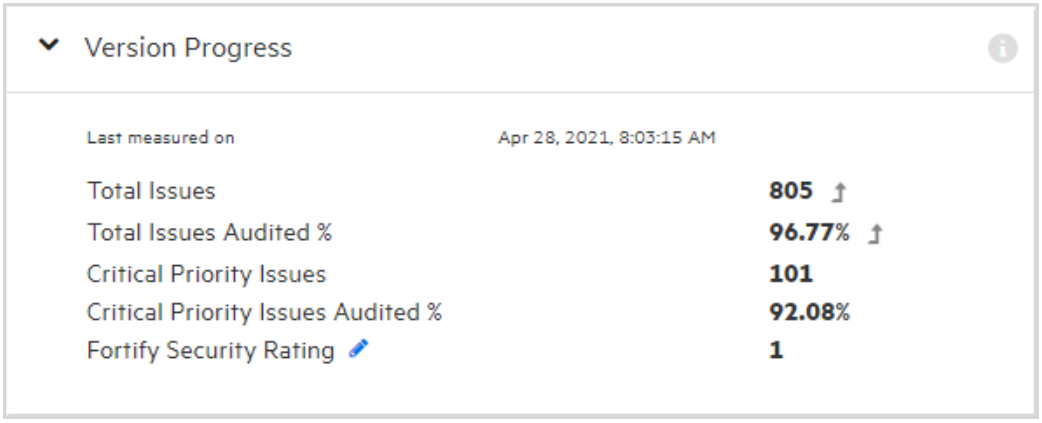
Note: To go from here to the AUDIT page for the application version, click **AUDIT**.

Viewing Summary Metrics on the Overview Page

To view high-level summary results for an application version from the Overview page:



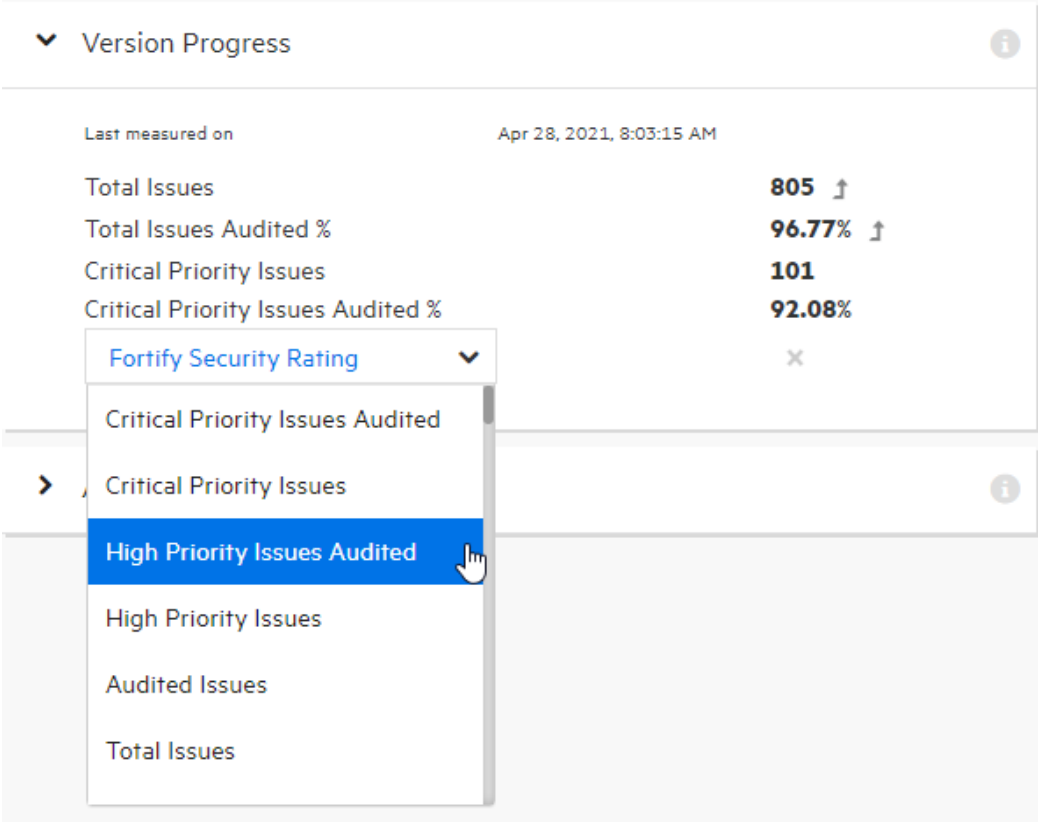
1. On the Fortify Dashboard, hover your cursor over the link for the version you are interested in, and then select **Overview** from the shortcut menu.
2. On the **Overview** page, if the pane on the right is collapsed, expand it.



The **Version Progress** section displays summary information with trending arrows.

3. To display a metric other than Fortify Security Rating, click the edit icon , and

then select a different metric to display from the list.



See Also

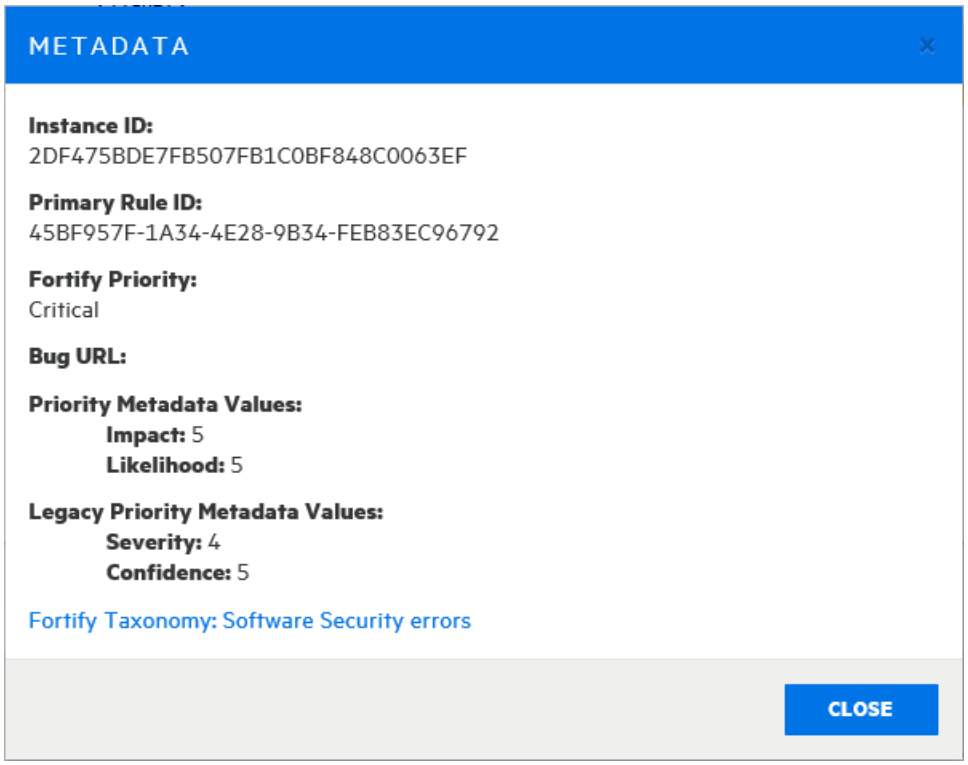
"Auditing Scan Results" on page 340

Viewing Issue Metadata

To view metadata for an issue:

1. Navigate to the AUDIT page for the application version of interest.
2. In the issues table, if you have selected a grouping, expand a group to view issues it contains.
3. Click the row that displays the issue name.

   The **Code** tab displays an overview of the issue, the **Analysis** value (if set), the stack trace, and the section of code in which the issue was uncovered.
4. At the bottom left of the issue details section, click **METADATA**.



The METADATA box displays the unique issue identifier (Instance ID), the unique identifier for the rule that generated the issue (Primary Rule ID), priority metadata values, and legacy priority metadata values.

Note: The instance ID displayed is unique to the specific application version and is not associated with any other Fortify Software Security Center application versions.

5. To go to the website that provides detailed information about software security errors, select the **Fortify Taxonomy: Software Security errors** link.

Mapping Scan Results to External Lists

Fortify distributes an external metadata document with Rulepacks. This document includes mappings from the Fortify categories to alternative categories (such as OWASP 2010, PCI, or CWE). Security leads can create their own files to map issues to different taxonomies, such as internal application security standards or additional compliance obligations.

Note: For detailed information about how to create custom mappings, see the *Micro Focus Fortify Static Code Analyzer Custom Rules Guide*.

To apply the modified or new external metadata document across all applications, you must first import it into Fortify Software Security Center.

To import a new or modified external metadata document into Fortify Software Security Center:

1. Log in as Administrator, and then, on the Fortify header, click the **ADMINISTRATION** tab.
2. In the left pane, under **Metrics &Tracking**, select **Rulepacks**.
3. In the upper right corner of the Rulepacks page, click **IMPORT**.
4. In the IMPORT RULEPACK dialog box, click **+ ADD FILES**.
5. Navigate to and select your document, and then click **START UPLOAD**.

If you are conducting a collaborative audit between Fortify Software Security Center and Audit Workbench, you can import the changed mapping document to Fortify Software Security Center, and then open the FPR file in Audit Workbench to see how the mapping works with the scan results.

Purging Scan Artifacts

Purging an artifact recovers space from the Fortify Software Security Center database by removing the uploaded artifact, the temporary results of artifact processing, and the cross-reference information for source files.

Before you purge artifacts for an application version, consider the following:

- After the purge, you cannot delete the purged artifacts, or the earliest artifact not purged.
- Purging does not affect any issue-base metrics in the system.
- If you have custom reports, consult Fortify Customer Support (https://www.microfocus.com/support) first to determine whether an artifact purge will affect them.
- Purging removes *all* artifacts that have the same or earlier analysis date.

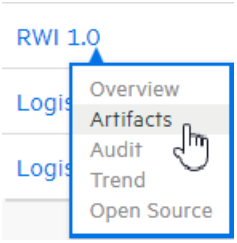
You can purge an artifact if it meets *all* of the following conditions:

- It has not already been purged.
- It does not contain just one scan generated from a given analysis engine type. For example, if only one Fortify Static Code Analyzer-generated artifact exists for an application version, you cannot purge it. If two artifacts from the same analysis engine were uploaded for the application version, you can purge only the older of the two artifacts.
- Its status is one of the following:
  - PROCESS_COMPLETE
  - ERROR_PURGING
  - ERROR_DELETING

You cannot purge an artifact if:

- It is being processed
- An error occurred during processing
- It contains the latest scan for the analysis engine type.

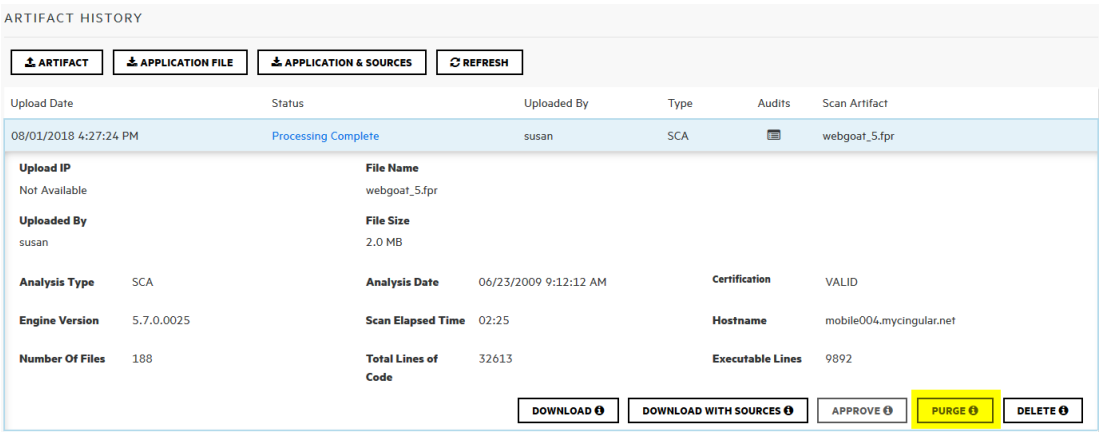
To purge a scan artifact from the Fortify Software Security Center database:



1. From the DASHBOARD, move your cursor to the application version with artifacts that you want to purge, and then select **Artifacts** from the shortcut menu.

   The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the application version.
2. Click the row that displays the artifact you want to purge from the database.

   The table expands to show the details for the selected artifact.



3. Below the artifact details, click **PURGE**.

   Fortify Software Security Center prompts you to confirm that you intend to purge the artifact.
4. Click **OK**.

See Also

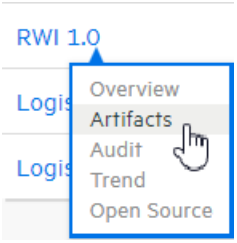
"Deleting Artifacts" below

Deleting Artifacts

Deleting an artifact removes all traces of the artifact. Use this option if you upload an artifact by mistake.

Note: You cannot delete an artifact that is being processed or one that has already been purged.

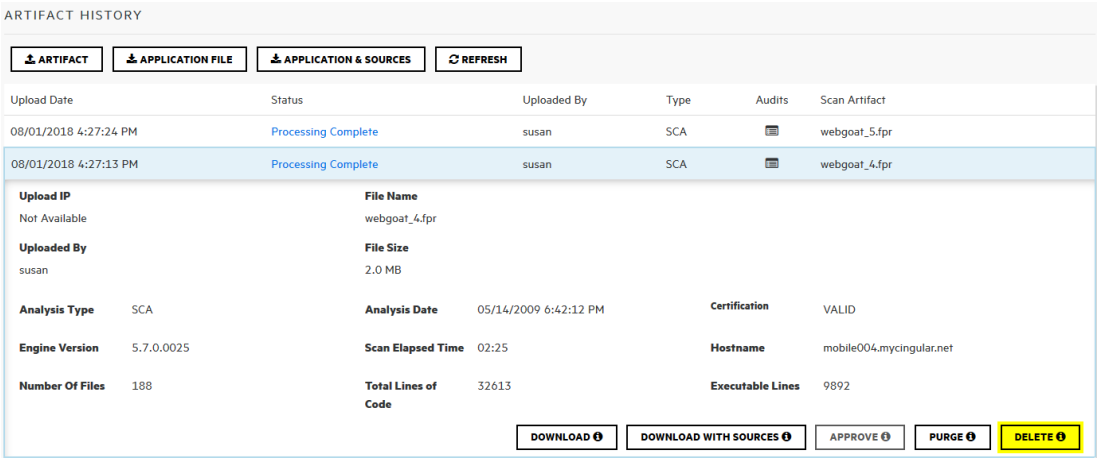
To delete a scan artifact from the Fortify Software Security Center database:



1. From the DASHBOARD, move your cursor to the application version with artifacts that you want to delete, and then select **Artifacts** from the shortcut menu.

   The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the application version.
2. Click the row that displays the scan artifact you want to delete.

   The table expands to show the details for the selected artifact.



3. Below the artifact details, click **DELETE**.

   Fortify Software Security Center prompts you to confirm that you want to delete the artifact.
4. Click **OK**.

See Also

"Purging Scan Artifacts" on page 323

Chapter 15: Collaborative Auditing

When an analysis engine (analyzer such as Fortify Static Code Analyzer) scans source code, all of its discoveries are presented as *potential* vulnerabilities, not actual vulnerabilities. Because every application is unique and all functionality runs within a particular context understood best by the development team, no technology can fully determine if a suspect behavior should be considered a vulnerability without direct developer confirmation.

Issue audits, whether performed in Fortify Software Security Center or Audit Workbench, or by Audit Assistant, accomplish the following:

- Condense and focus application information
- Enable the security team to collaboratively decide which issues represent real vulnerabilities
- Enable the security team to collaboratively prioritize issues based on vulnerability

Fortify Software Security Center uses issue templates to categorize and display issues.

Fortify Software Security Center provides a web-based collaborative environment for auditing issues associated with Fortify Software Security Center applications. The following sections provide an overview of the auditing process and instructions on how to display and use the auditing interface.

The information in these topics is presented based on the assumption that you know how to create and configure Fortify Software Security Center application versions. (For information about Fortify Software Security Center applications and application versions, see "Applications and Application Versions" on page 232.)

Topics covered in this section:

About Current Issues State

Fortify Software Security Center keeps track of which analysis engine (analyzer) uncovers each issue in an application version and merges any new information into the existing body of results for the application version. After new audit information is uploaded to the server or entered on the AUDIT page, Fortify Software Security Center merges that information into any existing audit information for a given issue.

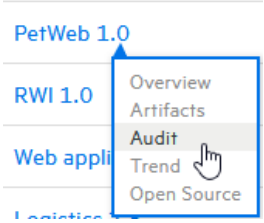
Fortify Software Security Center also marks an issue as *removed* after the analysis engine no longer finds the issue.

Whenever new scan results are uploaded, Fortify Software Security Center checks every issue to determine whether it was uncovered in a previous scan.

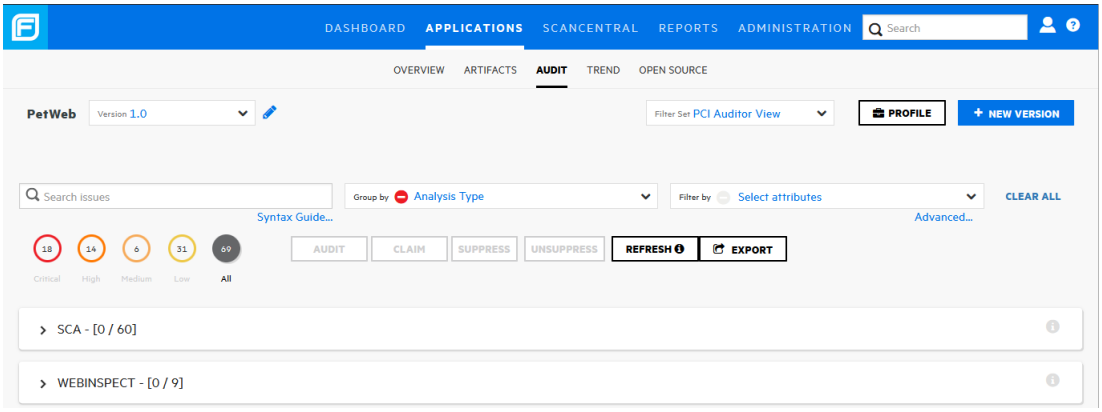
Viewing Information About Issues to Audit

To display the issues you want to audit:

1. Upload scan results for the application version you want to audit (see "Uploading Scan Artifacts" on page 311).

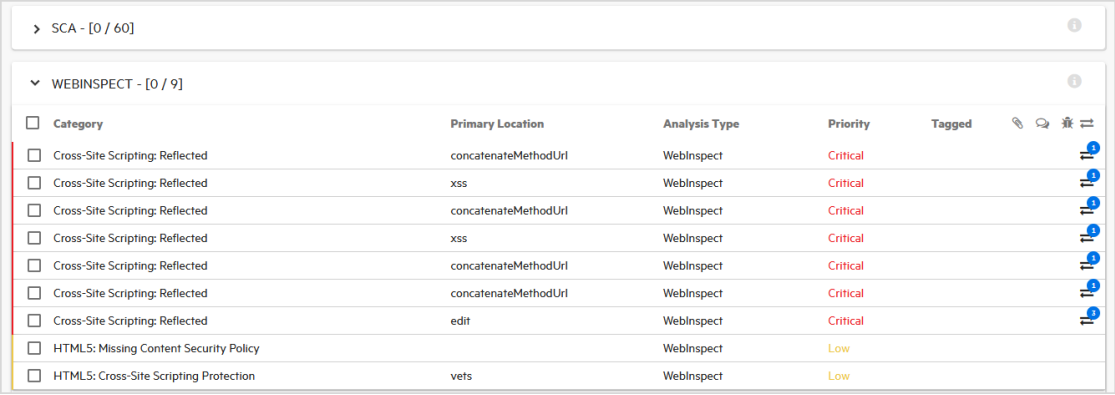


2. Open the AUDIT page for the application version.
3. To selectively display the issues you want to audit, apply filters to the issues list. (See "Filtering Issues for Display on the OVERVIEW and AUDIT Pages" on page 332 and "Viewing Issues Based on Folders" on page 330.)



4. In the issues table, if you have selected a grouping, expand a group to view the

issues it contains.



The following table lists the columns in the issues table and a description of each. To sort listed issues, click a column heading.

Note: You cannot sort the **Contains attachment** (), **Contains comments** (), or **Bug submitted** () columns.

Column	Description
Category	Displays the category of issue uncovered (Sort is alpha-numeric.)
Primary Location	Shows the file scanned and line of code on which the issue was detected (Sort is alpha-numeric.)
Analysis Type	Displays the analysis engine used in the scan
Priority	Shows the relative threat the issue represents (Sort is from high to low or low to high priority.)
Tagged	Displays the custom tag value applied to the issue, if any
Attachments	Indicates whether any attachments are associated with the issue
Contains comments	Indicates whether any comments were added to the issue
Bug submitted	Indicates whether any defects were submitted against the issue
⇄	Indicates that static and dynamic results for the

Column	Description
Has correlated issues	issue are correlated. If they are, the issue is listed twice in the table, once for each analysis type. If either a subsequent static scan or dynamic scan shows an issue was fixed, the correlation icon is removed. (Sort displays correlated issues first or last.)

See Also

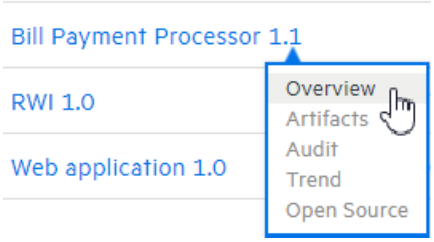
"Auditing Scan Results" on page 340

Viewing Issues Based on Folders

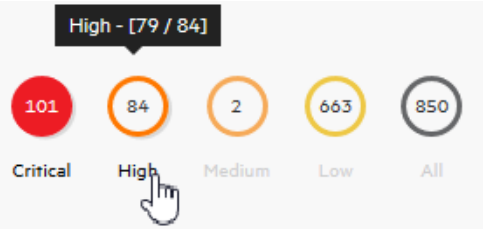
The OVERVIEW and AUDIT pages include **Critical**, **High**, **Medium**, **Low**, and **All** links, which you can use to view issues based on their assignment to a Fortify folder. By default, the folders correspond to Fortify priority values (and the potential risk they pose to the enterprise), However, the folders displayed can include any custom folders created in and added to a filter set (and then an issue template) from Fortify Audit Workbench (see the *Fortify Audit Workbench User Guide*).

To view issues from the OVERVIEW page based on Fortify folder assignment:

1. On the Dashboard, hover your cursor over the version number of the application of interest, and then select **Overview**.



   The OVERVIEW page for the application version opens. To the left of the **Group by** and **Filter by** lists, the **you can see** the total number of issues in their respective folders. By default, all issues are shown. (If you select attributes to filter by, the numbers displayed for the folders changes accordingly.)
2. To see the number of issues in a folder that have been reviewed, move your cursor to the folder.

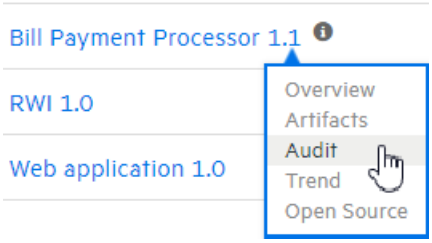


The number of reviewed issues is on the left, and the total number of issues is on the right. In the example shown here, you can see that 79 of 84 total high priority issues were reviewed.

3. To view issue charts on the OVERVIEW page based on an assigned folder, select the folder or the folder label.

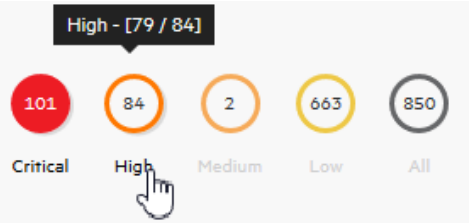
To view issues from the AUDIT page based on Fortify folder assignment:

1. On the Dashboard, hover your cursor over the version number of the application of interest, and then select **Audit**.



The OVERVIEW page for the application version opens. Below the search field, you can see the number of issues in their respectiveassigned folders. By default, all issues are shown. (If you select attributes to filter by, the numbers displayed for the folders changes accordingly.)

2. To see the number of issues assigned to a given folder that have been reviewed, move your cursor to the folder.



The number of reviewed issues is on the left, and the total number of issues is on the right. In the example shown here, 79 of 84 total high priority issues were reviewed.

3. To list issues on the AUDIT page based on folder assignment, select the folder.

See Also

"Filtering Issues for Display on the OVERVIEW and AUDIT Pages" on the next page

Viewing Issues Assigned to You

To view all issues assigned to you:

1. On the Fortify header, click **APPLICATIONS**.
2. In the Applications view, select the **My assigned issues** check box.

   The Applications view lists the application versions and shows the number of issues for each that are assigned to you. If Fortify Software Security Center finds no issues assigned to you, it displays a message to let you know.

See Also

"Setting Issue Viewing Preferences" on page 350

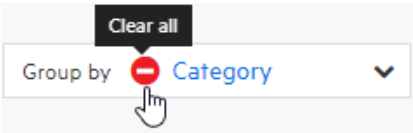
Filtering Issues for Display on the OVERVIEW and AUDIT Pages

Use the following steps to filter issues for display for an application version from either the OVERVIEW page or from the AUDIT page.

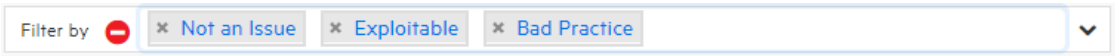
Note: You can also select a filter set to change the issues displayed on the OVERVIEW and AUDIT pages. For information and instructions, see "Changing Displayed Issues Using Filter Sets" on page 352.

To filter issues for display on the OVERVIEW or AUDIT page:

1. From the **Group by** list, select the attribute to use to group the issues in the issues table.

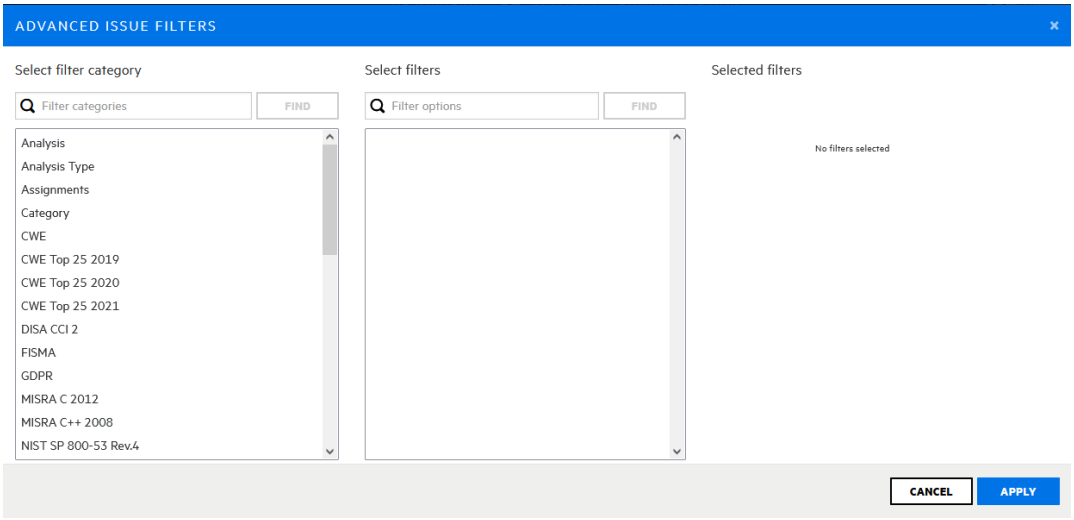
   

   (To remove the selected attribute, click the **Clear all** icon.)
2. From the **Filter by** list, select the attributes to use to filter the issues for display in the issues table. You can select multiple attributes from this list. (You must select attributes one at a time.)

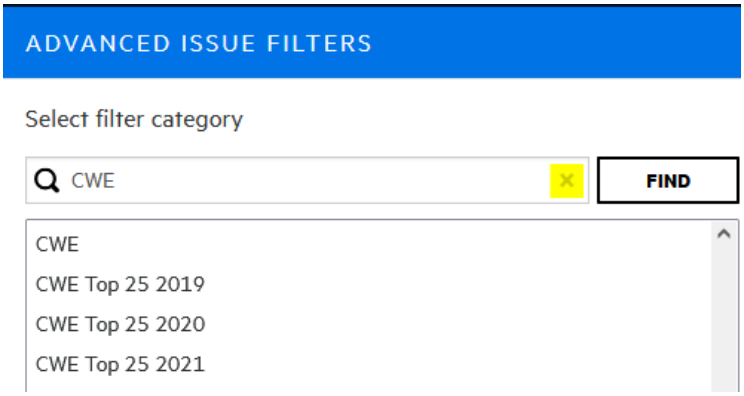
   

   (To remove a selected attribute, click the **x** icon next to its name. To remove all selected attributes, click the **Clear all** icon.)

3. To filter issues based on values for a custom tag other than Analysis, or based on risks related to OWASP, WASC, or other security threat classifications:
   a. Click the **Advanced** link which is located under the **Filter by** list.



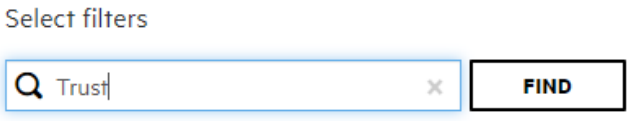
   b. In the ADVANCED ISSUE FILTERS window, from the **Select filter category** list, select a category. To refine the categories listed, type a text string in the **Filter categories** box, and then click **FIND**.



   The **Select filters** list is populated with the filters available for the selected category.

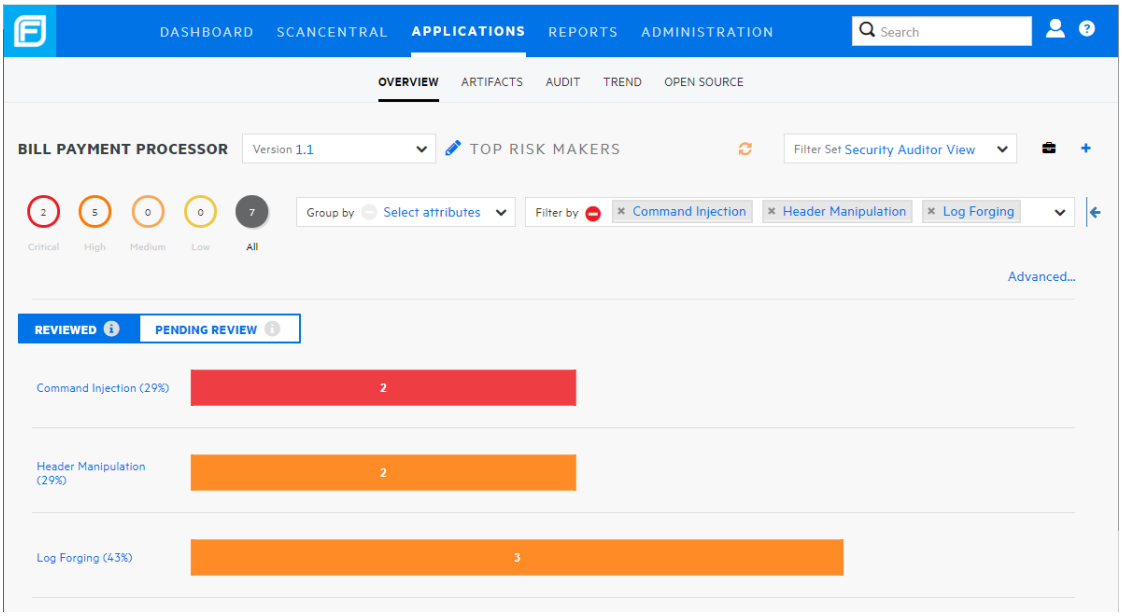
   c. To refine the **Select filters** list further, type a text string in the **Filter options** box, and then click **FIND**.

   The **Select filters** list displays the filters that contain the matching text.



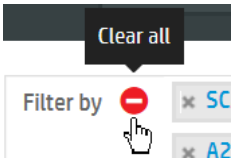
   To see the complete list of filters again, click the **x** in the **Filter categories** box.

d. In the **Select filters** list, click each of the filters you want to add to the **Selected filters** list to the right.
e. To add filters for another filter category, repeat these steps.
f. Click **APPLY**.



The **Filter by** box now displays all of the filters you have selected.

4. To remove one of the filters, click the close symbol to its left.



5. To clear all **Group by**, **Filter by**, and advanced filter selections, click **CLEAR ALL**.
6. For information about viewing correlated issues, see "Auditing Correlated Issues" on page 348.

See Also

"Searching Issues" on the next page

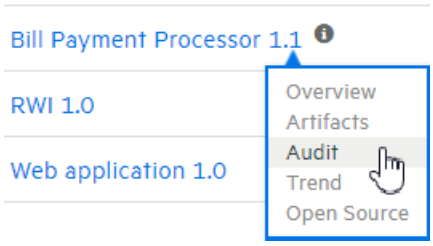
"Viewing Issues Based on Folders" on page 330

"Searching Globally in Fortify Software Security Center" on page 365

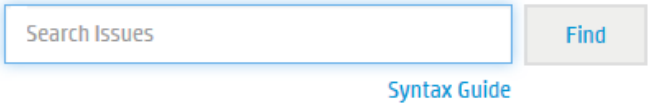
Searching Issues

You can create search queries to refine the list of issues displayed for an application version.

To create a query to search issues:



1. In the application version summary table on the Dashboard, move your cursor to the application version of interest, and then select **Audit**.



2. In the **Search Issues** box, type a search query using the following syntax. To indicate the type of comparison to perform, wrap search terms with delimiters.

Comparison	Description
contains	Searches for a term without any special qualifying delimiters
equals	Searches for an exact match if the term is enclosed in quotation marks (`""`)
number range	Uses standard mathematical syntax, such as "`(`" and "`)`" for exclusive range and "`[`" and "`]`" for inclusive range where `(2,4]` means greater than two less than or equal to four
not equal	Excludes issues specified by the string by preceding the string with an exclamation character (`!`) Example: `file:!Main.java` returns all issues that are not in `Main.java`

Note: To see example search strings, click the **Syntax Guide** link.

You can further qualify your search terms with modifiers using the syntax `modifier:<search_term>`. (See "Search Modifiers" on the next page.)

Note: If an application version is assigned a date-type custom tag, and you want to search for issues based on that tag, use one of the following

formats:

- To search for date tags that have no value set:
  `<DateCustomTag>: <none>`
- To search for date tags that have a (any) date set:
  `<DateCustomTag>: !<none>`
- To search for date tags with a specific date:
  `<DateCustomTag>: yyyy-mm-dd`

A search string can contain multiple modifiers and search terms. If you specify more than one modifier, Fortify Software Security Center returns only issues that match all of the modified search terms. For example, `file:ApplicationContext.java category:SQL Injection` returns only SQL injection issues found in `ApplicationContext.java`.

If you use the same modifier more than once in a search string, then the search terms qualified by those modifiers are treated as an OR comparison. For example, `file:ApplicationContext.java category:SQL Injection category:Cross-Site Scripting` returns SQL injection issues and cross-site scripting issues found in `ApplicationContext.java`.

For complex searches, you can also insert the `AND` or the `OR` keyword between your search queries. Note that `AND` and `OR` operations have the same priority in searches.

3. Click **Find**.
   Fortify Software Security Center lists all issues that match your search string.
4. To return to the complete issues list, clear the text in the search box.

See Also

"Filtering Issues for Display on the OVERVIEW and AUDIT Pages" on page 332

"Search Query Examples" on page 339

"Searching Globally in Fortify Software Security Center" on page 365

Search Modifiers

You can use a search modifier to specify which attribute of an issue the search term should apply to. To use a modifier that contains a space in the name, such as the name of the custom tag, you must delimit the modifier with brackets. For example, to search for issues that are new, enter `[issue age]:new`.

A search that you do not qualify using a modifier matches the search string based on the following attributes: kingdom, primary rule id, analyzer, filename, severity, class name, function name, instance id, package, confidence, type, subtype, taint flags, category, sink, and source.

To apply the search to all modifiers, enter a string such as `control flow`. This searches all modifiers and returns any result that contains the specified string.

To apply the search to a specific modifier, type the modifier name and the string as follows: `analyzer:control flow`. This returns all results whose analyzer is `control flow`.

The following table lists the search modifiers. A few of these have a shortened names, which are indicated in parentheses. You can use either modifier string.

Modifier	Description
`[issue age]`	Searches for the issue age, which is `new`, `updated`, `reintroduced`, or `removed`.
`<custom_tagname>`	Searches the specified custom tag. Note that tag names that contain spaces must be delimited by square brackets. Example: `[my tag]:value`
`analysis`	Searches for issues that have the specified audit analysis value (such as `exploitable`, `not an issue`, and so on).
`analyzer`	Searches the issues for the specified analyzer
`audience`	Searches for issues by intended audience. Valid values are `targeted`, `medium`, and `broad`. **Note:** This metadata is legacy information that is no longer used and will be removed in a future release. Fortify recommends that you not use this search modifier.
`audited`	Searches the issues to find `true` if the primary custom tag is set and `false` if the primary custom tag is not set. The default primary tag is the Analysis tag.
`category (cat)`	Searches for the given category or category substring.
`comments` `(comment, com)`	Searches for issues that contain the search term in the comments that have been submitted on the issue.

Modifier	Description
`commentuser`	Searches for issues with comments from the specified user.
`confidence (con)`	Searches for issues that have the specified confidence value. Fortify Static Code Analyzer calculates the confidence value based on the number of assumptions made in code analysis. The more assumptions made, the lower the confidence value.
[engine priority]	Searches for issues based on the original priority value determined by the engine that identified the issue.
`file`	Searches for issues where the primary location or sink node function call occurs in the specified file.
`[fortify priority order]`	Searches for issues that have a priority level that matches the specified priority. Valid values are `critical`, `high`, `medium`, and `low`.
`historyuser`	Searches for issues that have audit data modified by the specified user.
`kingdom`	Searches for all issues in the specified kingdom.
`maxconf`	Searches for all issues that have a confidence value equal to or less than the number specified as the search term.
`<metadata_listname>`	Searches the specified metadata external list. Metadata external lists include [OWASP Top 10 2013], [SANS Top 25 2011], and [PCI <*version*>], and others. Square braces delimit field names that include spaces.
`minconf`	Searches for all issues that have a confidence value equal to or greater than the number specified as the search term.
`package`	Searches for issues where the primary location occurs in the specified package or namespace.

Modifier	Description
	For dataflow issues, the primary location is the sink function.
`[primary context]`	Searches for issues where the primary location or sink node function call occurs in the specified code context. Also see sink and [source context].
`primaryrule (rule)`	Searches for all issues related to the specified sink rule.
`sink`	Searches for issues that have the specified sink function name. Also see [primary context].
`source`	Searches for dataflow issues that have the specified source function name. Also see [source context].
`[source context]`	Searches for dataflow issues that have the source function call contained in the specified code context Also see source and [primary context].
`sourcefile`	Searches for dataflow issues with the source function call that the specified file contains. Also see file.
`status`	Searches issues that have the status reviewed, not reviewed, or under review.
`suppressed`	Searches for suppressed issues.
`taint`	Searches for issues that have the specified taint flag.

For examples of search queries that use modifiers, see "Search Query Examples" below.

See Also

"Searching Issues" on page 335

Search Query Examples

The following are search query examples that use search modifiers.

- To search for all privacy violations in file names that contain `jsp` with `getSSN()` as a source, type:
  ```
  category:"privacy violation" source:getssn file:jsp
  ```
- To search for all file names that contain `com/fortify/ssc`, type:
  ```
  file:com/fortify/ssc
  ```
- To search for all issues that contain `cleanse` as part of any modifier, type:
  ```
  cleanse
  ```
- To search for all audited issues that have the `[my tag]` assigned and set to `P1`, type:
  ```
  [my tag]:P1
  ```
- To search for all suppressed vulnerabilities with `asdf` in the comments, type:
  ```
  suppressed:true comments:asdf
  ```
- To search for all categories except for SQL Injection, type:
  ```
  category:!SQL Injection
  ```
- To search for all issues in file names that contain either `java` or `jsp`, type:
  ```
  filename:java OR filename:jsp
  ```
- To search for all issues in file names that contain `java` and that occur on line number 12, type:
  ```
  filename:java AND line:12
  ```

See Also

"Searching Issues" on page 335

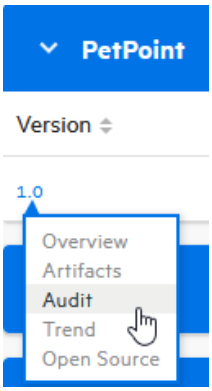
"Search Modifiers" on page 336

Auditing Scan Results

Note: The following procedure describes how to audit scan results from the AUDIT page. If you are working with open source results, you can audit these from either the AUDIT page or from the OPENSOURCE page.

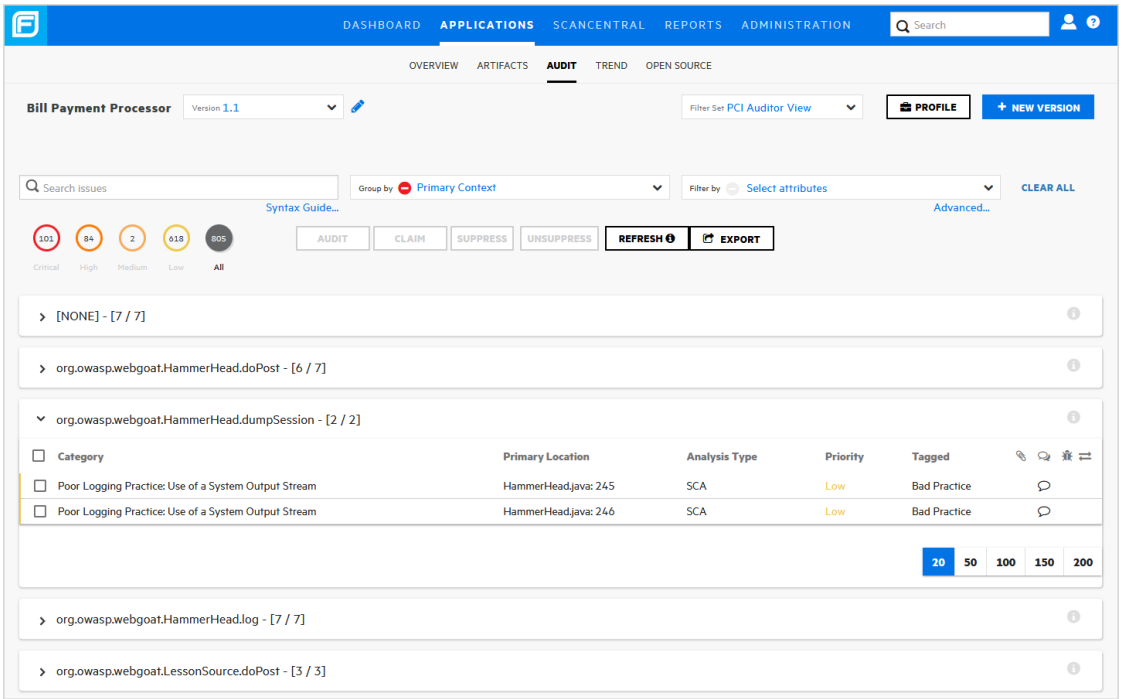
To display the issues you want to audit:

1. Upload scan results for the application version you want to audit. For instructions, see "Uploading Scan Artifacts" on page 311.



2. Open the AUDIT view for the application version.

   The table in the AUDIT view lists issues based on their assigned folders (by default, critical to low).
3. To selectively display the issues you want to audit, apply filters to the issues list. (See "Filtering Issues for Display on the OVERVIEW and AUDIT Pages" on page 332 and "Viewing Issues Based on Folders" on page 330.)
4. In the issues table, if you have selected an attribute to group by, expand a group to view the issues it contains.

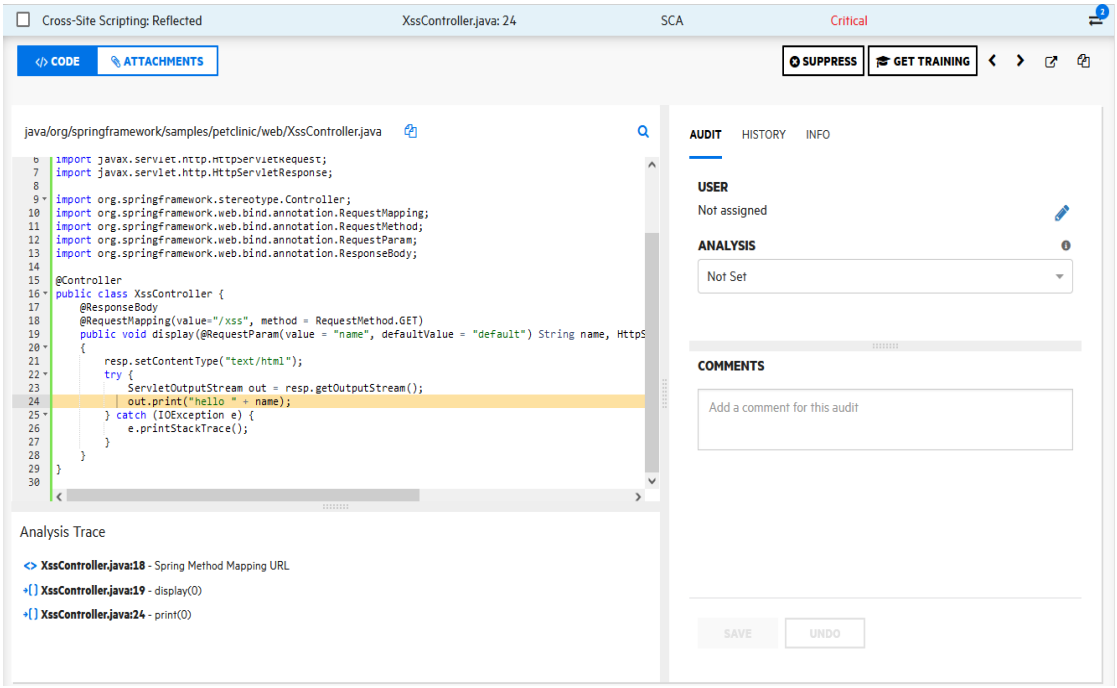


To audit an issue:

1. To expand an issue and view its details, click its row in the table.

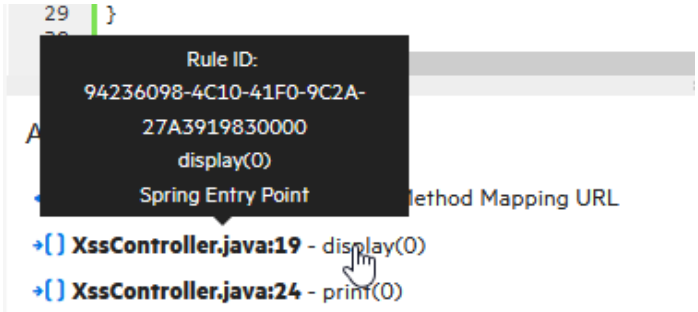
   The following screen capture shows the details for an issue uncovered during a Fortify Static Code Analyzer scan. For information about viewing Fortify

WebInspect results, see "Viewing Fortify WebInspect Scan Results in Fortify Software Security Center" on page 373.



Tip: To view the details for the issue in a new browser window, click the **Open in a new tab** button (). To copy the issue link so that you can easily access it later, click the **Copy issue link to clipboard** button ().

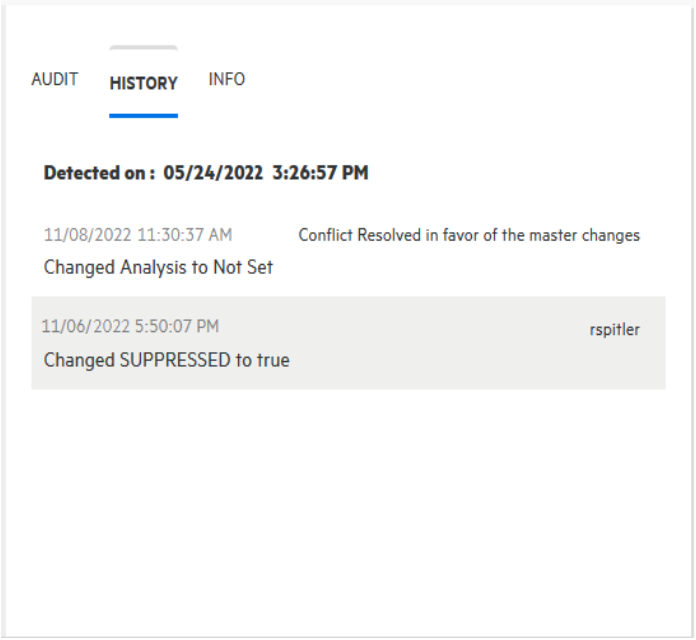
The **CODE** tab displays the path the tainted data have taken in the source code associated with the issue.



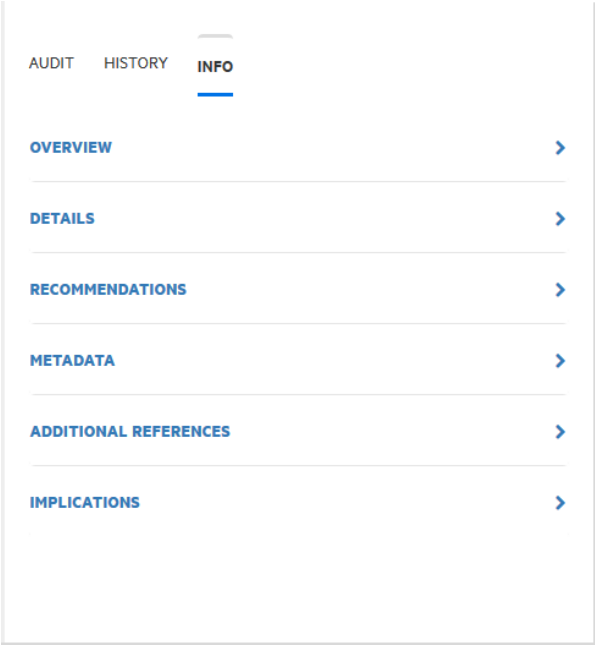
2. To view summary details about a step along the course that tainted data has taken, under **Analysis Trace**, move your cursor to that step.
3. To view code associated with a step, click the step under **Analysis Trace**.
   The corresponding line of code is highlighted on the **CODE** tab.

4. To search for a specific string in the code associated with the issue:
   a. Click the search icon .

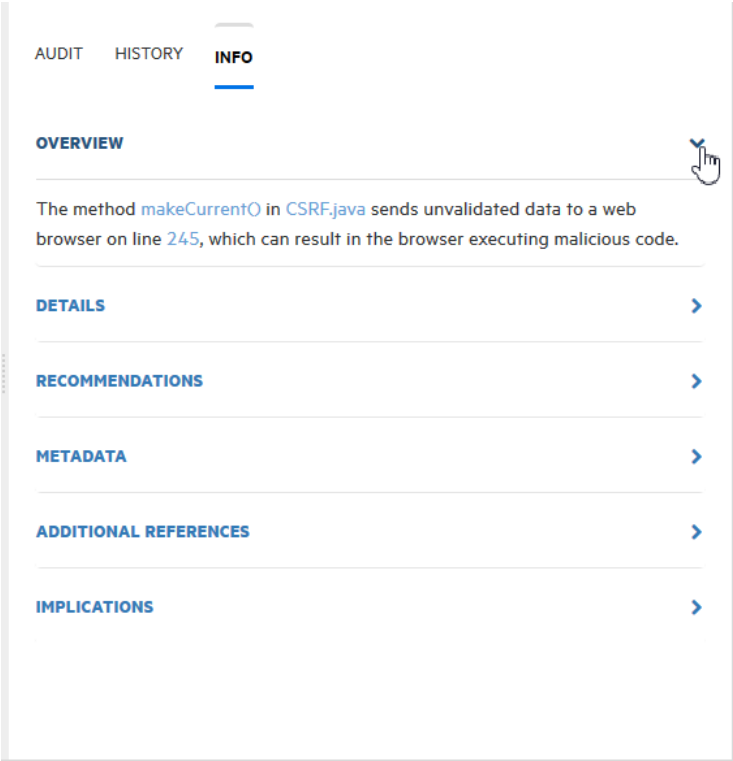
   b. In the text box displayed, type a character string. Use the next and previous icons to move through the search results.



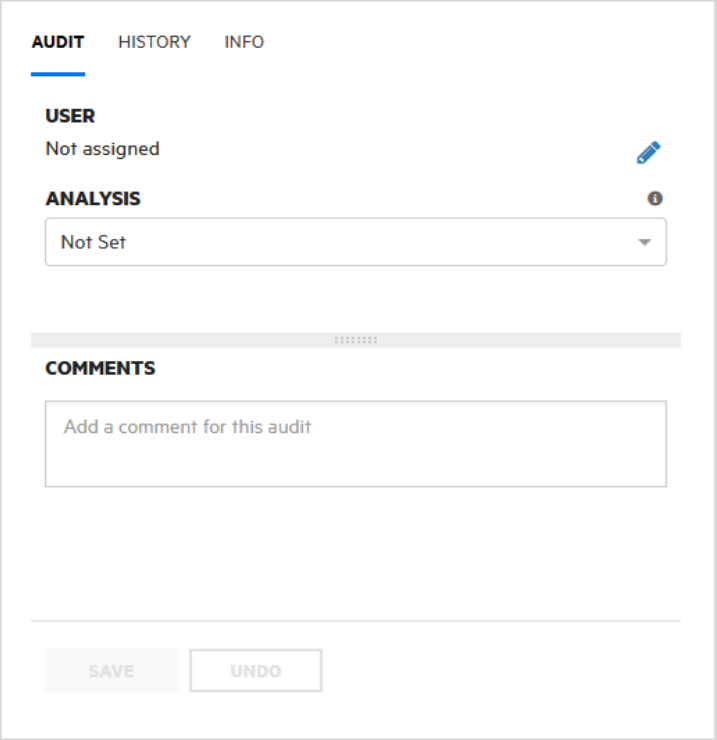
5. To view any audit history available for the issue, in the right pane, select the **HISTORY** tab.



6. To see an issue overview, details about the finding, recommendations for remediation, issue metadata, references to additional resources, and implications for your application version, in the right pane, select the **INFO** tab.



7. To expand a row and view a class of information, select the corresponding arrow (›).



8. When you have enough information to start your audit, in the right pane, select the **AUDIT** tab.

9. (Optional) To exclude an issue from display because you know it is fixed or it is not of immediate concern, click **SUPPRESS**.

10. (Optional) If your administrator has configured application security training in Fortify Software Security Center (see "Configuring Application Security Training" on page 88) you can click **GET TRAINING** to get contextually-appropriate guidance on how to mediate the selected issue. A message advises you that you are about to leave Fortify Software Security Center. Click **OK**.

    Fortify Software Security Center opens the application security training website in a new browser tab that displays training content based on the category, subcategory, and language of the selected issue.

    Note: After a file is attached to an issue, you can modify only its description.

11. To attach a file to the issue:

    a. In the left pane, click **ATTACHMENTS**.
    b. Click **CLICK HERE TO ADD**.

c. In the UPLOAD ATTACHMENT dialog box, click **BROWSE**, and then navigate to and select the file to upload.

   Supported file formats are TXT, LOG, DOC, DOCX, PDF, PPT, PPTX, JPG, JPEG, BMP, PNG, TIFF, GIF, ZIP, GZIP, TAR, and 7ZIP. (Documents in XML format are not supported.)

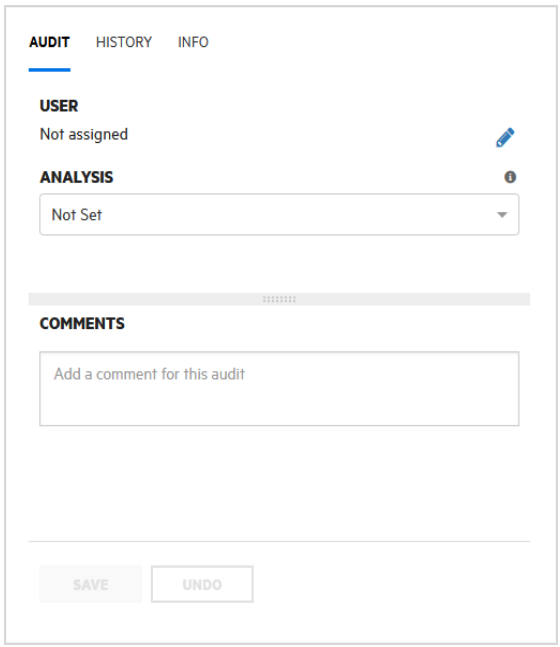
   Note: The file size must not exceed 3 MB.

d. (Optional) In the **Description** box, type a description of the file.

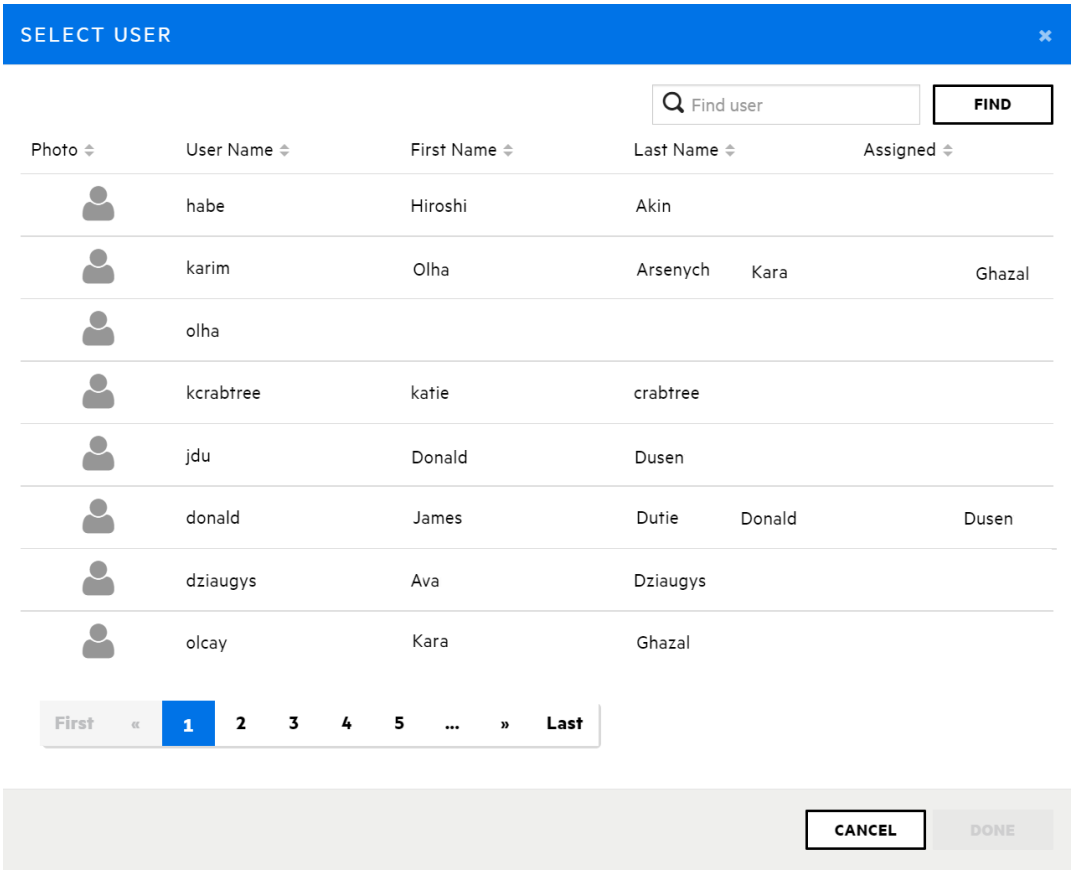
e. Click **SAVE**.

   If you attached an image file, Fortify Software Security Center displays a preview of the image on the right, under **Image Preview**.

12. Click **CODE**, and then, in the right pane, select the **AUDIT** tab.



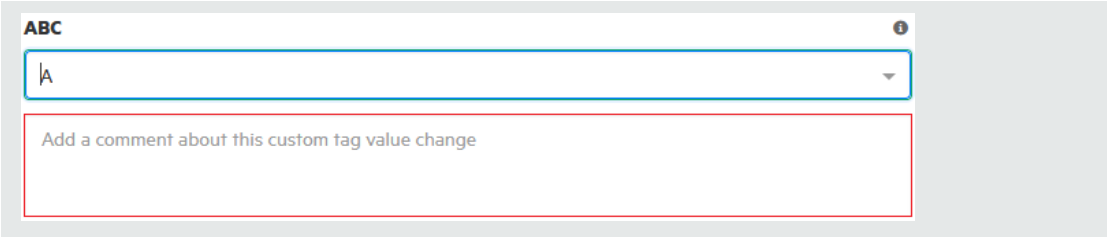
13. To assign a user to the issue:
    a. Under **USER**, click the **Edit assigned user** icon.



    b. To locate a user to assign to the issue from the SELECT USER dialog box, in the **Find user** box, type part or all of a user's name, and then click **FIND**.
    c. In the list of returned names, click the name of the user to assign to the issue.
    d. Click **DONE**.

    The **AUDIT** tab now displays the selected user name and avatar (if available).
14. From the ***<Primary_Tag_Name>*** list, select a value that reflects your assessment of this issue. Fortify Software Security Center treats the issue as unaudited.
15. If additional custom tags are associated with the application version, specify the values for those tags.

    Note: If an administrator specified that a comment is required for a custom tag you assign, then you must type a comment in the box outlined in red, which appears under the custom tag value list.



Note: If Audit Assistant assessed the issues, the right pane displays additional fields **AA_Prediction**, **AA_Confidence**, and **AA_Training**). For information about how to use these fields, see "Reviewing Audit Assistant Results" on page 364.

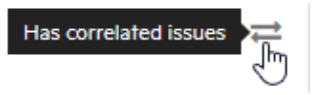
16. In the **COMMENTS** box, type a comment about this issue audit. (After you save your audit settings, the **COMMENTS** section lists your comment, as well as any other comments previously saved.)
17. At the bottom of the **AUDIT** tab, click **SAVE**.

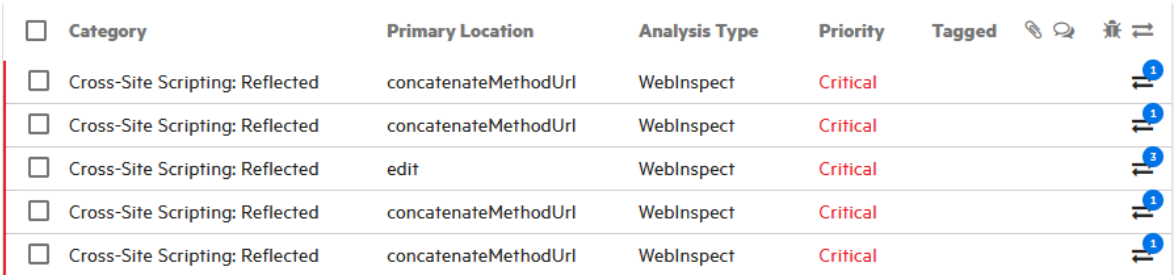
Auditing Correlated Issues

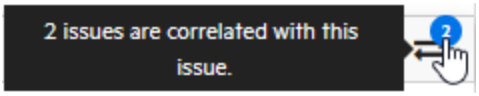
If the artifacts uploaded for the application version include results from both static (Fortify Static Code Analyzer) and dynamic (WebInspect) analyses, some issues may be correlated with one another.

If an issue is correlated with one or more other issues uncovered using a different analysis engine, the **Has correlated issues** icon is displayed, along with the number of correlated issues that either target or originate from the selected issue.

To list issues that are correlated with other issues at the top of the table, click the **Has correlated issues** icon twice.



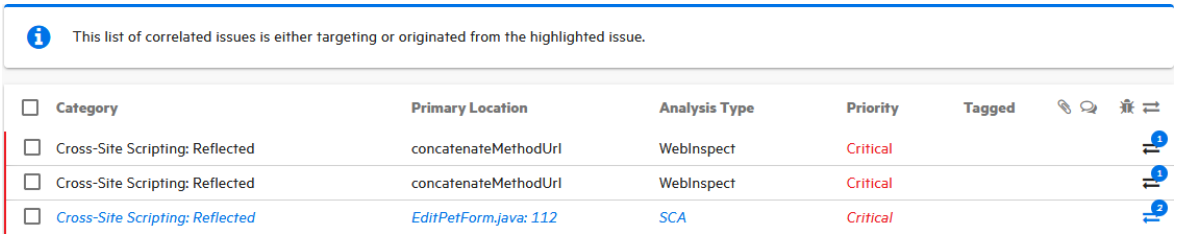




The number shown in the blue circle indicates how many issues are correlated with an issue.

To list the correlated issue or issues:

- Click the circle or the **Has correlated issues** icon,



You can audit the listed issues as described in "Auditing Scan Results" on page 340.

Note: If, following an audit, a developer fixes the root problem uncovered in one issue, the remaining correlated issues may also be fixed.

To return to the complete issues table, to the right of the **Filter by** list, click **CLEAR ALL**.

See Also

"Auditing a Batch of Issues" on page 358

"About Audit Assistant" on page 88

About Suppressed, Removed, and Hidden Issues

You can control whether the issues pane lists suppressed, removed, and hidden issues.

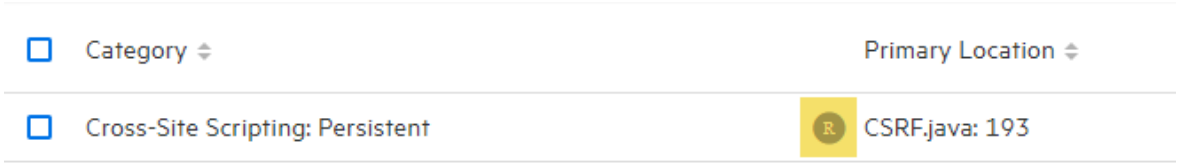
Suppressed issues

As you assess successive scans of an application version, you might want to completely *suppress* some exposed issues. It is useful to mark an issue as suppressed if you are sure that the specific vulnerability is not, and will never be, an issue of concern. You might also want to suppress warnings for specific types of issues that might not be high priority or of immediate concern. For example, you can suppress issues that are fixed, or issues that you plan not to fix.

Suppressed issues are not included in the **Total Issues** value shown in the **Version Progress** section of the expandable pane of the OVERVIEW page. Suppressed issues are also not included in the calculation of application version metrics. For information about how to suppress an issue, see "Auditing Scan Results" on page 340. For information on how to see suppressed issues, see "Setting Issue Viewing Preferences" on the next page.

Removed issues

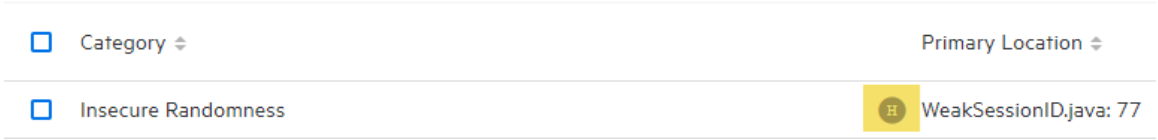
As multiple scans are run on an application over time, issues are often remediated or become obsolete. As Fortify Software Security Center merges scan results, it marks issues that were uncovered in a previous scan, but are no longer evident in the most recent analysis results as *Removed*.



Removed issues are not included in the **Total Issues** value shown in the **Version Progress** section of the expandable pane on the OVERVIEW page. For information on how to see removed issues, see "Setting Issue Viewing Preferences" below.

Hidden issues

In Fortify Audit Workbench, users typically hide a group of issues temporarily so that they can focus on other issues. For example, you might hide all issues except those assigned to you.



For information on how to see hidden Issues, see "Setting Issue Viewing Preferences" below.

Setting Issue Viewing Preferences

You can set certain viewing preferences for individual application versions from the Application Profile dialog box.

Viewing Suppressed Issues

To view the suppressed issues associated with an application version:

1. From the Dashboard or Applications view, select the version for the application version you are interested in.

   Fortify Software Security Center opens the AUDIT page for the selected version.
2. On the application version toolbar, click **PROFILE**.

   The APPLICATION PROFILE dialog opens to the **ADVANCED OPTIONS** tab.

Below the check boxes, the **Issue counts by state, based on current selections** shows the number of hidden, suppressed, and removed issues in the database associated with the selected application version.

Note: The filter set you select does not affect the number of suppressed issues shown. For example, if a suppressed issue is hidden in the selected filter set, it is still included in the count of suppressed issues.

3. Select the **Show suppressed issues** check box.
4. Click **APPLY**, and then click **CLOSE**.

Now, the AUDIT page displays all suppressed issues. Each suppressed issue is tagged with an "S" icon in the **Primary Location** column.

Viewing Removed Issues

When Fortify Software Security Center merges uploaded scan results, it removes issues that were uncovered in the previous analysis but are no longer evident in the most recent results.

To view the issues that were removed for an application version:

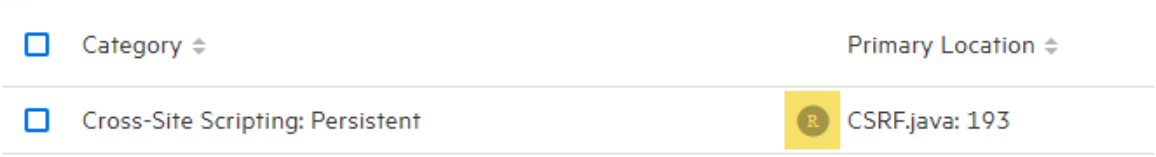
1. From the Dashboard or Applications view, select the version name for the application version you are interested in.

   Fortify Software Security Center opens the AUDIT page for the selected version.
2. On the application version toolbar, click **PROFILE**.

   The APPLICATION PROFILE dialog opens to the **ADVANCED OPTIONS** tab.

   Below the check boxes, the **Issue counts by state, based on current selections** shows the number of hidden, suppressed, and removed issues in the database associated with the selected application version.

   Note: The filter set you have selected does not affect the number of removed issues shown. For example, if a suppressed issue is hidden in the selected filter set, it is still included in the count of removed issues.
3. Select the **Show removed issues** check box.
4. Click **APPLY**, and then click **CLOSE**.



Now, the AUDIT page displays all removed issues. Each removed issue is tagged with an "R" icon in the **Primary Location** column.

Viewing Hidden Issues

In Fortify Software Security Center, hidden issues are the issues that are not shown because of the filter set rules currently in effect.

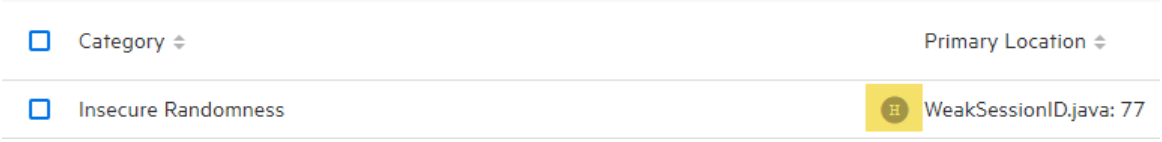
To reveal any hidden issues associated with an application version:

1. From the Dashboard or Applications view, select the version for the application version you are interested in.

   Fortify Software Security Center opens the AUDIT page for the selected version.
2. On the application version toolbar, click **PROFILE**.

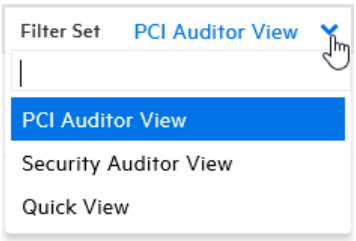
   The APPLICATION PROFILE dialog opens to the **ADVANCED OPTIONS** tab.

   Below the check boxes, the **Issue counts by state, based on current selections** shows the number of hidden, suppressed, and removed issues in the database associated with the selected application version.
3. Select the **Show hidden issues** check box.
4. Click **APPLY**, and then click **CLOSE**.



Now, the AUDIT page displays all hidden issues. Each hidden issue is tagged with an "H" icon in the **Primary Location** column.

Changing Displayed Issues Using Filter Sets



Note: The filter sets listed depend on the issue template assigned to the application version. The three filter sets shown here are included in the issue templates that Fortify provides. However, you can use other issue templates that have different filter set names and filter conditions.

Fortify Software Security Center provides the following filter sets for changing the display of application version issues on the OVERVIEW, AUDIT, and OPEN SOURCE pages:

- Quick View

  The Quick View filter set provides a view of issues in the Critical folder (these have a potentially high impact and a high likelihood of occurring) and the High folder (these have a potentially high impact and a low likelihood of occurring). This filter set provides a useful first look at results that enables you to quickly address the most pressing issues.

- Security Auditor View

  This view reveals a broad set of security issues to be audited. The Security Auditor View filter contains no visibility filters, so all issues are shown.

- PCI Auditor View

  This view is defined for individuals responsible for auditing an application with respect to its compliance with Payment Card Industry Security Standards.

Overriding Assigned Issue Priority

When scan results are parsed and loaded into Fortify Software Security Center, the scan parser for each supported engine type assigns a priority value to each issue. However, this priority value does not reflect the full context of the affected code or application. Other factors that concern the use of the affected code may justify assigning a different priority. For example, a vulnerability assigned the "critical" priority value may be better classified as "medium" or "low" priority if the section of code in question is never invoked in the application, or if the application is intended for use exclusively by a small department and has no connections to other applications and systems, so the identified vulnerability would have a low likelihood of being exploited. To enable such a use case, Fortify Software Security Center provides the capability for trusted users to change the priority originally assigned to an issue. Such priority changes are reflected in generated reports.

Caution! Enabling or disabling this feature must be considered as a long-term change in that it affects generated reports, computed metrics, and so on, depending on the data in the system. Make sure that, before you enable or disable it, you discuss the planned change with your security lead.

Enabling and Disabling Priority Override Capability on Fortify Software Security Center

You can enable priority overrides on your system either during a new deployment of Fortify Software Security Center, or on an existing Fortify Software Security Center instance.

Enabling the Priority Override Capability

To enable the priority override capability:

1. In the left pane of the ADMINISTRATION view, select **Configuration**, and then select **Issue Audit**.
2. Select the **Enable priority override** check box.
3. Click **SAVE**.
4. Restart the server.

After server restart, the feature is enabled and is applied to all application versions. On the AUDIT page, the issue details (AUDIT tab) now includes the **PRIORITY OVERRIDE** list tag.

Enabling Trusted Users to Override Issue Priority

To enable your users to make use of this functionality, create a new user role for them that includes the "Edit restricted custom tag values" permission. Grant these roles only to trusted users who have the knowledge and diligence to accurately assess issue priority. For information about how to create a user role, see "Creating Custom Roles" on page 223.

Note: Any user roles with permission to edit restricted custom tag values can override issue priority. (The system-defined Security Lead role already has the ability to edit restricted custom tags.)

Disabling the Priority Override Capability

To disable the priority override capability:

1. In the left pane of the ADMINISTRATION view, select **Configuration**, and then select **Issue Audit**.
2. Clear the **Enable priority override** check box.
3. Click **SAVE**.
4. Restart the server.

After server restart, the feature is disabled system-wide, and the **PRIORITY OVERRIDE** list tag is no longer visible in the issue details.

Overriding Priority Values During an Audit

To override the priority value for an issue during an audit:

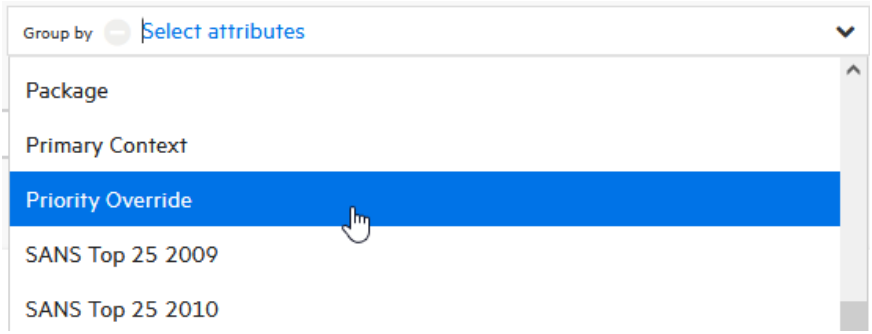
1. On the AUDIT page, expand the row that contains the issue.
2. On the **AUDIT** tab in the right pane, from the **PRIORITY OVERRIDE** list, select the preferred priority value.
3. (Required) In the box outlined in red below the list, type a comment to explain why you changed the value.

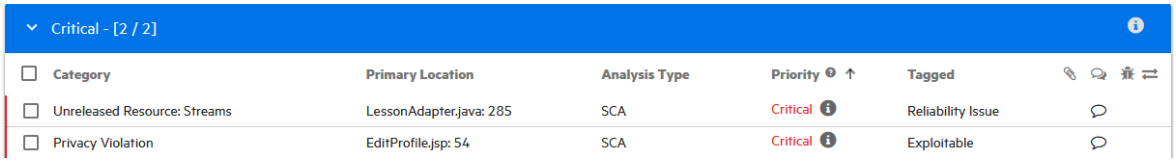
   Note: If you want to undo the override *before* you save the audit, click **UNDO** at the bottom of the pane.

4. To save the new priority value and associated comments, click **SAVE**.

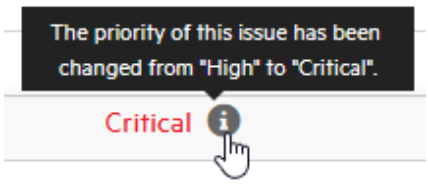
Viewing Issues That Have Changed Priority Values

To view issues that have priority values that you and others have manually assigned, from the **Group by** list, select**Priority Override**.





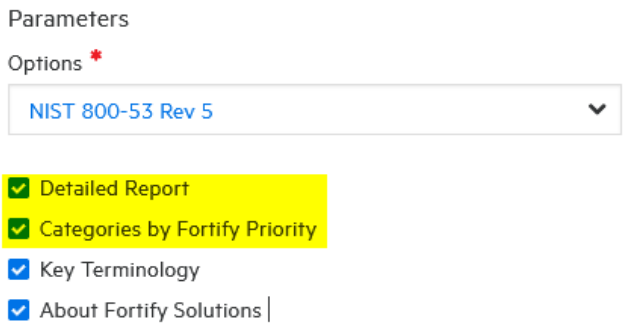
The issues table lists issues with overridden priorities, grouped by PRIORITY OVERRIDE tag value. Issues with unchanged priority values are grouped under **Not Set**.



To see how the **Priority** value was changed, hover your cursor over the information icon.

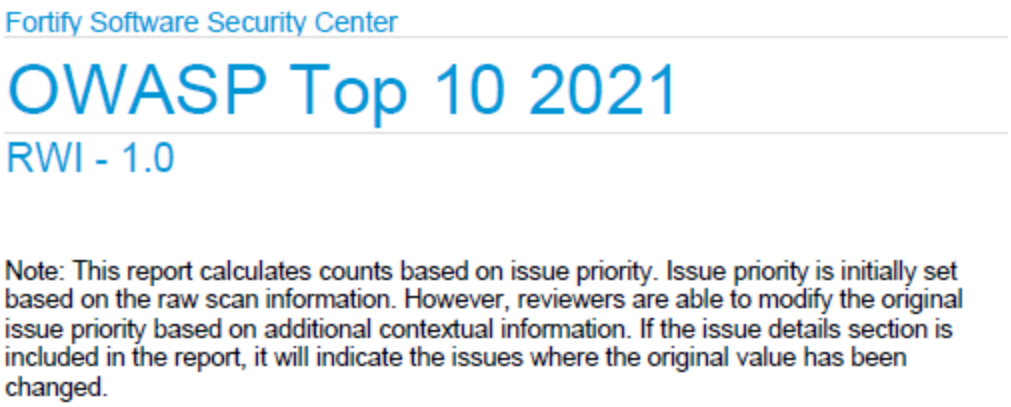
Viewing Priority Override Information in Issue Reports

If the priority override tag was used in auditing an application version, you can include the information in the issue reports you generate.

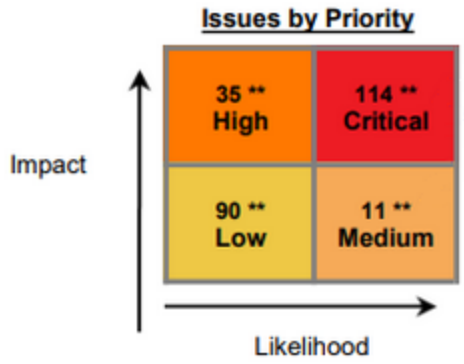


To include priority override information in a new issue report, as you specify the parameters for the report, leave the **Detailed Report** and **Categories by Fortify Priority** check boxes selected.

If an issue report includes issues that have overridden priority values (and have **Detailed Report** and **Categories by Fortify Priority** options selected), a note to that effect is displayed on the cover page, as shown here:



If the priority override feature is used, and the **Detailed Report** and **Categories by Priority** parameters are selected (either manually or by default), the **Issues by Priority** cube in the **Executive Summary** displays a double asterisk where issues have changed priority values.



The **Issue Details** sections of these reports show the current priority values, along with the original priority values.

Path Manipulation ***Remediation Effort(Hrs): 0.5***		**Low** **Original: Critical**
Package: com.order.splc		
Location	**Analysis Info**	**Analyzer**
WEB-INF/src/java/com/order/splc/ConnFactory.java:20 Priority Override: Low Analysis: Not an Issue	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** ConnFactory() **Source:** java.lang.System.getProperty() **from** com.order.splc.ConnFactory.ConnFactory() **In** WEB-INF/src/java/com/order/splc/ConnFactory.java:16	SCA
WEB-INF/src/java/com/order/splc/ConnectionFactory.java:30 Priority Override: Low Analysis: Not an Issue	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** ConnectionFactory() **Source:** java.lang.System.getProperty() **from** com.order.splc.ConnectionFactory.ConnectionFactory() **In** WEB-INF/src/java/com/order/splc/ConnectionFactory.java:26	SCA

Reverting to Original Priority Values

If you overrode the originally-assigned priority value for an issue, and then saved it, but you now want to revert the priority value to its original value:

1. On the AUDIT page, expand the row that contains the issue.
2. To the right of the **PRIORITY OVERRIDE** list tag, click the revert icon ( ).
3. (Required) In the box outlined in red below the list, type a comment to explain why you changed the value.
4. To save the new priority value and associated comments, click **SAVE**.

Reports reflect the current effective priority value, whether that is the original priority set by the engine (if unmodified) or the overridden value. If a user changed the priority value, those reports show the changed value. If not, the reports show the original priority.

Viewing Bugs Submitted for Issues

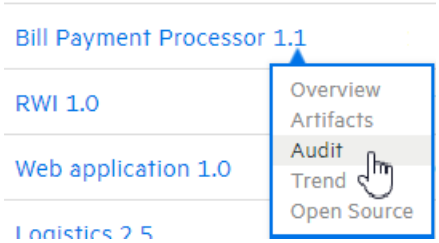
The issues table on the AUDIT page includes a **Bug submitted** column that shows whether a bug has been submitted against a listed issue.

To view the bug, click the **VIEW BUG** icon, and log in to the assigned bug tracking application.

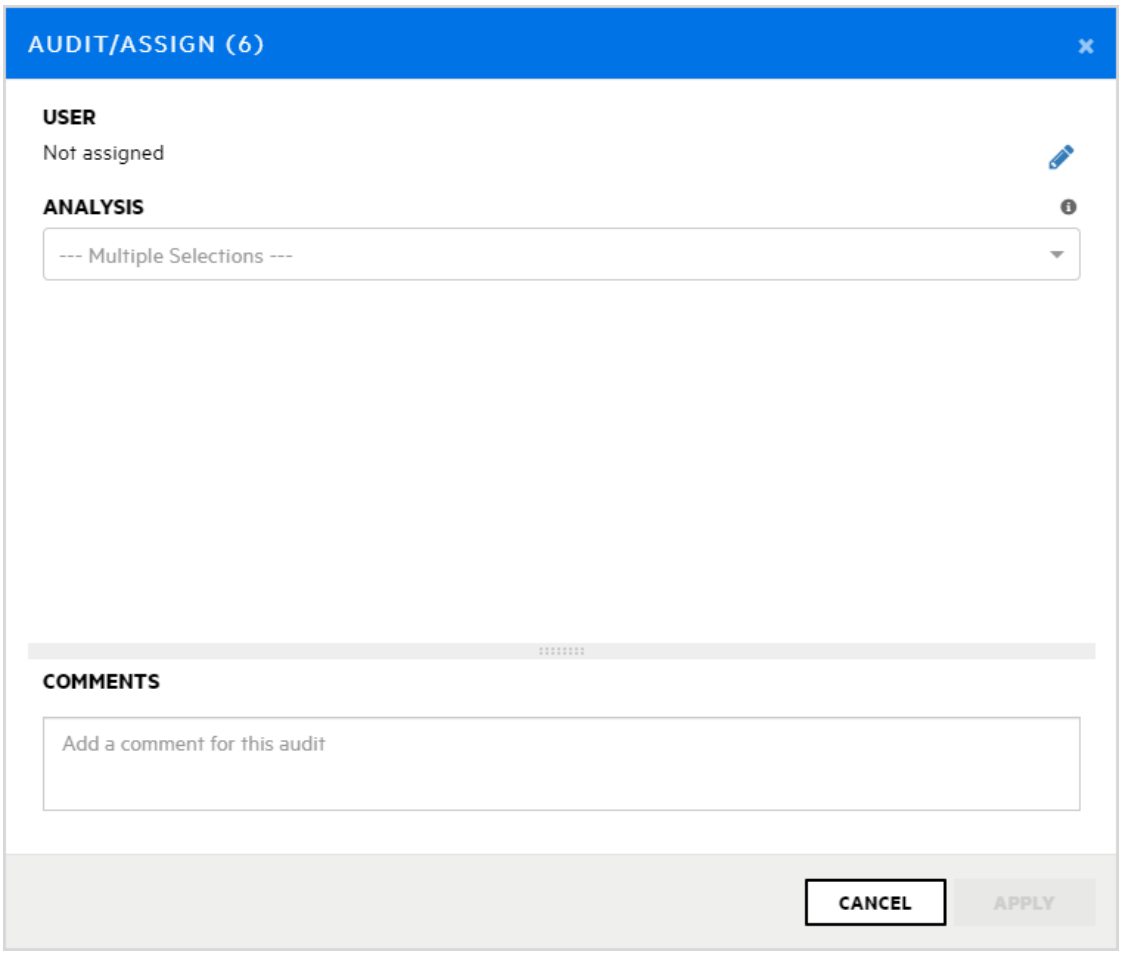
Tip: To view a bug, you must use a browser supported by the bug tracker application.

Auditing a Batch of Issues

To audit multiple issues at a time for an application version:



1. Open the AUDIT view for the application version.
2. In the issues list, select all of the check boxes for the issues you want to include in the batch audit.
3. Click **AUDIT**.



The AUDIT/ASSIGN dialog box opens.

4. To assign a user to the selected issues:
   a. To open the SELECT USER dialog box, select the **Edit assigned user** icon .
   b. To locate a user to assign to these issues, in the **Find user** box, type part or all of a user's name, and then click **FIND**.
   c. In the list of returned names, click the name of the user to assign.
   d. Click **DONE**.

      The **USER** section now displays the selected user name and avatar (if available).
5. From the **ANALYSIS** list, select a value that reflects your assessment of this batch of issues.
6. (Optional) In the **COMMENTS** box at the bottom, type a comment about this issue audit.
7. Click **APPLY**.

See Also

"Auditing Scan Results" on page 340

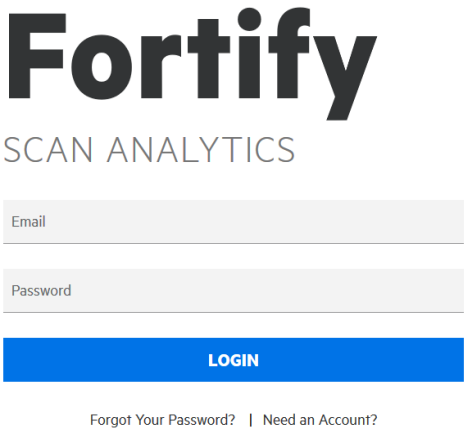
Using Audit Assistant

The following sections provide information about Audit Assistant workflow, prediction policies and how to use them, how to enable metadata sharing, how to submit data to Audit Assistant, and how to review Audit Assistant results.

Audit Assistant Workflow

The workflow for using Audit Assistant is as follows:

1. Obtain a Fortify Scan Analytics account, as follows:
   a. Go to https://analytics.fortify.com.



   b. Click **Need an Account?**
   c. Complete the fields on the Request a Fortify Scan Analytics Tenant form, and then click **Request Now**.

   Fortify sends an email with information about how to connect to Fortify Scan Analytics.
2. From Fortify Scan Analytics, create one or more policies.
3. (Optional) Choose to share anonymous metadata.
4. Obtain a Fortify Scan Analytics token.
5. From Fortify Software Security Center:
   - Configure and test the connection to Fortify Scan Analytics and then, on the Audit Assistant Configuration page, click **REFRESH POLICIES** to populate the **Default prediction policy** list (see "Configuring Audit Assistant" on page 90).
   - Specify a default prediction policy.
   - (Optional) Enable Audit Assistant to automatically send unaudited issues to Fortify Scan Analytics for prediction.

- (Optional) Enable Audit Assistant to automatically apply predicted values to custom tags.

6. From Fortify Software Security Center, open an application version, and submit the latest completely audited scan to Audit Assistant. This step is referred to as *training*.
7. From Fortify Software Security Center, open an application version and submit its Fortify Static Code Analyzer scan results to Audit Assistant.
8. After Audit Assistant completes its assessment, view those results and, if necessary, adjust them.
9. Submit corrected results to Audit Assistant.

The following sections describe how to obtain an authentication token from Fortify Scan Analytics, and then use that token to configure a connection to Fortify Scan Analytics. Later sections describe how to prepare Scan Analytics for metadata submission, submit data, review Audit Assistant results, and then submit corrected audit data.

See Also

"About Prediction Policies" below

"Defining Prediction Policies" on the next page

"Configuring Audit Assistant" on page 90

"Enabling Auto-Apply and Auto-Predict for an Application Version" on page 253

"Enabling Metadata Sharing" on page 363

"Submitting Training Data to Audit Assistant" on page 363

"Reviewing Audit Assistant Results" on page 364

About Prediction Policies

To use Audit Assistant to process your scan results, you must first define at least one *prediction policy* in Fortify Scan Analytics. Prediction policies determine the confidence thresholds that Audit Assistant (and Fortify Scan Analytics) uses to determine which issues to treat as indeterminate - that is, neither a true issue nor a non-issue.

Note: During Audit Assistant configuration, the administrator selects a default global prediction policy, which Scan Analytics uses for the application version if no prediction policy is specified for that application version. If a prediction policy is specified for an application version, then Scan Analytics uses that policy to assess issues.

See Also

"Defining Prediction Policies" on the next page

"Configuring Audit Assistant Options for an Application Version" on page 273"Configuring Audit Assistant" on page 90

"Configuring Audit Assistant" on page 90

"About Audit Assistant Auto-Prediction" on page 92

Defining Prediction Policies

To use Audit Assistant, you must define at least one prediction policy that Audit Assistant can use to determine which issues to treat as indeterminate (neither a true issue nor a non-issue). For more information, see "About Prediction Policies" on the previous page.

To define a prediction policy:

1. Log in to Fortify Scan Analytics (https://analytics.fortify.com).
2. On the Fortify header, select **PREDICTION POLICIES**.
3. On the Prediction Policies page, click **+ADD**.
4. In the **Policy Name** box on the Prediction Policies > Add page, type a name for the policy.

   The Prediction Policies | Add page contains two confidence threshold settings. You use these to configure which issues Audit Assistant is to treat as indeterminate - that is, neither a true issue nor a non-issue.

   Audit Assistant results include the following:

   - The **AA_Prediction** value groups issues based on Audit Assistant's assessment of their exploitability. Possible values are **Exploitable**, **Below Threshold – Exploitable**, **Not an issue**, **Below Threshold – Not an issue** and **Not Predicted**.

     Note: Audit Assistant only predicts on dataflow and control flow static analysis issues.

   - The **AA_Confidence** value (percentage value that ranges from 0.00 to 1.00) shows Audit Assistant's level of confidence in the **AA_Prediction** value.

   If the **AA_Confidence** value falls below either of the confidence thresholds you set here for the prediction policy, then Audit Assistant treats the issue as indeterminate, and assigns it the **AA_Prediction** value **Not Predicted**.
5. Set the **Confidence Threshold - Not an Issue** and the **Confidence Threshold - Exploitable** sliders to acceptable levels for the applications on Fortify Software Security Center.

   Note: The higher you set the threshold values, the less likely it is that the Audit Assistant results contain false negatives. (Tests using the default 80% threshold values result in false negative occurrence of less than one percent.)

6. (Optional) In the **Description** box, type a policy description.
7. Click **SAVE**.

See Also

"About Prediction Policies" on page 361

"Configuring Audit Assistant" on page 90

"Configuring Audit Assistant Options for an Application Version" on page 273

Enabling Metadata Sharing

You can contribute your audit metadata to the Fortify Community Intelligence data set (pool of anonymous auditing metadata from Fortify users). If you do, you can take advantage of the Fortify Community Intelligence data pool to assess your own data. Otherwise, Audit Assistant restricts the metadata it uses to assess your issues to just the training metadata you submit.

Note: If you submit no training data *and* you do not enable metadata sharing, then Fortify Scan Analytics Fortify Scan Analytics assesses no issues.

To enable data sharing:

1. Log in to Fortify Scan Analytics (https://analytics.fortify.com).
2. In the left pane, select **Settings**.
3. Select the **Share anonymous issue metrics** check box.
4. Click **Save**.

See Also

"Configuring Audit Assistant" on page 90

"About Prediction Policies" on page 361

Submitting Training Data to Audit Assistant

The following procedure describes how to submit training data to Audit Assistant for assessment. Keep in mind that all data transferred from the Fortify Software Security Center environment is anonymized and contains no sensitive information. Also, be aware that only the primary custom tag for an application version is included in the data sent to Audit Assistant for training.

To submit training data to Audit Assistant:

1. From the Dashboard, open the OVERVIEW, ARTIFACTS, AUDIT or TREND page for the application version of interest.
2. On the application version toolbar, click **PROFILE**.

3. In the APPLICATION PROFILE dialog box, click the **AUDIT ASSISTANT TRAINING** tab.

   Note: The **AUDIT ASSISTANT TRAINING** tab is visible only if an administrator has configured Audit Assistant integration with Fortify Software Security Center. For information about Audit Assistant configuration, see "Configuring Audit Assistant" on page 90.

   The **Data last sent for training** field shows the date and time training data for the application version was last submitted.
4. To submit new training data, click **SEND FOR TRAINING**.

   The **Data last sent for training** field displays the **Sending** status.
5. After the **Data last sent for training** field is refreshed with the updated date and time, close the APPLICATION PROFILE dialog box.
6. On the application version toolbar, click **ARTIFACTS**, and then check to see whether the **Status** field for your upload is **Processing Complete**.

After processing is completed, you can view the results from the AUDIT page. For instructions, see "Reviewing Audit Assistant Results" below.

See Also

"About Audit Assistant" on page 88

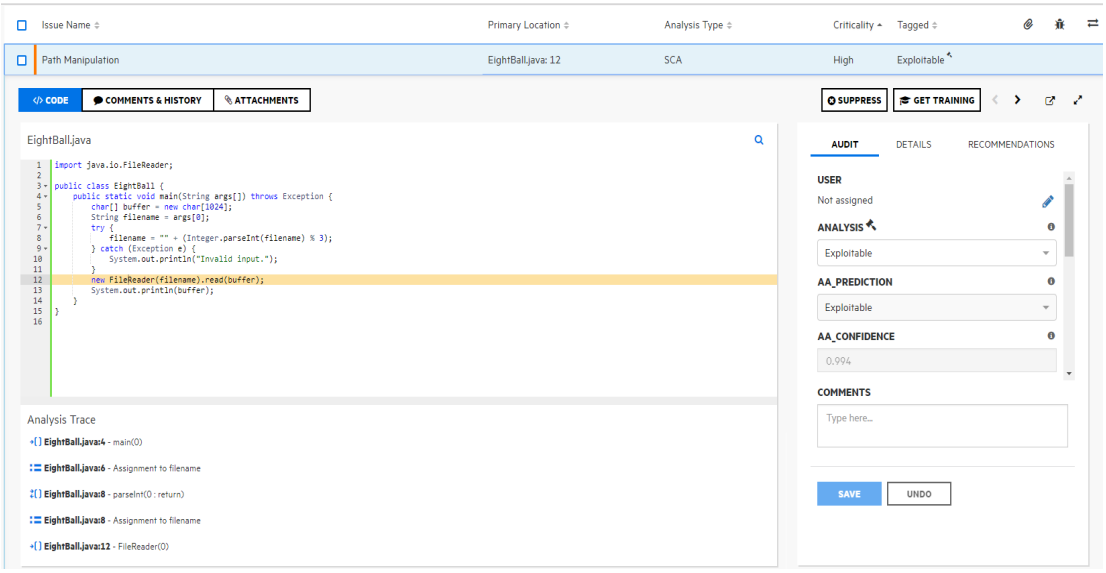
"Enabling Auto-Apply and Auto-Predict for an Application Version" on page 253

Reviewing Audit Assistant Results

After you submit scan results to Audit Assistant and Audit Assistant finishes its assessment of the issues, you can examine the results.

To view Audit Assistant results:

1. Navigate to the AUDIT page for the application version.
2. Use the Fortify Priority risk links, the **Group by** list, and **Filter by** lists to display the issues you want to audit. (See "Viewing Issues Based on Folders" on page 330 and "Filtering Issues for Display on the OVERVIEW and AUDIT Pages" on page 332.)
3. In the issues table, if you have selected a grouping, expand a group to view the issues it contains.
4. To expand an issue and view its details, click its row in the table.



5. In addition to the Analysis tag and any other custom tags associated with the application version, the right pane displays:
   - **AA_PREDICTION** - Exploitability level that Audit Assistant assigned to the issue.
   - **AA_CONFIDENCE** - Audit Assistant's level of confidence in the accuracy of its **AA_PREDICTION** value. This is a percentage, expressed in values that range from 0.000 to 1.000. For example, the value 0.982 Indicates a confidence level of 98.2 percent.
6. If your exploitability assessment agrees with the **AA_Prediction** value displayed, you can select the value that corresponds to the AA assessment from the list of custom tag values. Otherwise, select a different custom tag value.
7. Click **SAVE**.

See Also

"About Audit Assistant" on page 88

"Auditing Scan Results" on page 340

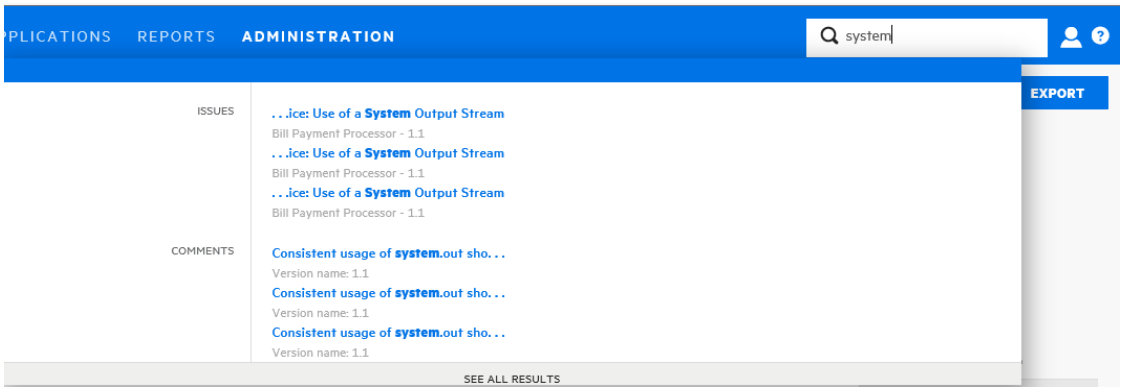
Searching Globally in Fortify Software Security Center

Regardless of where you are in the Fortify Software Security Center user interface, you have access to the global **Search** field on the Fortify header. Any search string you type here is applied across all application versions, issues, reports, comments, and users.

Note: The search box is visible only if **Enable global search** was selected during Fortify Software Security Center setup. For more information, see "Configuring Fortify Software Security Center for the First Time" on page 72.

To use the global **Search** field:

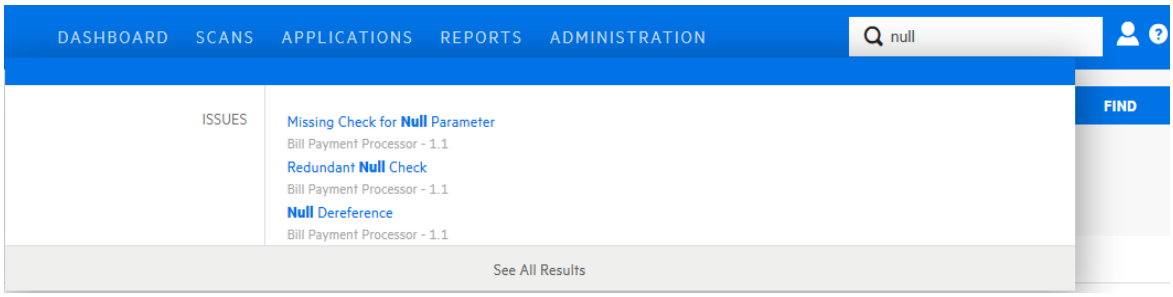
1. From any view, type a search string into the **Search** box.



   Fortify Software Security Center displays the first several items that match your search string, grouped by category. The application version is also displayed.
2. To go to a specific item listed, click the item.

   Fortify Software Security Center opens the user interface where you can view or work on the item.
3. To see a list of all search results, below the listed items, click **See All Results**.

Example: Finding issues



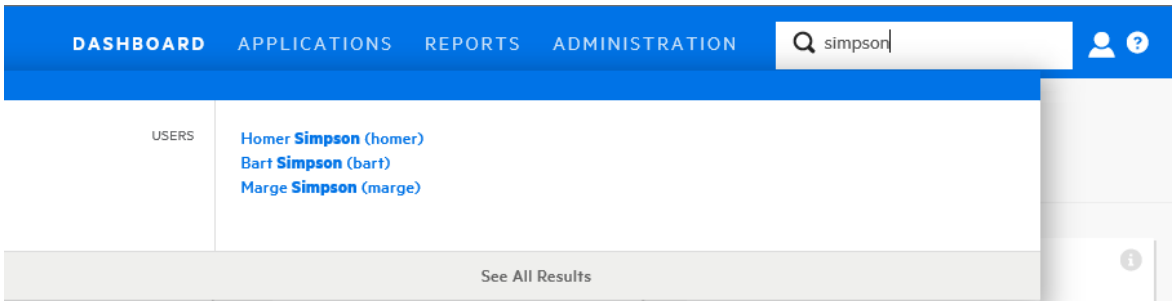
After you select an issue from the listed results, Fortify Software Security Center takes you to the corresponding version page with the issue expanded to full view.

If you select **See All Results**, Fortify Software Security Center takes you to the Search Results page. From here, you can open the first match with the issue expanded to full view. From there, you can use the next and previous buttons to page through all of the findings.

Note: The search results for issues may include removed, hidden or suppressed issues. If the AUDIT page does not display an item you selected, check the

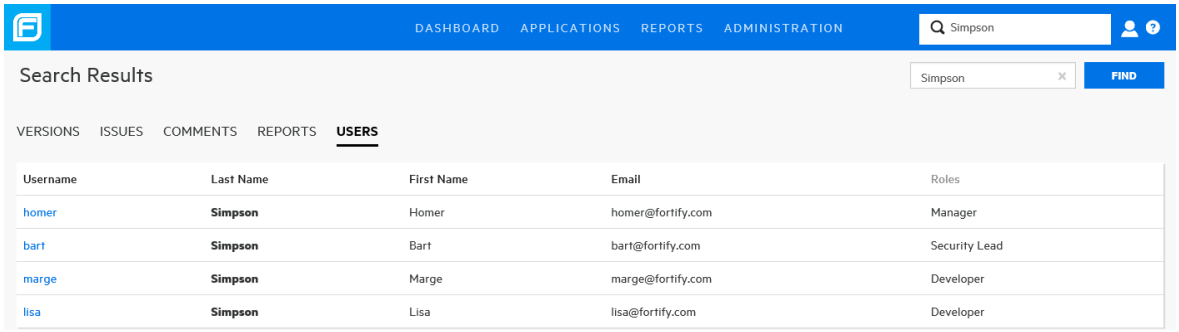
viewing preferences set for the application version to make sure that you have the appropriate flags enabled on the **ADVANCED OPTIONS** tab to display removed, hidden, and suppressed issues. For instructions, see "Setting Issue Viewing Preferences" on page 350.

Example: Finding users



After you select a single user from the listed results, assuming you have the required permission, Fortify Software Security Center takes you to the details for the user account in the ADMINISTRATION view.

If you select **See All Results**, Fortify Software Security Center takes you to the **Search Results** page.



See Also

"Searching Applications and Application Versions from the Applications View" on page 254

Viewing Open Source Data

After you download, install, and enable the Debricked or Sonatype parser plugin for Fortify Software Security Center (see "Preparing Fortify Software Security Center to Display Debricked Results" on page 177 and "Preparing Fortify Software Security Center to Display Sonatype Results" on page 175), you can view the open source vulnerability data uploaded to Fortify Software Security Center for an application

version. You can view the results uploaded for an application version either from the AUDIT page, or from the OPEN SOURCE page.

Viewing Open Source Data from the AUDIT Page

To view open source vulnerability results from the AUDIT page:

1. On the Fortify header, click **APPLICATIONS**.
2. In the Applications view, expand the row for the application of interest, and then select the version for which results have been uploaded.
3. From the **Group by** list on the AUDIT page, select **Analysis Type**.
4. Expand the **DEBRICKED** or **SONATYPE** header, and then expand the row for a result you want to examine.

For detailed information about how to interpret Debricked vulnerability data displayed, see the Debricked documentation (https://debricked.com/docs). For information about how to interpret Sonatype vulnerability data displayed, see the Sonatype documentation.

Auditing Open Source Results

For information about how to audit open source results, see "Auditing Scan Results" on page 340.

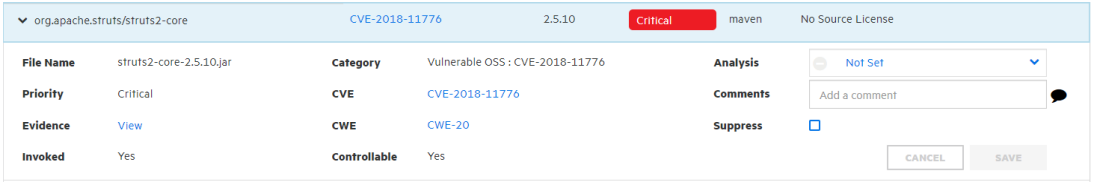
Viewing Open Source Data from the OPEN SOURCE Page

To view open source results from the OPEN SOURCE page:

1. On the Fortify header, click **APPLICATIONS**.
2. On the Applications page, select the application version for which open source results have been uploaded.
3. On the AUDIT page header, click **OPEN SOURCE**.

   Note: The OPEN SOURCE page is visible only if open source results have been uploaded for the selected application version.

4. In the **OPEN SOURCE COMPONENTS** table, click the row for an issue you want to examine.



The following table contains descriptions of the details shown.

Field	Description
File Name	Name of the component file in which the issue was discovered.
Category	OSS index category: Common Vulnerabilities and Exposures ID
Analysis (or other assigned primary tag)	If you audit the issue from the OPEN SOURCE page, you can select a primary tag value to assign from this list.
Priority	Fortify priority rating
CVE	CVE (Common Vulnerabilities and Exposures) ID number assigned to the vulnerability. Click the link to go directly to a highly detailed description of that vulnerability on the CVE site.
Comments	If you audit the issue from the OPEN SOURCE page, you can add comments here.
Evidence	A link to any evidence if the vulnerability is invoked or controllable.
CWE	Common Weakness Enumeration. Click this link (if present) to go to the Common Weakness Enumeration website and see details about the software weakness type uncovered.
Suppress	Select this check box if you think that the issue is not of concern. For more information about issue suppression, see "About Suppressed, Removed, and Hidden Issues" on page 349.
Invoked	This field shows whether the issue was invoked in the code.
Controllable	This field shows whether or not user-controlled input reaches the method or function.

For detailed information about how to interpret the Debricked vulnerability data displayed, see the Debricked documentation (https://debricked.com/docs).

See Also

"Preparing Fortify Software Security Center to Display Debricked Results" on page 177

About Susceptibility Analysis of Web Applications

Susceptibility analysis is a feature co-developed by Fortify and Sonatype. It takes into account known vulnerabilities that Sonatype reveals about a web application, and which are a part of your application's classpath. It determines whether you have actually invoked or allowed user-controlled input to reach the function or method, which indicates that your code is truly vulnerable to the publicly-exposed issue. Susceptibility analysis determines whether you are actually susceptible to the vulnerability described, and not simply that you have that dependency in your collection of your libraries for an application.

Sonatype checks to see if a vulnerable component has a non-vulnerable version to which it can be upgraded. If it does, it writes a signature for the function or method. Fortify Software Security Center then takes this signature and checks to determine whether this function is called or whether user-controlled input reaches this function. If the function is invoked, Fortify Software Security Center labels it as "invoked." If user-controlled input reaches this function, Fortify Software Security Center labels it as "controllable." After you audit your Sonatype data, you can prioritize upgrading any open-source component with a vulnerability proven to exist in your application over one for which there is no evidence of exploitability. Running susceptibility analysis scans on your web application code markedly improves the results you see in Fortify Software Security Center.

Susceptibility Analysis Requirements

To perform susceptibility analysis on your web applications, in addition to Fortify Software Security Center you must have:

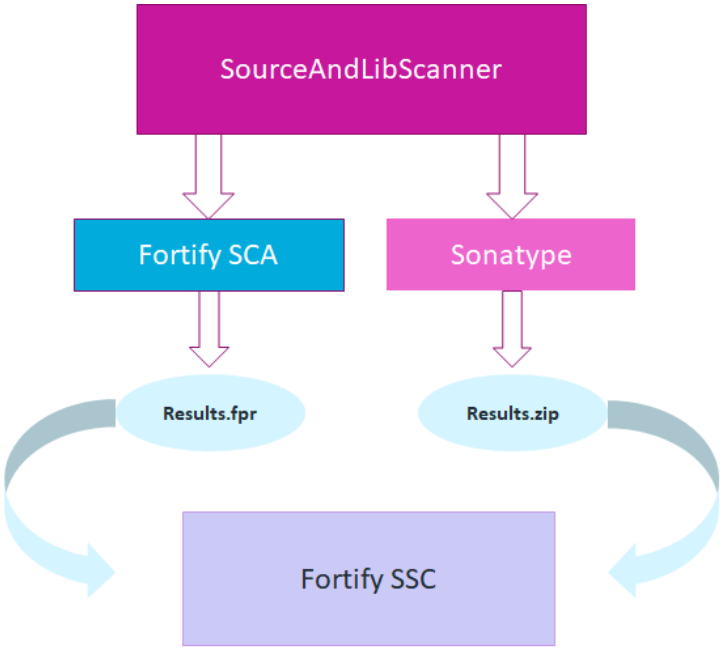
- Fortify Static Code Analyzer
- Sonatype plugin for Fortify Software Security Center

  For instructions on how to download and configure the plugin, see "Preparing Fortify Software Security Center to Display Sonatype Results" on page 1.)
- Fortify SourceAndLibScanner

  To obtain SourceAndLibScanner, go to https://marketplace.microfocus.com/cyberres/content/fortify-sourceandlibscanner.

  For information about the SourceAndLibScanner software requirements, and how to install and use the tool, see the*Fortify SourceAndLibScanner User Guide*, which is packaged with the SourceAndLibScanner utility.

Typical Workflow to Optimize Results for an Application



Steps to achieve the best scan results for an application are as follows:

1. Download and install the Sonatype plugin. (See "Preparing Fortify Software Security Center to Display Sonatype Results" on page 175.)
2. To obtain results that include susceptibility analysis findings (on the OPEN SOURCE page only), use SourceAndLibScanner to run a Sonatype scan that uncovers open-source component vulnerabilities in your application and to run a Fortify Static Code Analyzer scan of a web application version and upload the resulting FPR file to the application version on Fortify Software Security Center. For more information, see "About Susceptibility Analysis of Web Applications" on the previous page.

   For information about how to use the SourceAndLibScanner to perform a Fortify Static Code Analyzer scan and/or a Sonatype library scan, and then upload the results to Fortify Software Security Center, see the *Fortify SourceAndLibScanner User Guide*.
3. Upload the resulting ZIP file to the application version in Fortify Software Security Center.
4. Upload the resulting FPR file to the specified application version in Fortify Software Security Center.

   SourceAndLibScanner and Fortify Statics Code Analyzer provide the susceptibility analysis that corresponds to the open-source component vulnerabilities.

Note: The issues uncovered by a Fortify Static Code Analyzer scan initiated using SourceAndLibScanner are significant only in the context of the Sonatype findings. Because of this, they are hidden on the AUDIT page by default.

5. Audit the results from the OPEN SOURCE page. Although you can audit Sonatype issues from the AUDIT page, you can only see the results of susceptibility analysis on the OPEN SOURCE page, where they are represented by the **Invoked**, **Controllable**, and **Evidence** fields.

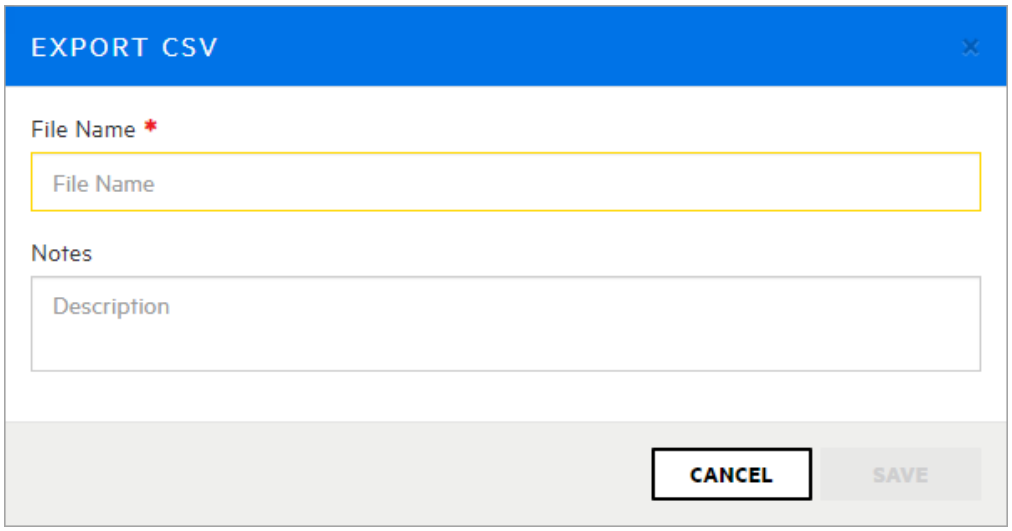
Exporting Open Source Data

To export open source data displayed on the OPEN SOURCE COMPONENTS page:

1. After you upload open source data for an application version in Fortify Software Security Center, go to the OPEN SOURCE COMPONENTS page for that application version.

2. To open the EXPORT CSV dialog box, above the OPEN SOURCE COMPONENTS table, click **EXPORT**.

3. In the **File Name** box, type the name for the CSV file to generate.
4. (Optional) In the **Notes** box, type any notes to associate with the generated file.
5. Click **SAVE**.
6. To view the exported result:
   a. On the Fortify header, click REPORTS.
   b. On the Reports page, click the DATA EXPORTS tab.

c. In the resulting table, move your cursor to the row for the exported file, and then click the Download icon .

In the resulting CSV file, open source fields are displayed as `<engine_type>.<field_name>`. For example, `SONATYPE.cweurl` corresponds to the Sonatype **CWE URL** field.

To determine how long the system retains your CSV files before deleting them, see the instructions provided in "Configuring Job Scheduler Settings" on page 135. The default expiration period for these reports is two days.

Integrating Fortify Software Security Center with Fortify WebInspect Enterprise

Fortify Software Security Center and Fortify WebInspect Enterprise are closely integrated and can share scan results. Administrators can also submit requests for WebInspect dynamic scans from the user interface. This section describes how to view Fortify Software Security Center WebInspect results in Fortify Software Security Center and provides instructions for Fortify Software Security Center users on how to request dynamic scans.

Viewing Fortify WebInspect Scan Results in Fortify Software Security Center

Fortify WebInspect saves scan results (results data and audit data) in FPR format, which you can upload to Fortify Software Security Center. (See "Uploading Scan Artifacts" on page 311.) Fortify WebInspect issue details differ somewhat from those shown for issues uncovered by other analyzers, such as Fortify Static Code Analyzer.

Important! To successfully integrate Fortify WebInspect with Fortify Software Security Center, you must install a trusted CA certificate on the Java Runtime environment on both the Fortify Software Security Center and WebInspect servers.

In the left pane of the **CODE** tab, the **Overview** section displays summary information about the finding and the **Implications** section. The **Additional References** section lists any pertinent references available.

The center pane displays the following information:

URL: Website page on which the vulnerability was detected

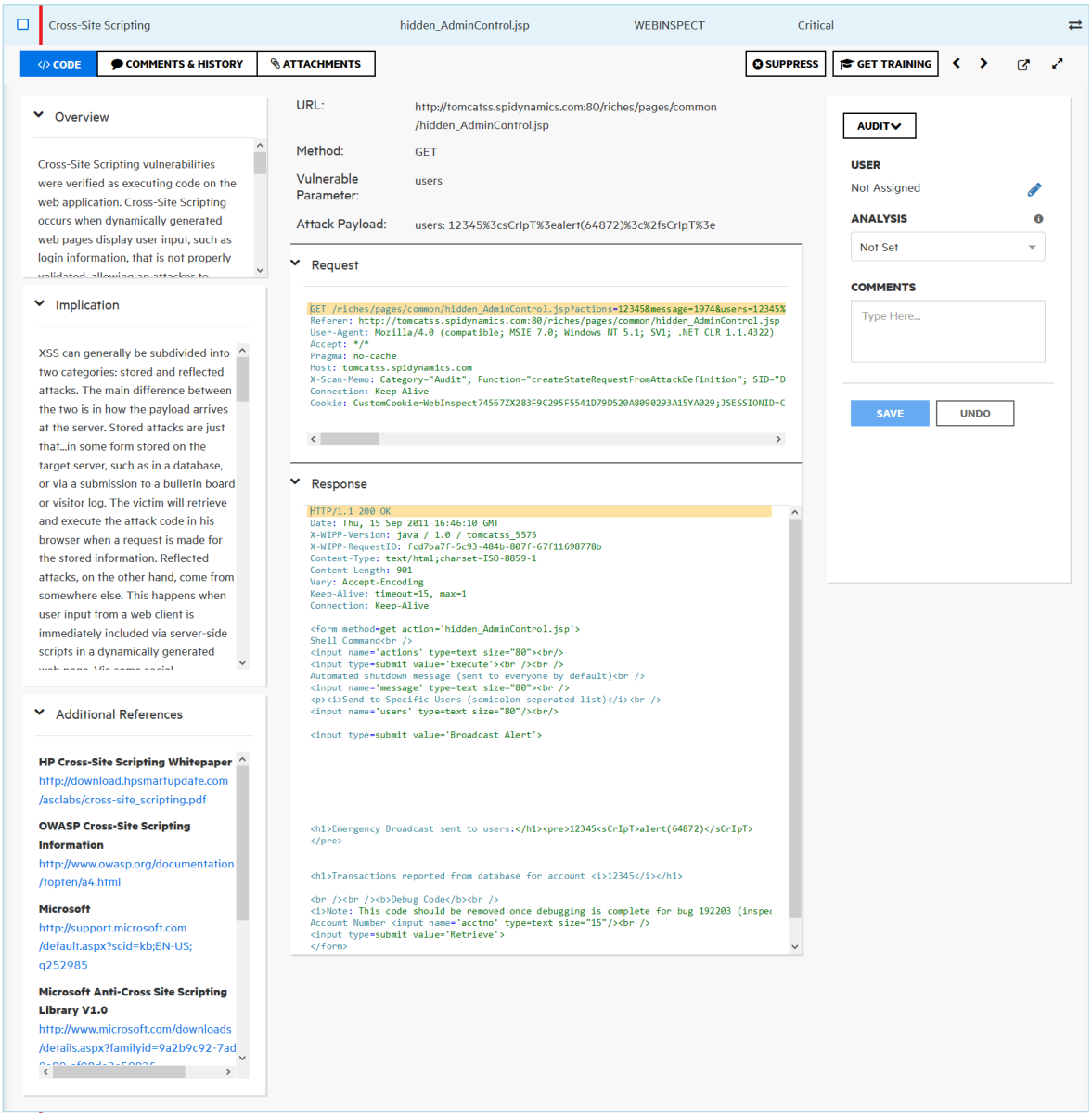
Method: HTTP method used for the attack (for example GET, PUT, and POST)

Vulnerable Parameter: Name of the vulnerable parameter

Attack Payload: Shellcode used as the payload for exploiting the vulnerability

Below this information, the **Request** section displays the request made, with the attack highlighted. The **Response** section displays the response to the request, with the trigger highlighted.

Note: If responses contain binary data or a large volume of data (more than 50 KB), you can see the **Download Response** button at the bottom of the **Response** section. To download responses such as these in a text file, click **Download Response**.



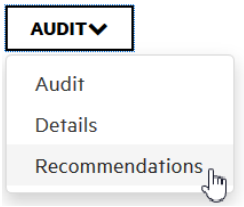
The **Steps** tab is available only if the steps are included in the WebInspect results file.

Viewing Additional Details and Recommendations

To view additional details and recommendations for the issue, on the issue toolbar, click one of the following:

- **Open in new tab**
- **Expand to full screen**

On the right, the **DETAILS** section provides suggestions on what to look for in this issue.



To view recommendations and tips on how to address the issue, from the **DETAILS** list, select **Recommendations**.

For information about how to use the pane on the right to audit the issue, see "Auditing Scan Results" on page 340.

WebInspect Audit Data

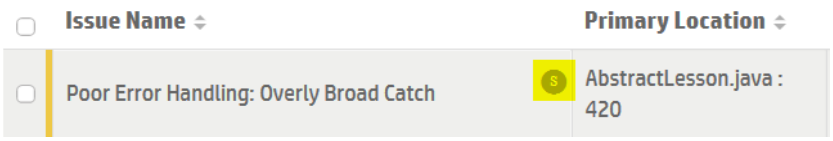
In addition to screen shots, the following types of audit data are transferred from WebInspect to Fortify Software Security Center:

- **Vulnerability Notes**. Vulnerability notes in WebInspect are transferred to Fortify Software Security Center as issue comments.
- **Ignored Vulnerabilities**. Vulnerabilities marked as “Ignored” in WebInspect are marked “Suppressed” upon transfer to Fortify Software Security Center.
- **False Positives**.

False Positives

Fortify Software Security Center does not have a direct equivalent of the Fortify WebInspect “false positive” status. If a Fortify WebInspect user marks a vulnerability as a false positive, the vulnerability is hidden from the vulnerability lists and is removed from the vulnerability counts.

To emulate the false positive status in Fortify Software Security Center, you can use the default **Analysis** custom tag. A Fortify WebInspect false positive is assigned the **Analysis** value “Not an Issue” in Fortify Software Security Center. To emulate the Fortify WebInspect behavior of hiding the issue from lists and counts, the issue is marked as **Suppressed**.



Note: If the selected value for **Analysis** has changed from "Not an Issue" or is missing, or if the **Analysis** list has been removed from your application version, then the false positive status of the issue is lost. The issue is marked as "Suppressed."

See Also

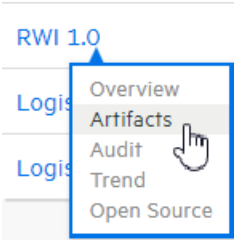
"Setting Issue Viewing Preferences" on page 350

Submitting Dynamic Scan Requests to Fortify WebInspect Enterprise

If WebInspect is installed in your environment, and you are assigned to one of the following roles, you can request WebInspect scans from Fortify Software Security Center:

- Administrator
- Security Lead
- Manager
- Developer

To create a scan request for an application version:



1. On the Dashboard, move your cursor to the application version that you want to have scanned, and then select **Artifacts** from the shortcut menu.
2. On the ARTIFACT HISTORY page, click **DYNAMIC SCAN**.
3. In the DYNAMIC SCAN - <*APPLICATION VERSION*> dialog box, provide the information described in the following table.

   Note: The following table does not list custom dynamic scan attributes that you or another Fortify Software Security Center administrator may have added to the system.

Dynamic Scan Attribute * (Required field)	Description
*URL	URL of the site to scan
Site Login	Username required to log on to the site to scan
Site Passcode	Password to use to gain access to the site
Network Login	Username required for network authentication
Network Passcode	Password required for network authentication
Related Host Name(s)	Allowable hosts for the application to scan
Web Services Used	Comma-delimited list of web services used by the application to scan
Technologies Used	Comma-delimited list of technologies used by the site to scan
Compliance Implications	Information about any potential compliance implications
Allowable Scan Times	Dates and times during which the tester can perform the scan **Example:** From 17:00 h to 06:00 h, Monday through Friday, from 09/03/18 to 11/30/18 You can run the scan immediately instead of scheduling it to run later. For instructions, see "Processing Dynamic Scan Requests from Fortify WebInspect Enterprise" on the next page.
WSDL	Browse to and select your Web Services Description Language file (*.wsdl, *.webmacro, or *.xml)

Note: The dynamic tester who handles the scan request on WebInspect may be interested in additional application version attributes, such as business risk and compliance implications. The tester can use existing web services methods to retrieve those attributes for an application version.

4. Click **SUBMIT**.

Fortify Software Security Center displays a message to verify that the request submission was successful.

Next, the WebInspect tester who monitors and responds to scan requests runs the scan during the hours you specified, and then uploads the results to Fortify Software Security Center.

5. If you are a Fortify Software Security Center Administrator or Application security tester, you can run the requested dynamic scan immediately from WebInspect Enterprise. For instructions, see "Processing Dynamic Scan Requests from Fortify WebInspect Enterprise" below.

See Also

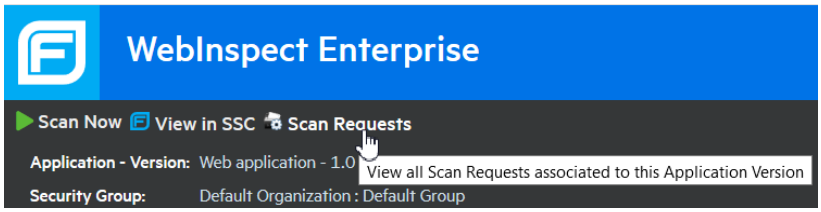
"Viewing Fortify WebInspect Scan Results in Fortify Software Security Center" on page 373

Processing Dynamic Scan Requests from Fortify WebInspect Enterprise

If you are in the role of Administrator or Application security tester, you can start Fortify WebInspect Enterprise, where you can view and process dynamic scan requests submitted by Fortify Software Security Center users.

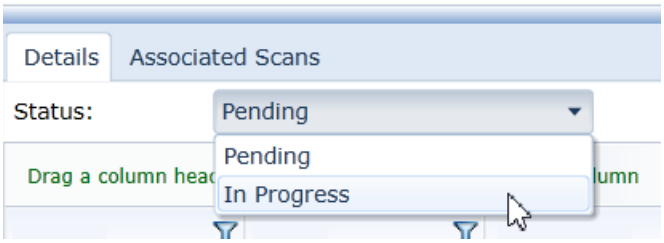
To process dynamic scan requests in WebInspect Enterprise:

1. From Fortify WebInspect Enterprise, initialize Fortify Software Security Center, and then use the WebInspect Enterprise Console to synchronize Fortify Software Security Center application versions with WebInspect projects. (For instructions, see the *Micro Focus Fortify WebInspect Enterprise User Guide*.)
2. On the Fortify Software Security Center Dashboard, move your cursor to an application version for which a dynamic scan has been requested, and then select **Artifacts** from the shortcut menu.
3. On the ARTIFACTS page, click **LAUNCH WIE**.



4. Under the Fortify WebInspect Enterprise header, click **Scan Requests**.

   The SCAN REQUESTS view lists all dynamic scan requests submitted from Fortify Software Security Center to Fortify WebInspect Enterprise.
5. Select the pending request.



6. In the lower pane, on the **Details** tab, from the **Status** list, select **In Progress**, and then click **Change Status**. In Fortify Software Security Center, users assigned to the application version can now see that the scan request is no longer pending.
7. At the top of the view, click **Create a Web Site Scan** and complete the steps in the Scan Wizard to run the scan and upload the results to Fortify Software Security Center. For detailed instructions, see the *Micro Focus Fortify WebInspect Enterprise User Guide*.

See Also

"Submitting Dynamic Scan Requests to Fortify WebInspect Enterprise" on page 376

Editing and Cancelling Dynamic Scan Requests

To view the current status of the last dynamic scan request submitted for an application version:

1. Navigate to the Issues tab on the details page for the application version for which you submitted a scan request.
2. From the **Dynamic Scan Request** list, select **Last Scan Status**.

Fortify Software Security Center displays the date and time the scan request was submitted, and request status information.

Dynamic Scan Request States

After you submit a dynamic scan request, (see "Submitting Dynamic Scan Requests to Fortify WebInspect Enterprise" on page 376) the request enters the PENDING state. As soon as the tester starts the scan from WebInspect, the request state is IN_PROGRESS. After the WebInspect tester completes the scan, the scan request enters the COMPLETED state.

As long as a dynamic scan request is pending, you can edit or cancel it. As soon as the scan is started, however, you can no longer edit or cancel it.

Editing Dynamic Scan Requests

To edit a dynamic scan request:

Note: You can edit only scan requests that you have submitted.

1. Navigate to the Issues tab on the details page for the application version for which you have requested a dynamic scan.
2. From the **Dynamic Scan Request** list, select **Edit**.
3. In the Dynamic Scan Request dialog box, edit the values for the dynamic scan attributes, and then click **Submit**.

Cancelling Dynamic Scan Requests

To cancel a pending dynamic scan request, do the following:

Note: You can cancel only scan requests that you have submitted.

1. Navigate to the Issues tab on the details page for the project version for which you have requested a dynamic scan.
2. From the **Dynamic Scan Request** list, select **Cancel**.
   Fortify Software Security Center prompts you to confirm that you want to cancel the last dynamic scan request.
3. Click **Yes**.

Chapter 16: Working with Fortify ScanCentral SAST

If Fortify Software Security Center is configured to communicate with Fortify ScanCentral SAST, then the **SAST** tab is enabled in the SCANCENTRAL view. The **SAST** tab displays the Scan Requests, Sensors, Controller and Sensor Pools pages. The following sections describe these pages and their functionality. For information about how to configure the connection between Fortify Software Security Center and ScanCentral SAST, see "Configuring ScanCentral SAST Monitoring in Fortify Software Security Center" on page 134.

Topics covered in this section:

ScanCentral SAST Permissions

The following table shows which Fortify Software Security Center roles have permission to perform which ScanCentral SAST-related tasks.

Note: For information about how to install, configure, and use Fortify ScanCentral SAST to streamline the static code analysis process, see the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

Roles	Permissions
View-Only	View ScanCentral SAST data, except for jobs not assigned to any application version. **Restrictions:** • Users see only the scan requests for application versions to which they are assigned • Users see only sensor pool assignment for the application versions to which they are assigned
Administrator Security Lead Manager	View information on the Scan Requests, Sensors, and Sensor Pools pages Performing all tasks that involve changes to sensor pools Cancel scan requests Assign sensors and application versions to sensor pools. **Restrictions:** • Users can cancel only those scan requests for application versions to which they are assigned. • Users can assign only application versions to which they are assigned to sensor pools.
Administrator	View, download, and manage ScanCentral SAST data
Security Lead	View, download, and manage ScanCentral SAST data, except for jobs not assigned to any application version **Restrictions:** • Users can cancel only those scan requests for application versions to which they are assigned. • Users can assign only application versions to which they are

	assigned to sensor pools.
Manager	View, download, and manage ScanCentral SAST data, except for jobs not assigned to any application version **Restrictions:** • Users can cancel only those scan requests for application versions to which they are assigned. • Users can assign only application versions to which they are assigned to sensor pools.
Developer	View ScanCentral SAST data, except for jobs not assigned to any application version.

To see what actions each Fortify Software Security Center role can perform:

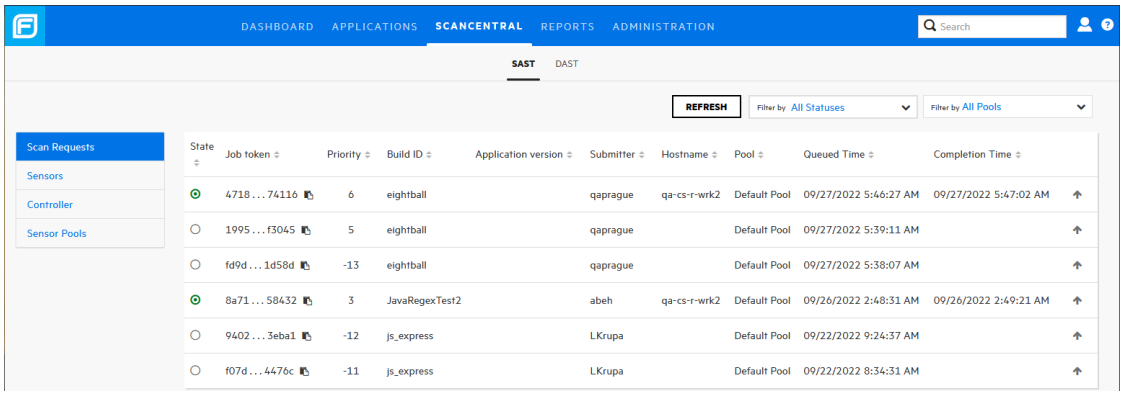
1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Users**, and then select **Roles**.
   The **Roles** table lists all of the roles to which you can assign users.
3. To see all of the actions a user in a given role can perform, click the row for the role.

Viewing ScanCentral SAST Scan Request Details

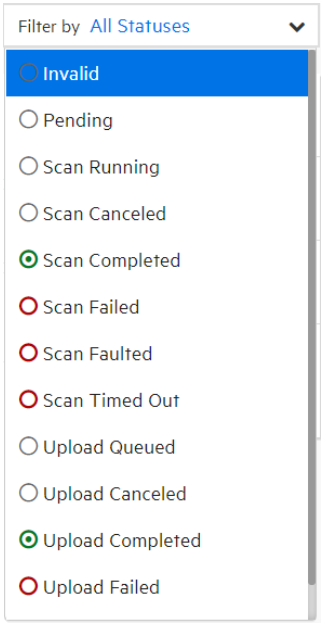
To view details about ScanCentral SAST scan requests.

Note: For information about how to install, configure, and use Fortify ScanCentral SAST to streamline the static code analysis process, see the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

1. On the Fortify header, click **SCANCENTRAL**, and then select the **SAST** tab.
   The **Scan Requests** page lists all scan requests and the details for each.

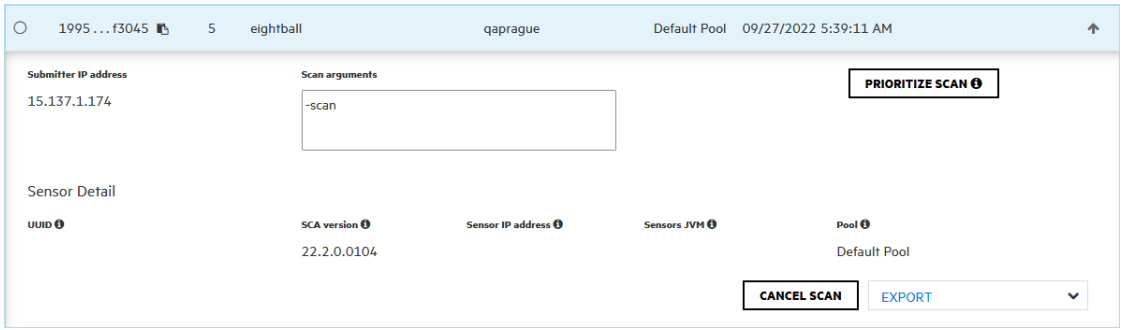


The possible scan requests states are as follows:



To see the true state of a scan request, move your cursor to the state indicator icon.

2. (Optional) To filter the displayed requests based on current state, from the **Filter by** list, select a state.
3. To expand a row and see more detail about a given scan, click its row.



4. To export the scan request details:
   a. From the **EXPORT** list, select either **FPR** to export an FPR file with vulnerabilities uncovered by the scan, or **Log** to export the log file from the scan.
   b. Specify the location for the exported file.
5. To update the data displayed, click **REFRESH**.

See Also

"Prioritizing a ScanCentral SAST Scan Request" below

"Canceling ScanCentral SAST Scan Requests" on the next page

"Viewing ScanCentral SAST Sensor Information" on the next page

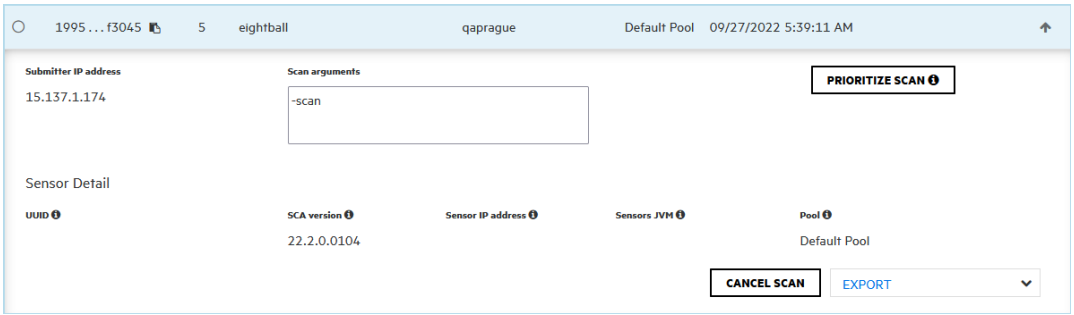
"Viewing ScanCentral Controller Information" on page 387

Prioritizing a ScanCentral SAST Scan Request

If several scan requests are assigned to a given scan pool, and you want one of these to be run before any of the others, you can prioritize it, which moves it to the top of the job queue for that pool.

To prioritize a scan request:

1. On the Fortify header, click **SCANCENTRAL**.
   The SAST page opens to the **Scan Requests** tab, which lists all scan requests.
2. From the **Filter by** list on the left, select **Pending**.
   The numbers in the **Priority** column indicate the order in which the scan jobs are to be run. The lower the number, the sooner the scan is run in the pool. For example, a scan request with a priority of -10 is run before a scan request in the same pool with a priority of -2.
3. Do one of the following:
   a. Expand the row for the scan request that you want to run first.



   b. Click **PRIORITIZE SCAN**.
   Alternatively, you can click the upward pointing arrow (↑) on the right end of the row for the scan request you want to run first.

Canceling ScanCentral SAST Scan Requests

Note: For information about how to install, configure, and use Fortify ScanCentral SAST to streamline the static code analysis process, see the *Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

To cancel a pending ScanCentral scan request:

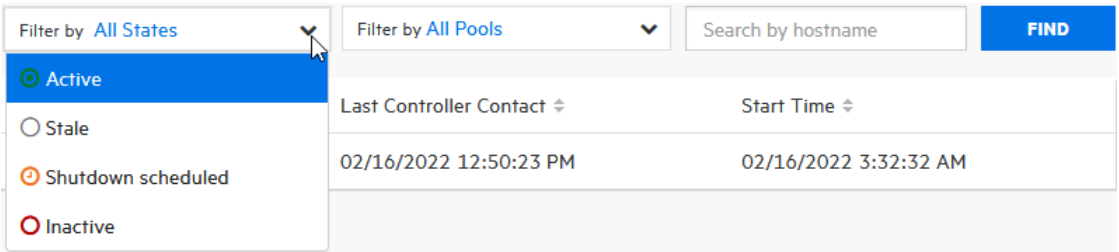
1. On the Fortify header, click **SCANCENTRAL**.
   The SAST page opens to the **Scan Requests** tab, which lists all scan requests.
2. To filter the displayed requests based on current state, from the **Filter by** list, select **Pending**.
3. Expand the row for the pending scan request that you want to cancel.
4. At the bottom right, click **CANCEL SCAN**.
   Fortify Software Security Center prompts you to confirm that you want to cancel the request.
5. Confirm the cancellation.
6. To update the data displayed on the Scan Requests table, click **REFRESH**.

Viewing ScanCentral SAST Sensor Information

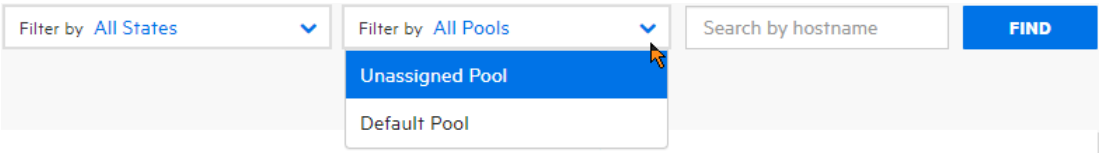
To view current information about ScanCentral SAST sensor states and activities.

Note: For information about how to install, configure, and use Fortify ScanCentral SAST to streamline the static code analysis process, see the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

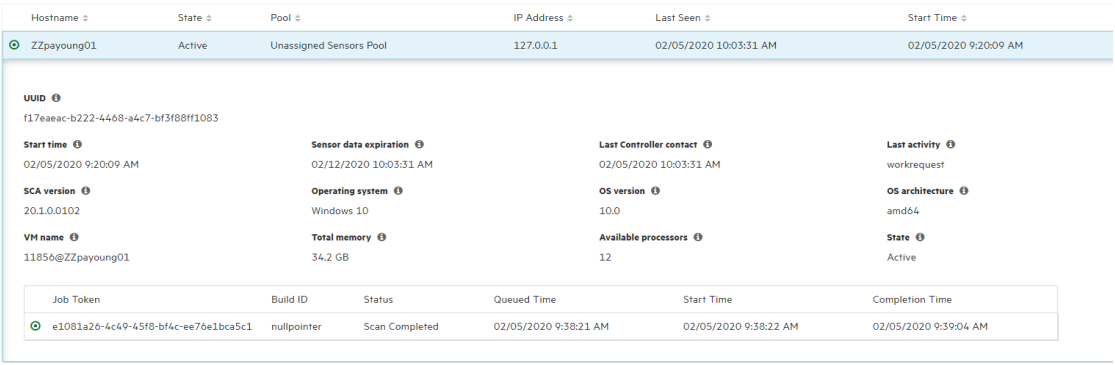
1. On the Fortify header, click **SCANCENTRAL**.
2. Select the **SAST** tab.
3. In the left pane, select **Sensors**.



4. To filter the sensors displayed based on current state (**Active**, **Inactive**, **Stale**, or **Shutdown scheduled**), from the first **Filter by** list, select a state. (**All States** is the default.)



5. To filter the sensors displayed based on the pool to which each is assigned, from the second **Filter by** list, select **Unassigned Pool**, a named pool, or **All Pools** (the default).
6. To expand a row and see details for a sensor, click its row.



See Also

"Canceling ScanCentral SAST Scan Requests" on the previous page

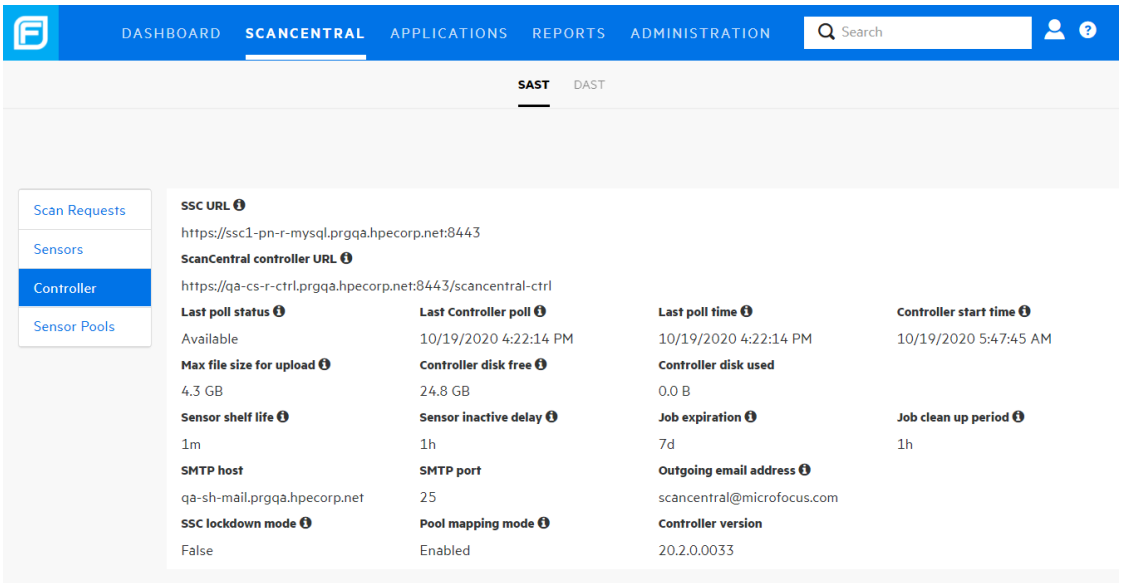
"Viewing ScanCentral SAST Scan Request Details" on page 383

Viewing ScanCentral Controller Information

To view ScanCentral Controller information.

Note: For information about how to install, configure, and use Fortify ScanCentral SAST to streamline the static code analysis process, see the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

1. On the Fortify header, click **SCANCENTRAL**.
2. In the left pane, select **Controller**.



3. For descriptions of each value displayed, click the information icons.

See Also

"Viewing ScanCentral SAST Scan Request Details" on page 383

"Canceling ScanCentral SAST Scan Requests" on page 386

"Viewing ScanCentral SAST Sensor Information" on page 386

Stopping the Controller

You can stop the Controller immediately using the following procedure. However, Fortify strongly recommends that you first place the Controller in maintenance mode to preserve any scans that are running. ("Placing the ScanCentral SAST Controller in Maintenance Mode" on the next page.)

To stop the Controller:

1. On the machine where the Controller is installed, navigate to the Tomcat bin directory:

   On a Windows system:

   ```
   cd <controller_dir>\tomcat\bin
   ```

   On a Linux system:

   ```
   cd <controller_dir>/tomcat/bin
   ```

2. Type one of the following commands:

   On a Windows system:

   ```
   shutdown.bat
   ```

On a Linux system:

```
./shutdown.sh
```

See Also

"Placing the ScanCentral SAST Controller in Maintenance Mode" below

Placing the ScanCentral SAST Controller in Maintenance Mode

An abrupt shutdown of the ScanCentral SAST Controller can result in the loss of scans already started on sensors. To prevent this from happening, place your Controller in maintenance mode. After you do, the Controller accepts no new job requests from clients and assigns no queued jobs to sensors.

After the Controller is placed in maintenance mode, sensors complete the scans they are currently running, but accept no new scans. After the Controller is back up and running, the sensors again become available.

The following procedure describes how to place the Controller in maintenance mode.

Important! To place the Controller in maintenance mode, the Controller must be version 21.2.0 or later.

To place the Controller in maintenance mode:

1. Log on to Fortify Software Security Center as an administrator, and then, on the Fortify header, click **SCANCENTRAL**.
2. In the left pane of the SAST page, select **Controller**.
3. Click **START MAINTENANCE MODE**.

The Controller receives the maintenance request from Fortify Software Security Center and, if any sensors are running scans, the Controller mode changes from ACTIVE to WAITING_FOR_JOB_COMPLETED. If no job is being processed, the mode changes directly from ACTIVE to MAINTENANCE. At this point, you can safely shut down the Controller.

Safely Shutting Down Sensors

This section describes how to move ScanCentral SAST sensors to shutdown, or shutdown scheduled mode from Fortify Software Security Center.

Important! If the Controller is in maintenance mode (see "Placing the ScanCentral SAST Controller in Maintenance Mode" above), you cannot shut down sensors from the Fortify Software Security Center user interface. Also, in order to shut down sensors from the Fortify Software Security Center user interface, the sensors must be version 21.2.0 or later.

Shutting Down Sensors

To shut down active sensors:

1. Log on to Fortify Software Security Center as an administrator, and then, on the Fortify header, click **SCANCENTRAL**.
2. In the left pane of the **SAST** tab, select **Sensors**.
3. In the sensors table, do one of the following:
   - Expand the row for a sensor you want to shut down, and then click **SHUT DOWN**.
   - Select the check boxes for one or more sensors you want to shut down, and then click **SHUT DOWN**.

Note: If the **SHUT DOWN** button is not enabled, it can mean that:

- The sensor version is earlier than 21.2.0
- The sensor was already shut down
- The Controller is in maintenance mode
- The sensor is inactive or disabled

If a sensor you shut down is running a scan, the **State** value for the sensor changes from **Active** to **Shutdown scheduled**. After the scan is completed, the state then changes to **Inactive**.

Removing the ScanCentral SAST Controller from Maintenance Mode

To remove the Controller from maintenance mode:

1. Log on to Fortify Software Security Center as an administrator, and then, on the Fortify header, click **SCANCENTRAL**.
2. In the left pane of the SAST page, select **CONTROLLER**.
3. Click **END MAINTENANCE MODE**.

See Also

"Placing the ScanCentral SAST Controller in Maintenance Mode" on the previous page

"Stopping the Controller" on page 388

About ScanCentral SAST Sensor Pools

If your Fortify Software Security Center server is integrated with Fortify ScanCentral SAST, and you are an Administrator, Manager, or Security Lead, you can create

groups of sensors, or *sensor pools* based on any criteria, which you can then target for scan requests.

Sensor pools give you more control over what sensors are used for scan requests. Here are a couple of examples of how you might use sensor pools:

- Create pools based of sensor computing power (size of physical memory) and assign scan requests that require a lot of memory to those pools.
- Create pools based on teams or business units in your organization, so that your resources are distributed and no team can consume all sensors and block scan requests submitted by other teams.

If a scan request is associated with an application version, the Controller queries Fortify Software Security Center for available sensor pools. If the scan request is not associated with an application version, ScanCentral SAST clients can request a specific sensor pool for a scan request.

Note: By default, sensors are removed 168 hours (7 days) after they become inactive. For details on how to change this default value, see the *ScanCentral SAST Installation, Configuration, and Usage Guide*.

Pre-defined Sensor Pools

Fortify Software Security Center provides two pre-defined sensor pools: the *unassigned sensor pool* and the *default pool*. The unassigned sensor pool, which contains all newly-registered sensors, serves as a shared sensor pool for other pools. If the **Use unassigned sensors** check box is selected, the default sensor pool uses sensors from the unassigned sensor pool. It contains scan requests that were not assigned to a specific sensor pool.

See Also

"Creating ScanCentral SAST Sensor Pools" below

"ScanCentral SAST Permissions" on page 382

"Deleting ScanCentral Pools" on page 394

Creating ScanCentral SAST Sensor Pools

If your Fortify Software Security Center server is integrated with ScanCentral SAST, you can create sensor pools, which you can then target for scan requests.

Note: For information about how to install, configure, and use ScanCentral SAST to streamline the static code analysis process, see the *Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

To create a new sensor pool:

1. On the Fortify header, select **SCANCENTRAL**.
2. Select the **SAST** tab.
3. In the left pane, select **Sensor Pools**.

   The Sensor Pools page lists the default pool and any other sensor pools created on the system.

   Note: The default pool includes all application versions that have not been assigned to a sensor pool.

4. To open the CREATE NEW POOL dialog box. click **+ NEW POOL**.

   Note:

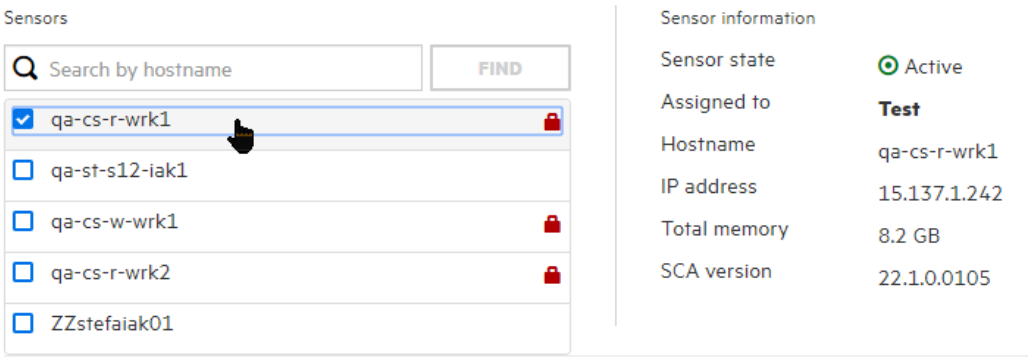
   A disabled **+ NEW POOL** button indicates that Fortify Software Security Center is not connected to the Controller. If the button is disabled, check your SCANCENTRAL SAST CONFIGURATION settings (see "Configuring ScanCentral SAST Monitoring in Fortify Software Security Center" on page 134).

5. In the **Name** box, type a name for the new pool. Note that the first character of the pool name must be a Unicode alphanumeric character (lower or upper case a through z, or 0 through 9).
6. (Optional) In the **Description** box, type a description of the new pool (its properties or purpose).
7. To enable the new pool to use any unassigned sensors, select the **Use unassigned sensors** check box.

   Note: Selecting the **Use unassigned sensors** check box does not assign those sensors to the new pool. Instead, it allows the pool to take advantage of available unassigned sensors. The sensors remain unassigned.

   Note: You can have up to ten sensors in a pool.

   The **Sensors** table lists the host names of all of the sensors in the system, including those that are assigned to other pools. (The padlock icon next to the host name indicates that the sensor is assigned to a pool.) To see information about a sensor, select its row. The **Sensor information** section on the right lists basic information about the sensor, including the pool to which it is currently assigned, if any.



8. To find a specific sensor, type its host name in the search box at the top of the table, and then click **FIND**.
9. Select the check box for each of the sensors you want to assign to the new pool. If you select the check box for a sensor that it already assigned, that sensor will be moved from the pool to which it is currently assigned.

   To assign application versions to the pool:

   a. Under **Versions**, click **ADD**.
   b. In the **APPLICATION** pane (left) of the SELECT APPLICATION VERSION dialog box, select an application that you want to assign to this pool.

      The **VERSIONS** pane (center) lists all active versions of the selected application.
   c. To list any inactive versions of the selected application, select the **Show inactive** check box.
   d. To assign all of the listed versions to the new pool, select the **Select All** check box. Otherwise, to assign only a subset of the application versions, select the check boxes next to the version names.

      The **SELECTED VERSIONS** pane (right) lists your selections.
   e. To assign versions of another application to this pool, repeat steps b through d.
   f. To remove an application version from the **SELECTED VERSIONS** list, click the trash icon ( ) next to its name.
   g. Click **DONE**.
10. In the CREATE NEW POOL dialog box, click **SAVE**.

The **Sensor Pools** table now lists your new pool. The **Pool** column in the table also lists the new pool name for the sensors included.

You can edit or delete the pool at any time.

See Also

"Deleting ScanCentral Pools" on the next page

"Viewing ScanCentral SAST Sensor Information" on page 386

Moving ScanCentral SAST Sensors Between Pools

To move ScanCentral SAST sensors between pools:

1. On the Fortify header, select **SCANCENTRAL**.
2. If Fortify Software Security Center is integrated with both ScanCentral SAST and ScanCentral DAST, select the **SAST** tab to open the Scan Requests page for ScanCentral SAST.
3. In the left pane, select **Sensor Pools**.
4. On the SENSOR POOLS page, select the sensor pool with sensor(s) that you want to assign to a different pool or pools.
5. Click **EDIT POOL**.
6. Under **Sensors** in the EDIT POOL: *<pool name>* dialog box, clear the check box for the sensor(s) you want to assign to a different pool.
7. Click **SAVE**.
8. On the SENSOR POOLS page, select the sensor pool to which you want to assign the now unassigned sensor(s), and then use the steps provided in "Creating ScanCentral SAST Sensor Pools" on page 391 to assign the now unassigned sensor(s).

See Also

"About ScanCentral SAST Sensor Pools" on page 390

Deleting ScanCentral Pools

To delete a ScanCentral pool:

1. On the Fortify header, select **SCANCENTRAL**.
2. In the left pane of the Scan Requests page for ScanCentral, select **Sensor Pools**.

   The Sensor Pools page opens to **Sensor Pools** tab, which lists all existing pools. The last column of the table displays a **Delete Pool** icon for each pool. If the icon is blue, you can delete the pool. If the icon is gray, you cannot delete the pool.
3. Click the **Delete Pool** icon that corresponds to the pool you want to delete.

Fortify Software Security Center removes the pool from the list and adds all sensors assigned to the deleted pool to the **Unassigned Sensors** tab.

See Also

"Viewing ScanCentral SAST Sensor Information" on page 386

"Creating ScanCentral SAST Sensor Pools" on page 391

Chapter 17: Working with Fortify ScanCentral DAST

If Fortify Software Security Center is configured to communicate with Fortify ScanCentral DAST to request and manage dynamic scans, then the **DAST** tab in the SCANCENTRAL view includes the Scans, Sensors, Sensor Pools, Settings List and Scan Schedules pages. For information about how to configure the connection between Fortify Software Security Center and ScanCentral, see "Enabling the Running and Management of ScanCentral DAST Scans from Fortify Software Security Center" on page 135.

Topics covered in this section:

ScanCentral DAST Permissions

The following table shows which Fortify Software Security Center roles have permission to perform which ScanCentral DAST-related tasks.

Roles	Permissions
View-Only	View ScanCentral DAST data, except for jobs not assigned to any application version. **Restrictions:** • Users see only the scans for application to which they are assigned • Users see only sensor pool assignment for the applications to which they are assigned
Administrator, Security Lead, and Manager	• View information on the Scan Requests, Sensors, and Sensor Pools pages • Performing all tasks that involve changes to sensor pools • Cancel scan requests • Assign sensors and application versions to sensor

	pools. **Restrictions:** • Users can cancel only those scan requests for application versions to which they are assigned. • Users can assign only application versions to which they are assigned to sensor pools.
Security Lead	• View DAST data • Create, run, change, and delete DAST scans, schedules and settings • Manage DAST pools and sensors • Download DAST artifacts
Manager	• View, download, and manage ScanCentral SAST data, except for jobs not assigned to any application • View DAST data • Manage DAST pools and sensors **Restrictions:** • Users cannot update scan-related data • Users can cancel only those scan requests for application versions to which they are assigned. • Users can assign only application versions to which they are assigned to sensor pools.
Developer	• View DAST data • Run a DAST scan by referencing an existing settings template • Download DAST artifacts
Application Security Tester	• View DAST data • Create, run, modify and delete DAST scans, schedules, and settings • Download DAST artifacts

To see what actions each Fortify Software Security Center role can perform:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left pane, select **Users**, and then select **Roles**.
   The **Roles** table lists all of the roles to which you can assign users.
3. To see all of the actions a user in a given role can perform, click the row for the role.

Submitting Requests for Dynamic Scans to ScanCentral DAST

If Fortify Software Security Center is integrated with Fortify ScanCentral DAST, and you are assigned to one of the following roles, you can request ScanCentral DAST dynamic scans from Fortify Software Security Center:

- Administrator
- Application Security Tester
- Security Lead
- Developer

For information about how to configure ScanCentral DAST scans and work with scans, sensors, sensor pools, settings, and scan schedules, see the *Micro Focus Fortify ScanCentral DAST Configuration and Usage Guide*.

See Also

"Enabling the Running and Management of ScanCentral DAST Scans from Fortify Software Security Center" on page 135

"ScanCentral DAST Permissions" on page 395

Chapter 18: BIRT Reports

Fortify Software Security Center reports are based on the Business Intelligence and Reporting Technology (BIRT) system. BIRT is an open source reporting system based on Eclipse.

For information about BIRT, see the following page on the Eclipse website:

http://www.eclipse.org/birt/phoenix/intro

Fortify Software Security Center provides templates in the following report categories:

- Application Reports:

  Use the Application Summary report to summarize a single version of an application. This report includes a high-level look at the outstanding issues associated with the application version and detailed information related to its risk profile. It also includes a summary of the user activities.
- Issue Reports

  The Issue report group summarizes the presence of specific vulnerability categories in a single Fortify Software Security Center application version.
- Portfolio Reports:

  The Portfolio report group contains reports that enable you to compare issues trends and indicators across multiple Fortify Software Security Center application versions.

BIRT Libraries

With BIRT Libraries, commonly required functions and report items can be encapsulated. These libraries can then be imported into any number of BIRT reports for reuse. In addition, the concept of libraries helps segment report development tasks, as opposed to requiring a single report developer to create all components for each report by himself.

Note: Before you use the BIRT report libraries, you must acquire the BIRT Report Designer. For instructions, see "Acquiring the BIRT Report Designer" on page 402.

Reports that reference libraries are automatically updated during report execution. This is useful in cases where business or technical changes would otherwise require report rework. For example, if a library component such as a corporate logo is used in a large number of report designs, then a change to the logo would only require a change to the library. All referencing reports would reflect the change automatically.

Importing Report Libraries

If you are an Administrator-level user, you can add report libraries to the Fortify Software Security Center server.

To add a report library:

1. In the left pane of the ADMINISTRATION view, select **Templates**, and then select **Report Libraries**.

   The **Report Libraries** page lists all of the report libraries in the system.
2. To open the IMPORT NEW LIBRARY TEMPLATE dialog box, click **IMPORT**.
3. (Optional) In the **Description** box, type a description of the library you are importing.
4. Click **BROWSE**, and then navigate to and select the report library resource.
5. Click **SAVE**.

The **Report Libraries** table now includes the added library.

See Also

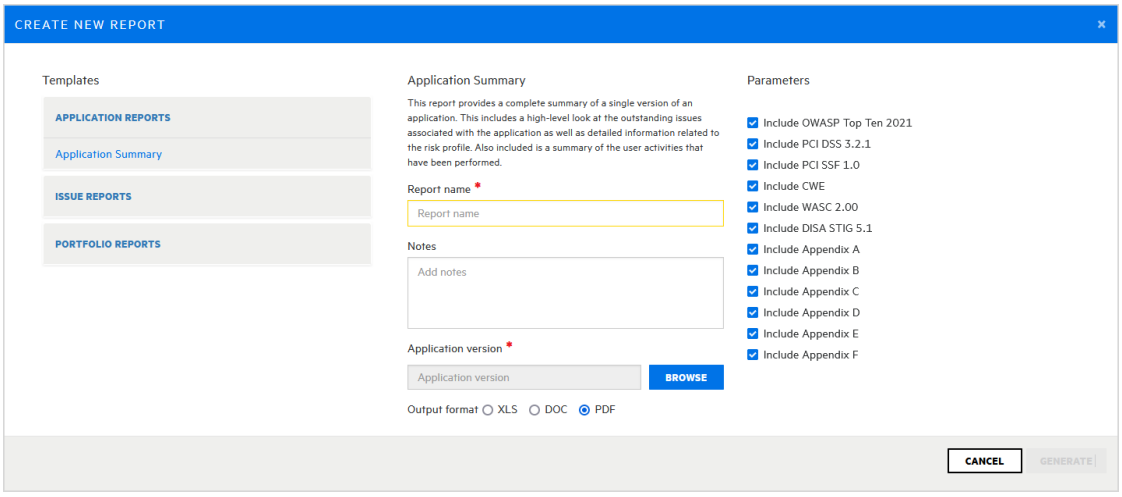
"Preventing Destructive Library and Template Uploads to Fortify Software Security Center" on page 181

"Generating and Viewing Reports" below

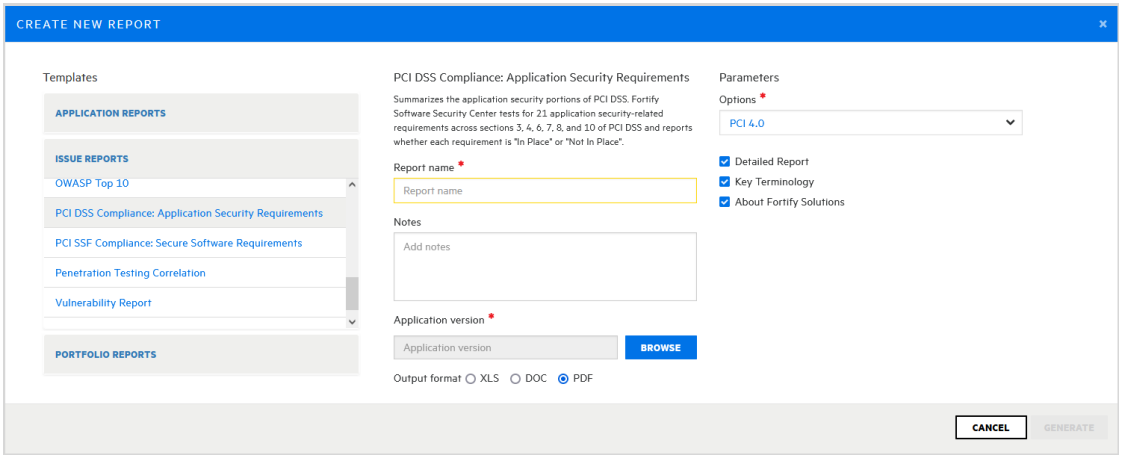
Generating and Viewing Reports

To generate and view a Fortify Software Security Center report:

1. On the Fortify header, click **REPORTS**.
2. To open the CREATE NEW REPORT dialog box, on the Reports page toolbar, click **+ NEW REPORT**.

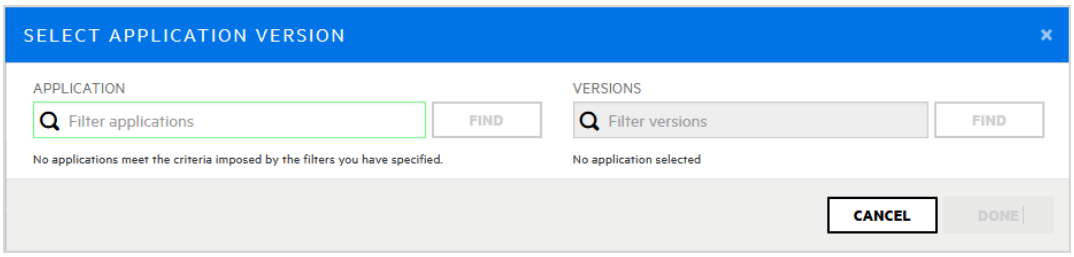


3. Navigate to and select the report template you want to use.

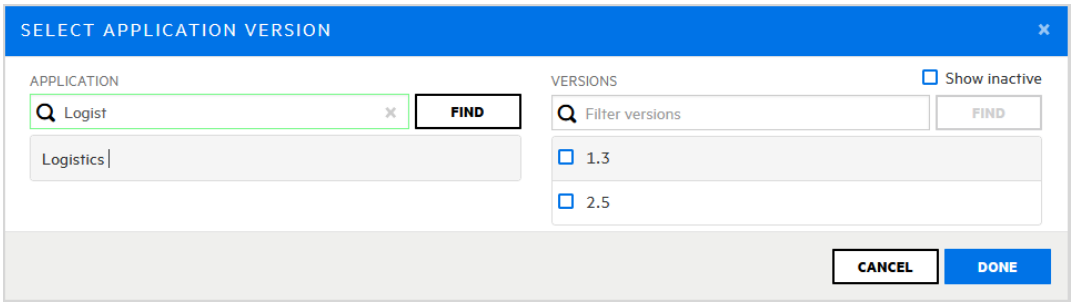


The panes on the right display the configuration fields for the template you select.

4. Specify the required report settings, including the report name, and output format.
5. To specify the application versions to include in the report:
   a. Under **Application version**, click **BROWSE**.

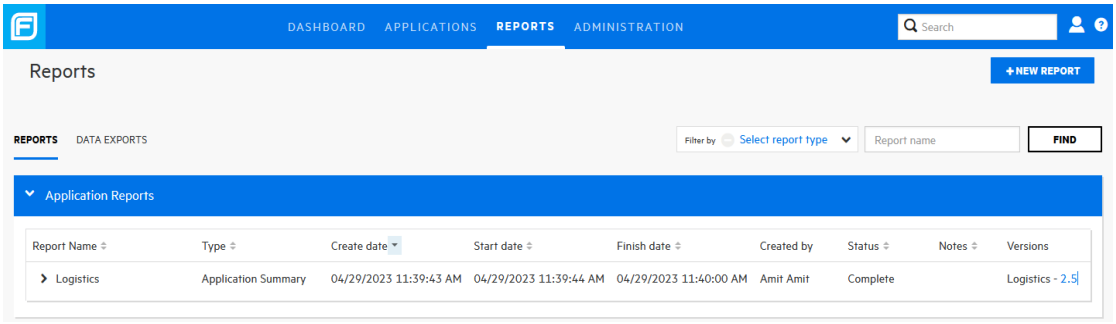


   b. In SELECT APPLICATION VERSION dialog box, under **APPLICATION**, select one of the applications listed, or, in the **Filter applications** box, enter part or all of the application name, and then select the name.



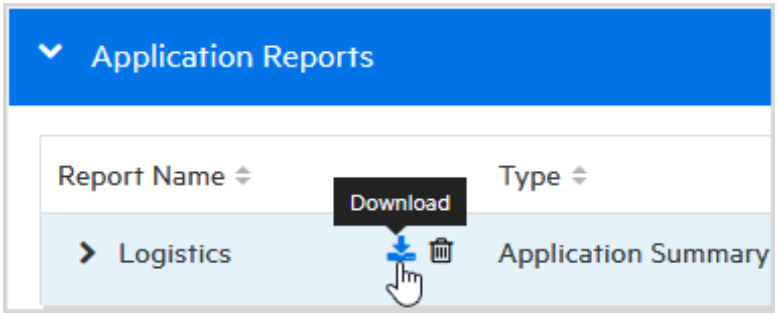
   The active versions of the selected application are listed under **VERSIONS**.
   c. Select the check box for the version to include in the report. (You can select only one.)
   d. Click **DONE**.

6. If multiple editions of a report template are available (for example, for CWE/SANS Top 25 issue reports), from the **Options** list, select the edition you want to generate. Depending on the report type, additional settings might be required or available.
7. To select the format for the report to generate, next to **Output format**, select **XLS**, **DOC**, or **PDF**.
8. In the CREATE NEW REPORT dialog box, click **GENERATE**.



Fortify Software Security Center adds the report to the **Reports** table, which lists all reports, based on category. After the report generation is completed, the **Status** field displays the value **Complete**.

> **Note:** If you typed content in the **Notes** box when you configured the report, the **Notes** column displays a note icon for the report.



9. To download and view the report, move your cursor to the report name, and then click the **Download** icon .

For information about how to specify the number of days for Fortify Software Security Center to keep reports before automatically removing them from the system, see "Configuring Job Scheduler Settings" on page 135.

See Also

"Downloading Report Templates" on page 403

"Importing Report Definitions" on page 404

Customizing BIRT Reports

Customizing BIRT reports is not a beginner-level activity. It requires an understanding of database operation and design, SQL syntax, and report design.

To customize a Fortify Software Security Center BIRT report:

1. Acquire a supported version of Eclipse BIRT Report Designer (*Report Designer*).

   For information about the BIRT Report Designer versions supported for Fortify Software Security Center reports, see the *Fortify Software System Requirements* document.

   For information about downloading Eclipse BIRT Report Designer, see "Acquiring the BIRT Report Designer" below.
2. Load a Fortify Software Security Center report definition into Report Designer.

   You typically first export a report definition from Fortify Software Security Center, and then upload that report definition into Report Designer. For information about how to export a Fortify Software Security Center report definition, see "Downloading Report Templates" on the next page.
3. Connect Report Designer to a running instance of the Fortify Software Security Center database.

   Connecting Report Designer to the Fortify Software Security Center database enables you to load and verify the database queries you add to a BIRT report.
4. Use the Report Designer to add report design elements to the report definition, and add database queries to those design elements.
5. Use a local instance of Fortify Software Security Center to test the operation of a customized BIRT report.
6. Import the customized report definition into Fortify Software Security Center.

For information about importing report definitions into Fortify Software Security Center, see "Importing Report Definitions" on page 404.

Acquiring the BIRT Report Designer

To customize Fortify Software Security Center reports, you must use a supported version of the Eclipse BIRT Report Designer (Report Designer). For information about supported versions, see the *Fortify Software System Requirements* document.

To download the Eclipse BIRT Report Designer:

1. Open a web browser window and go to the following download page:

   https://download.eclipse.org/birt/downloads/drops
2. Download the Report Designer Full Eclipse Install for your operating system.

3. Install the designer. For instructions, see https://www.eclipse.org/birt/documentation/install.php.

Downloading Report Templates

You can download a Fortify Software Security Center report template for modification.

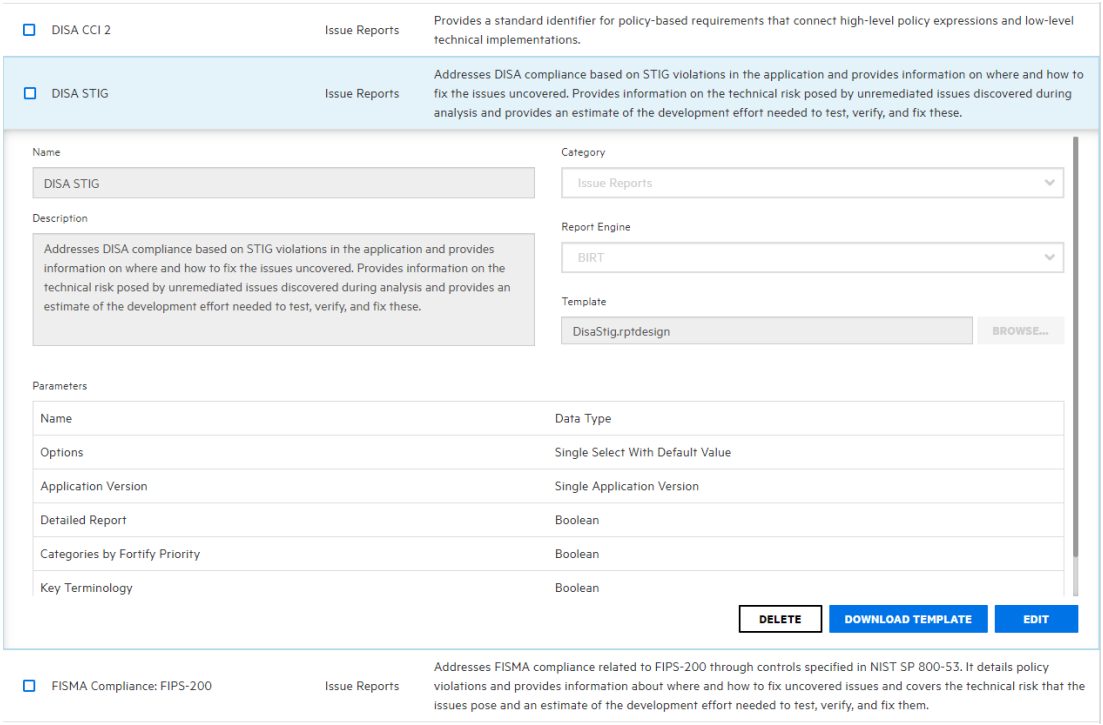
Caution! Although you can download, modify, and re-import Fortify Software Security Center report templates, keep in mind that Fortify does not support customized report templates.

Note: You cannot modify a parameter named "Options" in a BIRT report.

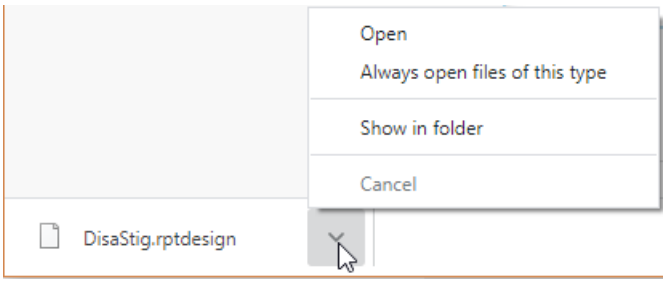
To download a Fortify Software Security Center report template:

1. On the Fortify header, click **ADMINISTRATION**.
2. In the pane on the left, expand **Templates**, and then select **Reports**.

   The table on the right lists the name, type, and description of each report in the system.
3. Click the row for the report of interest.



4. At the lower right of the report details section, click **DOWNLOAD TEMPLATE**.



5. At the bottom left of the screen, click the arrow next to the downloaded report template file name (`*.rptdesign`), and then select **Show in folder**.

You can use the BIRT Report Designer to modify the downloaded report, and then re-import the file into Fortify Software Security Center. If you do, make sure that you rename the modified report file so that it does not replace the original template when you import it.

For information about how to import a customized BIRT report into Fortify Software Security Center, see "Importing Report Definitions" below.

See Also

"Generating and Viewing Reports" on page 399

Importing Report Definitions

Fortify Software Security Center reports are based on the open-source Business Intelligence and Reporting Tools (BIRT) system. A BIRT report definition provides the Fortify Software Security Center report engine the information it needs to generate a report. This includes information such as the report name, report parameters, and the name of the report template file.

BIRT enables you to import report definitions files to Fortify Software Security Center. To do this, you need a Fortify Software Security Center BIRT definition (with the `rptdesign` filename extension).

Caution! When you develop BIRT reports, any database credentials specified are stored insecurely in the report design file. Make sure that you delete credentials from a report before you deploy it to Fortify Software Security Center.

To import a report definition:

1. On the Fortify header, click **ADMINISTRATION**.
2. In the left pane, select **Templates**, and then select **Report Templates**.

   The **Reports** table lists existing report templates, along with the report template types and descriptions.
3. Click **IMPORT**.

4. In the IMPORT NEW REPORT TEMPLATE dialog box, provide the information described in the following table.

Field	Description
Name	Type a name for the template.
Description	(Optional) Type a description of the template and its purpose.
Category	From this list, select the category to which the template belongs.
Report Engine	In this list, leave **BIRT** selected.
Template	Browse to and select a Fortify Software Security Center BIRT definition (with the filename extension `rptdesign`).

5. (Optional) Add one or more parameters to the report definition, as follows:
   a. Click **ADD PARAMETER**.
   b. In the ADD NEW PARAMETER dialog box, provide the information described in the following table.

Field	Description
Name	Type the name of the parameter that corresponds to the parameter in the template you are importing.
Description	(Optional) Type a description of the parameter.
Identifier	Type the unique identifier of the parameter.
Data Type	From this list, select the data type of this parameter.

6. Click **APPLY**.
7. To add the new report definition to the list of definitions, click **SAVE**.

See Also

"Generating and Viewing Reports" on page 399

Chapter 19: Authentication Tokens

Authentication tokens are unique keys that enable users to automate actions within Fortify Software Security Center without using passwords. The user requests a token, authenticates to the Fortify Software Security Center server, and receives back a string with permission to perform for a small set of time-limited actions. For example, the `AnalysisUploadToken` token does not allow the user to log in to the interface or view results. Common actions include uploading scan results and downloading reports.

Generating Authentication Tokens

You can generate authentication tokens from either the ADMINISTRATION view in Fortify Software Security Center, or from the command-line interface. Only you can see the details of your tokens. A Fortify Software Security Center administrator can extend the life of a token you create, but not beyond the maximum days to live for that token.

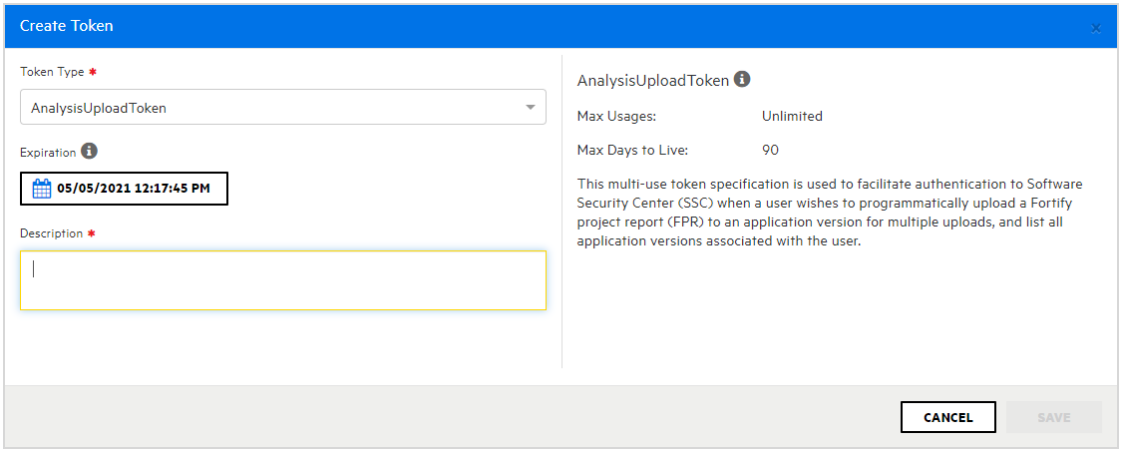
Note: Be aware that you can create a token of any type, but if you do not have the permission required to perform the action that the token is designed to perform, you will not be able to use the token.

Generating a Token from the ADMINISTRATION View

To generate an authentication token from the Fortify Software Security Center user interface:

1. On the Fortify page header, select **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, expand the **Users** section, and then select **Token Management**.
3. To open the Create Token dialog box, on the **Token Management** toolbar, click **NEW**.
4. From the **Token Type** list, select the type of token you want to create.

   To see a list of available token types, see the table in "Generating a Token from the Command Line" on page 408.

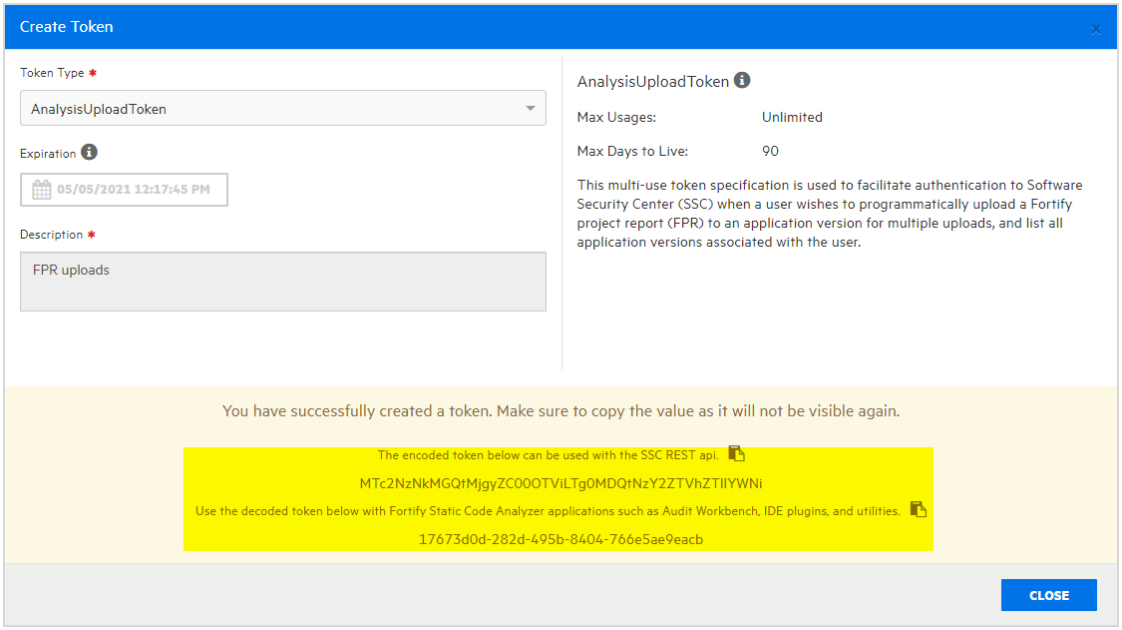


The Create Token dialog box displays a description of the selected token type in the right pane.

5. Use the **Expiration** calendar control to specify the date on which the token is to expire. (The expiration time is set to the current time on the specified date.)

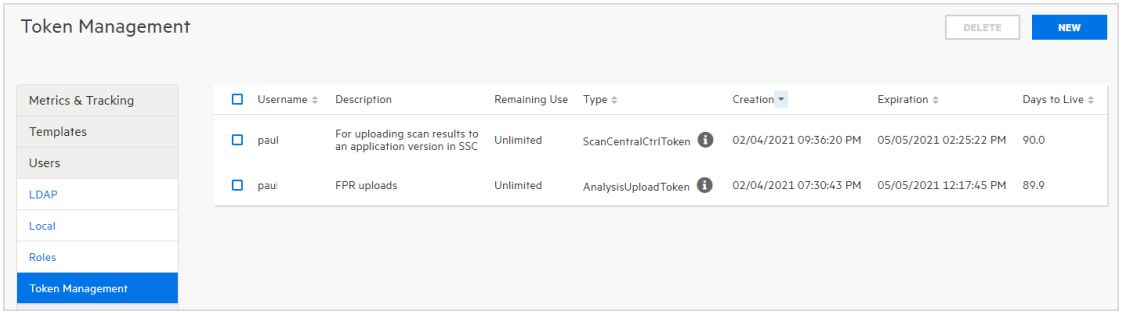
Note: By default, the expiration date value is set to the maximum number of days to live for the selected token type. You can set this to an earlier date to give the token a shorter life. .

6. In the **Description** box, type a description of the intended use of the new token.
7. Click **SAVE**.



The Create Token dialog box displays a message to let you know the token was successfully created.

8. At the bottom of the message, copy either the encoded or decoded token string and save it. (Software Security Center will not display these again.)



The Token Management page now lists the new token.

Generating a Token from the Command Line

To generate a token from the command line, run the following:

```
fortifyclient token -gettoken <token_name> -url <ssc_url> -user <username>
-password <password>
```

The following table lists the available *<token_name>* options.

Option	Description
AnalysisDownloadToken	Download merged result files
AnalysisUploadToken	Upload scan results to Fortify Software Security Center and list applications
AuditToken	Load details about current security issues and apply analysis tags
CIToken	Enables integration of Software Security Center with continuous integration plugins
PurgeProjectVersionToken	Provides the capability to programmatically request a list of all application versions, and to purge application versions from Fortify Software Security Center
ReportFileTransferToken	Typically created programmatically by automation scripts using the /fileTokens endpoint to support downloading an existing report within an authenticated session
ReportToken	Enables users to: Request list of saved reports

Option	Description
	Request saved report based on the report ID Delete saved reports Return list of saved reports associated with a specific application version Generate new reports
ScanCentralCtrlToken	For ScanCentral communications using the Fortify ScanCentral CLI tools
ToolsConnectToken	Use this token with the Fortify Static Code Analyzer applications (including Audit Workbench, IDE plugins, and utilities) that connect to Fortify Software Security Center for collaborative auditing, remediation, and uploading of scan results.
UnifiedLoginToken	Enables access to most of the REST API. It is intended for short-run automations that last less than a day.

Authentication tokens are defined at runtime in `WEB-INF/internal/serviceContext.xml`.

See Also

"Specifying DaysToLive for fortifyclient Authentication Tokens" on page 414.

Editing Authentication Tokens

You can change the descriptions of any of your tokens, and the expiration date for multi-use tokens. (An Administrator can also change the expiration date of multi-use tokens for you, but cannot see other information about the token.)

To modify the description for an authentication token and to change the expiration date for a multi-use token:

1. On the Fortify page header, select **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, expand the **Users** section, and then select **Token Management**.

   The Token Management page lists all of the tokens you have generated.
3. Click the row that displays the token you want to edit.

The row expands to reveal detailed information about the token.

4. Click **EDIT**.
5. To modify the expiration date for a token with a life of more than one day, under **Expiration**, click the calendar control, and then specify a different expiration date.

   Note: By default, the expiration date value is set to the maximum number of days to live for the selected token type. You can set this to an earlier date to give the token a shorter life.

6. Click **SAVE**.

See Also

"Generating Authentication Tokens" on page 406

Deleting Authentication Tokens

To delete an authentication token that you no longer need or that is no longer usable:

1. On the Fortify page header, select **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, expand the **Users** section, and then select **Token Management**.

   The Token Management page lists all of the tokens you have generated.
3. Select the check box for the token you want to delete, and then click **DELETE**.

   Fortify Software Security Center prompts you to confirm that you want to delete the token.
4. Click **OK**.

See Also

"Generating Authentication Tokens" on page 406

Appendix A: Using the fortifyclient Utility

The topics in this section provide information about the Fortify Software Security Center `fortifyclient` command-line utility (on Windows systems, this is `fortifyclient.bat`), which you can use to securely transfer objects to and from Fortify Software Security Center.

Note: Throughout this section, `<ssc_install_dir>` represents the directory into which you extracted the `Fortify_<version>_Server_WAR_Tomcat.zip` file.

This section contains the following topics:

fortifyclient Requirements

To use `fortifyclient` to upload scan results (FPR files), you must know the URL for your Fortify Software Security Center instance and have one the following:

- A user account on the Fortify Software Security Center server with privileges sufficient to perform the operation specified by the `fortifyclient` command-line utility
- A `fortifyclient` authentication token

Topics covered in this section:

About Specifying the Fortify Software Security Center URL

Most `fortifyclient` commands include the Fortify Software Security Center URL. The Fortify Software Security Center URL passed to `fortifyclient` must include both the port number and the context path `/ssc/`. The correct format for the Fortify Software Security Center URL is as follows:

```
http://<hostname>:<port>/ssc/
```

For example:

- For non-root applications: `http://www.company.com/ssc`
- For root applications: `http://ssc.company.com`

Note: In code examples in this guide, *<ssc_url>* represents a correctly formatted Fortify Software Security Center URL, as described in this topic.

fortifyclient Authentication Tokens

`fortifyclient` authentication tokens enable scripted processes to perform operations without revealing Fortify Software Security Center user names and passwords. You can use the credentials for any existing Fortify Software Security Center user account to create an authentication token.

An authentication token inherits the privileges of the account type (Administrator, Security Lead, Manager, or Developer) of the user who creates the token. When `fortifyclient` uses an authentication token to perform an operation, Fortify Software Security Center logs the operation under the account name used to create the token.

Listing fortifyclient Options and Parameters

To list `fortifyclient` commands and parameters:

1. From the command line, navigate to the *<ssc_install_dir>*`/Tools/fortifyclient/bin` directory.
2. At the command prompt, type `fortifyclient`. (On a Windows system, type `fortifyclient.bat`.)

In Fortify Software Security Center, command and option names are case-sensitive.

About Upload Authentication Tokens

`fortifyclient` upload authentication tokens enable the concealment of account and password information as FPRs are uploaded to Fortify Software Security Center.

Topics covered in this section:

Acquiring an Upload Authentication Token Using fortifyclient

You can get upload authentication tokens from either the ADMINISTRATION view in Fortify Software Security Center, or using `fortifyclient`. The following procedure describes how to use `fortifyclient` to acquire an upload authentication token. For information about how to generate one from the ADMINISTRATION view, see "Generating Authentication Tokens" on page 406.

To use `fortifyclient` to acquire an analysis upload token, you must have the following:

- Your Fortify Software Security Center URL (see "About Specifying the Fortify Software Security Center URL" on the previous page)
- A Fortify Software Security Center user account with privileges that enable you to use the `fortifyclient` access token

To acquire an analysis upload token using `fortifyclient`:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory, and run the following:

   ```
   fortifyclient -url <ssc_url> token -gettoken AnalysisUploadToken
       -user <account_name>
   ```

   where `AnalysisUpLoadToken` is the case-sensitive `fortifyclient` upload token specifier.
2. When prompted, type the password for `<account_name>`.

   `fortifyclient` displays a token of the general form:

   ```
   cb79c492-0a78-44e3-b26c-65c14df52e86
   ```
3. Copy the returned token into a text file.

The ability of `fortifyclient` to use the token to read or write information to or from Fortify Software Security Center depends on the privileges of the user account specified by the `-user` parameter.

Specifying DaysToLive for fortifyclient Authentication Tokens

As described in "About Upload Authentication Tokens" on the previous page, `fortifyclient` supports tokens that enable administration to conceal user account information.

You can use the `-daysToLive` parameter to configure `fortifyclient` tokens to expire after a specified number of days. The following example command illustrates the use of the `-daysToLive` parameter to acquire a token that expires after two days:

```
fortifyclient -url <ssc_url> token -gettoken AnalysisUploadToken
    -user admin -daysToLive 2
```

where `<ssc_url>` represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 412).

You must type the case-sensitive `daysToLive` parameter exactly as shown in the example above.

Listing fortifyclient Authentication Tokens

Fortify Software Security Center administrators can use `fortifyclient` to list all existing access tokens for all Fortify Software Security Center user accounts. The `fortifyclient` utility does not support filtering the list of tokens by Fortify Software Security Center account name or account privilege level.

To list all access tokens:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory, and run the following:

   ```
   fortifyclient -url <ssc_url> listtokens -user <admin_account_name>
   ```

   where `<ssc_url>` represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 412) and `<admin_account_name>` is the name of a Fortify Software Security Center Administrator-level user account.
2. When prompted, type the password for the administrator-level user account.

The utility returns a list that includes the ID, owner, creation date, and expiration date for all `fortifyclient` authentication tokens.

Invalidating Tokens

You can invalidate a token you have created by deleting it from the Fortify Software Security Center user interface or by running the `invalidatetoken` command.

To delete a token from the Fortify Software Security Center user interface:

1. On the Fortify page header, select **ADMINISTRATION**.
2. In the left pane of the ADMINISTRATION view, expand the **Users** section, and then select **Token Management**.
3. On the **Token Management** page, click the row that displays the token you want to delete.

   The row expands to reveal the token details.
4. Click **DELETE**.

   Fortify Software Security Center prompts you to confirm that you want to delete the token.
5. Click **OK**.

To invalidate an existing authentication token from the command line.

Note: An administrator can also do this for you.

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

```
fortifyclient -url <ssc_url> invalidatetoken [ -invalidateByID
   <token_ID> |
   -invalidateForUser <owner> | -invalidate <token> ]
```

where

<ssc_url>	represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 412)
<token_ID>	represents the ID of the token to invalidate
<owner>	represents the user for whom the token is to be invalid
<token>	represents the name of the token to invalidate

See Also

"Generating Authentication Tokens" on page 406

Listing Application Versions

You can use `fortifyclient` to list the Fortify Software Security Center application versions accessible by the account that was used to create a particular access token.

Note: Administrator-level users can view all application versions. Security Lead users can view all application versions they created or to which they have been granted access. Manager and Developer account users can view application versions to which they have been granted access.

To perform the command in this section, you must first obtain an upload authentication token. (See "About Upload Authentication Tokens" on page 413.)

To retrieve a list of application identifiers, application names, and application versions:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

   ```
   fortifyclient -url <ssc_url> -authtoken <token> listApplicationVersions
   ```

   where `<ssc_url>` represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 412) and `<token>` is a valid `fortifyclient` authentication token. You can also use the `-user` and `-password` parameters to specify user account credentials.

For all application versions accessible to the user account that created the token, the `fortifyclient` utility lists the application version ID, name, and number.

Purging Application Versions

To purge all artifacts in an application version that was scanned before a given date:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

   ```
   fortifyclient -url <ssc_url> purgeApplicationVersion <app_identifier>
       -scanDate <MMDDYYYY>
   ```

   where `<ssc_url>` represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 412) and `<app_identifier>` represents the `-application <app_name>`, `-applicationVersion <version_name>`, or `-applicationVersionID <id>`.

About Uploading FPRs

Users periodically upload application analysis results files (in FPR format) to Fortify Software Security Center. To do this, you can use an authentication token or a username and password. The topics in this section describe how to upload FPRs using an authentication token. For examples of how to use a username and password, see "About Downloading FPRs" on the next page.
`Fortifyclient` upload access tokens support the use of the `AccessUploadToken` token to conceal user credentials when using scripts to upload FPRs to Fortify Software Security Center. To provide additional security, you can also use an access token's `DaysToLive` parameter.

Note: To perform the procedures described in this section, you must first obtain an authentication token. (See "About Upload Authentication Tokens" on page 413.)

You can upload FPR files using one of the methods described in the following topics:

Using an Application Identifier to Upload FPR Files

To upload an FPR into Fortify Software Security Center using an application identifier:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

```
fortifyclient -url <ssc_url> -authtoken <token> uploadFPR -file
<fpr_name> -applicationVersionID <id>
```

where

<ssc_url>	represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 412)
<token>	represents a valid fortifyclient authentication token
<fpr_name>	represents the full path and name of the FPR file with its extension

`<id>`	represents the Fortify Software Security Center application version identifier

For information about how to acquire Fortify Software Security Center application identifiers, see "Listing Application Versions" on page 416.

Using an Application Name and Version to Upload FPR Files

To upload an FPR into a Fortify Software Security Center application version using the application name and version:

1. Navigate to the `ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

   `fortifyclient -url <ssc_url> -authtoken <token> uploadFPR -file <fpr_name> -application <app_name>, -applicationVersion <version_name>.`

   where

`<ssc_url>`	represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 412)
`<token>`	represents a valid fortifyclient authentication token
`<fpr_name>`	represents the full path and name of the FPR file with its extension
<*app_name*>	represents the Fortify Software Security Center application name
`<version_name>`	represents the Fortify Software Security Center application version that corresponds to the specified application name

See Also

"Using an Application Identifier to Upload FPR Files" on the previous page

About Downloading FPRs

You can use `fortifyclient` to download FPRs by specifying either the Fortify Software Security Center identifier or the application version. This section provides

the procedures to download FPRs using both methods.

You can download FPRs using an authentication token or username and password. The topics in this section describe downloading FPRs using a username and password. For examples using an authentication token, see "About Uploading FPRs" on page 417.

Topics covered in this section:

Downloading an FPR Using an Application Identifier

To use `fortifyclient` to download an FPR file to Fortify Software Security Center using an application identifier:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

```
fortifyclient -url <ssc_url> -user <Username> -password <password>
downloadFPR -file <FPRname> -applicationVersionID <id>
```

where

<ssc_url>	represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 412)
<Username>	represents the user name for a Developer-level (or higher) Software Security Center account with access to the application version that contains the FPR file
<password>	represents the password for the Developer-level (or higher) Software Security Center account with access to the application version that contains the FPR file
<FPRname>	represents the full path and name of the FPR file with its extension
<id>	represents the Fortify Software Security Center application version identifier

For more information about how to acquire Fortify Software Security Center application identifiers, see "Listing Application Versions" on page 416.

Downloading an FPR Using an Application Name and Version

To download an FPR into a Fortify Software Security Center application version using the application name and version:

1. Navigate to the *<ssc_install_dir>*/Tools/fortifyclient/bin directory.
2. Run the following:

```
fortifyclient -url <ssc_url> -user <username> -password
   <password> downloadFPR -file <fpr_name>
   -project <app_name> -version <app_version>
```

where

<ssc_url>	represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 412)
<username>	represents the user name for a Developer-level (or higher) Fortify Software Security Center account with access to the application version that contains the FPR file
<password>	represents the password for the Developer-level (or higher) Fortify Software Security Center account with access to the application version that contains the FPR file
<fpr_name>	represents the full path and name of the FPR file with its extension
<app_name>	represents the Fortify Software Security Center application name
<app_version>	represents the Fortify Software Security Center application version that corresponds to the named application

Importing Content Bundles

As part of its ongoing support for Fortify Software Security Center, Fortify periodically provides security content bundles (`.zip` filename extension) that contain one or more issue templates or report definitions.

Note: Fortify Software Security Center does not support the use of authentication tokens to import content bundles.

To import a content bundle into Fortify Software Security Center:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

```
fortifyclient -url <ssc_url> -user <username> -password <password>
    import -bundle <bundle_name>
```

where

<ssc_url>	represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 412)
<username>	represents the user name for a Manager-level (or higher) Fortify Software Security Center account with access to the application version that contains the fpr file.
<password>	represents the password for the Manager-level (or higher) Fortify Software Security Center account with access to the application version that contains the fpr file.
<bundle_name>	represents the full pathname to the content bundle (`.zip` filename extension)

Downloading Audit Attachment Files

To download an audit attachment file:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

```
fortifyclient -url <ssc_url> downloadAttachment -file <destination_
   file>
   -attachmentId <Attachment_Id>
```

where

<ssc_url>	represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 412)
<destination_file>	represents the full path for the downloaded FPR file
<Attachment_Id>	represents the id of the attachment to download

Appendix B: Authoring Bug Tracker Plugins

Fortify Software Security Center supports integration with external bug tracking systems. This integration allows Fortify Software Security Center users to log bugs for issues as they audit them in Fortify Software Security Center. As delivered, the system can integrate with Jira, Bugzilla, ALM, and Azure DevOps Server. (For specific versions supported, see the *Fortify Software System Requirements* document.) If your company uses a different bug tracker system, you can author a new plugin for it. This section provides information about how to author and deploy a new bug tracker plugin.

Note: In this guide and in the Fortify Software Security Center user interface, the terms *bug* and *defect* are used interchangeably.

Important! Fortify strongly recommends that you inspect the delivered plugin samples before you author your own plugin. You can find the samples in the following directory:

`<ssc_install_dir>/Samples/<BugTrackerPlugin_Name>`

This section contains the following topics:

Use Case

As the Fortify Software Security Center administrator, you can configure an external bug tracking system to use with a given application version, as described in "About Bug Tracker Integration" on page 169. Fortify Software Security Center displays the required configuration parameter fields for the bug tracker you select, and you set

the values for these just one time for the application version. After you test the bug tracker configuration parameter values for validity (optional), you save them to the database for use whenever a user logs a defect for the application version.

A user who submits a bug against an application version logs on to the bug tracker, and then completes the required fields that the bug tracker supplies for the bug parameters. Required parameter information can include such items as summary, description, severity level, component, and so on.

The plugin framework supports a dynamic aspect to bug-tracking parameters. Whenever a user changes a parameter value, the plugin detects the change and an updated list of bug parameters with new list selections becomes available.

When a bug is filed, the bug ID is saved in the database against the issue. The user can then navigate to the bug using an external bug link, which the plugin supplies.

The credentials accepted from the user filing the bug are saved in the server session, and are reused for bugs subsequently submitted against the application during the same session.

Component Setup

The bug tracker plugin can be an independent component that you can write using your preferred IDE.

Configure a bug tracker plugin with the following dependencies:

- Plugin must implement a public API defined and distributed in `fortify-public-<version>.jar` (required)
- Apache Commons Logging (optional)
- Apache Commons Lang (optional)

You can use your preferred build system to build your distributable.

Note: If a plugin has any dependencies on javaEE packages, the plugin developer must bundle the necessary javaEE jars into the plugin's own library path, and must not rely on these packages being available from the JRE. The JavaEE modules were deprecated with Java 9. Such packages include JAXB API and implementation, javax.activation, javax.annotation, javax.transaction, javax.xml.ws, and CORBA-related packages.

Implementation

Fortify Software Security Center versions that use the plugin framework require that all plugins implement the `com.fortify.pub.bugtracker.plugin.BatchBugTrackerPlugin` interface. Fortify

strongly recommends that your implementation class extend `com.fortify.pub.bugtracker.plugin.AbstractBatchBugTrackerPlugin` so that you can take advantage of any backward-compatibility support that becomes available in future releases.

The BatchBugTrackerPlugin interface, which is an extension of the BatchBugTrackerPlugin is as follows:

```
public interface BatchBugTrackerPlugin extends BugTrackerPlugin {

public void addCommentToBug (Bug bug, java.lang.String comment,
UserAuthenticationStore credentials);

public Bug fileMultiIssueBug (MultiIssueBugSubmission bug,
UserAuthenticationStore credentials);

public java.util.List<BugParam> getBatchBugParameters
(UserAuthenticationStore credentials);

public boolean isBugClosed (Bug bug, UserAuthenticationStore
credentials);

public boolean isBugClosedAndCanReOpen (Bug bug,
UserAuthenticationStore credentials);

public boolean isBugOpen (Bug bug, UserAuthenticationStore
credentials);

public java.util.List<BugParam> onBatchBugParameterChange
(java.lang.String changedParamIdentifier, java.util.List<BugParam>
currentValues, UserAuthenticationStore credentials);

public void reOpenBug (Bug bug, java.lang.String comment,
UserAuthenticationStore credentials);

}
```

The BugTrackerPlugin interface, which is the base interface of the BatchBugTrackerPlugin (maintained separately for backward compatibility) is as follows:

```
public interface BugTrackerPlugin {

public boolean requiresAuthentication();

public List<BugTrackerConfig> getConfiguration();

public void setConfiguration(Map<String, String> configuration);

public void testConfiguration(UserAuthenticationStore credentials);

public String getShortDisplayName();

public String getLongDisplayName();
```

```
public List<BugParam> getBugParameters(IssueDetail issueDetail,
        UserAuthenticationStore credentials);
public List<BugParam> onParameterChange(IssueDetail issueDetail,
        String changedParamIdentifier, List<BugParam> currentValues,
        UserAuthenticationStore credentials);
public Bug fileBug(BugSubmission bug, UserAuthenticationStore credentials);
public void validateCredentials(UserAuthenticationStore credentials);
public Bug fetchBugDetails(String bugId, UserAuthenticationStorecredentials);
public String getBugDeepLink(String bugId);
}
```

Plugin Methods and Method Calls

The following table lists the methods and calls to use with your plugin.

Method or Call	Description
requiresAuthentication	This method is expected to return `true` if it requires the framework to request credentials from the user for any bug-tracking operation. This almost always returns `true`, except in cases where the plugin gets its credentials using a different mechanism, perhaps from the credential store or if the plugin interacts with the bug-tracking system asynchronously and not in real time. If the method returns `false`, the system passes null for all the `UserAuthenticationStore` parameters of the plugin methods.
getBatchBugParameters	Used by the plugin framework to get the list of bug parameters the plugin needs to submit batch bugs. Provides default or null values. The `BugTrackerPlugin.setConfiguration (java.util.Map)` method is called on the plugin instance before this method is invoked. Parameter choice lists and defaults can be

Method or Call	Description
	made dynamic by having the implementation go to the bug tracking system to determine the list of valid choices.
getConfiguration	The plugin framework uses this method to get metadata about the questions to be presented to the user during plugin configuration. The return value is a list of BugTrackerConfig objects that provide required information about the configuration item. Each item corresponds to a text box in the user interface. The value field of each item is used to specify the default value for the text box.
setConfiguration (call)	After you select the bug-tracking system for the application version and save the configuration to the database, all future interactions with the plugin are preceded by the `setConfiguration` call, which sets the configuration for the plugin using which operations are to be carried out.
testConfiguration (call)	The plugin framework uses the `testConfiguration` call to test the configuration previously set using the `setConfiguration` call. This method is expected to hit the bug-tracking system using the configuration details set and validate them to the fullest extent possible. The user credentials are fetched from the user if this plugin declared that it requires authentication.
getShortDisplayName	The `getShortDisplayName` method is used to return a short display name for the plugin. This string is used to populate the list of available bug tracker plugins. **Important!** If you customize the sample bug-trackers code that Fortify Software Security Center provides, but you use the same plugin classname, do not change the

Method or Call	Description
	short display name of the plugin. (For consistency, also avoid changing the long display name.) If you *do* change the name of the main implementation class, then you must also change the display name(s) for the plugin.
getLongDisplayName	The `getLongDisplayName` method is used to return a value that includes additional identification of the bug tracking system obtained from the configuration. This method is used, for example, when the user is prompted to provide credentials for a bug-tracking system. **Caution!** If you customize the sample bug-trackers code that Fortify Software Security Center provides, but you use the same plugin classname, do not change the short display name of the plugin. (For consistency, also avoid changing the long display name.) If you *do* change the name of the main implementation class, then you must also change the display name(s) for the plugin.
getBugParameters	The `getBugParameters` method returns metadata about the bug parameters to present to users. Fortify Software Security Center supports the following three bug parameter types: • BugParamText translates to a text box. • BugParamTextArea translates to a multiple-line text box and is typically used for bug descriptions. • BugParamChoice translates to a list. • The `issueDetail` object encompasses the details of the issue for which the user is

Method or Call	Description
	attempting to log a bug. This defaults to various bug parameters such as the description and summary, which can be extracted from this object. The pluginHelper protected member has a helper method to build a suggested default bug description. (See "Plugin Helper" on page 432.)

onBatchBugParameterChange	If a user changes the value of a parameter in the user interface, this method fetches the updated choice list for other batch bug parameters. The `BugTrackerPlugin.setConfiguration(Map)` method is called on the plugin instance before this method is invoked. If the `BugParamChoice.getHasDependentParams()` attribute for a plugin bug parameter is set to `true`, then this method is called whenever the parameter value changes in the user interface layer.
	Recommendations:
	• Act on each bug parameter that has dependent parameters.
	• Do not forget to handle the case in which a parameter value changes to null (no selection made).
	• Do not forget to set the parameter value in return list to null when its choices change.
	• Before you add a new parameter, check to make sure that it is not already in the return list.
	• Return null if there is no change
	• Use either of the following strategies:
	  • Modify the `currentValues` parameter and return it.
	  • Construct the return value from the raw

Method or Call	Description
	parameters maintained. Set the values and choice lists before returning.

onParameterChange	The plugin framework calls the `onParameterChange` method whenever the value for a bug parameter marked as `hasDependentParams` (see BugParamChoice class javadoc) changes. This method can take action and return a new list of bug parameters to display.
	Keep the following guidelines in mind:
	• Act on each bug parameter that has dependent parameters.
	• Do not forget handling case when parameter value changes to null (no selection made).
	• Do not forget to set the parameter value in a return list to null when its selections change.
	• Before you add a new parameter, check the return list to make sure that it does not already include the parameter.
	• Return null if there is no change.
	• Use one of the following strategies:
	  • Modify the `currentValues` parameter and return it.
	  • Construct the return value from raw parameters maintained. Set values and choice lists before returning.

fileBug	This method files a bug on the external bug-tracking system. The `BugSubmission` object passed encompasses all bug details. Make sure that you correctly differentiate between the `bug.getIssueDetail()` object and the `bug.getParams()`object. The `bug.getIssueDetail()` object returns details of the issue, whereas the `bug.getParams()` object

Method or Call	Description
	returns the bug parameter values that the user provides. If you added Bug Description as a user-editable bug parameter, then fetch the bug description from the `bug.getParams()` object instead of from the `bug.getIssueDetail()`object. The return value of the fileBug object must be a bugId, which can be used to fetch the bug with the `fetchBug` method and formulate the deep link with the `getBugDeepLink` method. Use fields in B`ugSubmission.getIssueDetail()`, namely `getLastBuildWithoutIssue()`, `getDetectedInBuild()`, and `getFileName()` to perform changeset discovery if you have access to your repository.
fileMultiIssueBug	File bugs that contain multiple issues on the bug tracking system. The `BugTrack-erPlugin.setConfiguration(Map)` method is called on the plugin instance before this method is invoked. Recommendations: • Fortify Software Security Center provides the summary and description obtained using `MultiIssueBugSubmission.getIssueDetails()`. The user does not supply these values. If you added the summary and description as bug parameters, use `bug.getParams()` to retrieve the user-supplied values. • If you have access to your repository, use the `getLastBuildWithoutIssue()`, `getDetectedInBuild()`, and `getFileName()`fields in `MultiIssueBugSubmission.getIssueDetails()` to perform changeset discovery.
fetchBug	This method is used to fetch the current bug

Method or Call	Description
	status.
getBugDeepLink	This method is used to formulate a deep link to the bug. If the bug tracker does not support a deep link, return null.

For a detailed explanation of each parameter and other supporting classes, see the public API javadoc.

Plugin Helper

If your bug tracker plugin class extended from the class **AbstractBatchBugTrackerPlugin** provided, you will find a protected member **BugTrackerPluginHelper** available. This helper object can be used to perform frequently used plugin operations for locating parameters, loading default values, and so on. Please consult the javadoc for more details. Also look at its usage in the plugin samples.

Error Handling

For proper error handling and reporting, use the following strategy across all plugin methods to throw exceptions:

- Throw `com.fortify.pub.bugtracker.support.BugTrackerException` for any error that the user can act on. Example invalid configuration, errors arising from bug tracking system, bug tracking system failing, and so on. The error message with this exception is relayed back to the user and is expected to be user friendly.
- Throw `com.fortify.pub.bugtracker.support.BugTrackerAuthenticationException` if and only if credentials provided to the bug tracking system are incorrect. This exception results in cached bug tracker credentials being cleared.
- Throw `RuntimeException` or its subclasses for internal exceptions.

Almost Stateless

With every top-level request that Fortify Software Security Center sends to the plugin framework bug tracker (and that needs to communicate with the bug tracker provider), the `setConfiguration` call is made. The only states that should be saved within the plugin are the configuration values that this method provides. The

configuration values can be used during bug tracker plugin internal processing. From this point on, all plugin calls are expected to be stateless.

Plugin instances must not maintain any state, leave open connections, or try to use connections opened in the previous call. Software Security Center does not cache or reuse plugin instances across plugin operations. New states must be opened on each call and cleaned up before method exit.

Debugging a Bug Tracker Plugin

Apache Commons logging is supported in plugins. The resulting logs are appended into the file `plugin-framework.log` located in the `<fortify.home>/<appcontext>/plugin-framework/logs` directory. All exceptions are automatically logged. You can also perform remote debugging of your plugin by connecting to Tomcat Server from the plugin project within your IDE.

Deploying a Customized Bug Tracker Plugin

To deploy a customized bug tracker plugin, build a `JAR` that contains the plugin classes and any of its dependent classes.

The following is an example of a script used to build a bug tracker plugin with Gradle:

```
apply plugin: 'java'

sourceCompatibility = '1.8'

targetCompatibility = '1.8'

dependencies {

compile fileTree(dir: 'lib', include: '*.jar')

}

jar.enabled = false // There is no need to generate a default non-osgi jar
   during build.

clean {

delete "${projectDir}/dist"

}

task pluginJar(type: Jar) {

baseName "com.fortify.BugTrackerPluginAlm"

from sourceSets.main.output
```

```
destinationDir = file("${projectDir}/dist")
manifest {
from "${projectDir}/META-INF/MANIFEST.MF"
}
from(projectDir) {
include "plugin.properties"
include "plugin.xml"
}
into("lib") {
from "${projectDir}/lib"
include "*.jar"
exclude "fortify-public*.jar"
}
}
build.dependsOn(pluginJar)
```

Important! If you customize the sample bug-trackers code that Fortify Software Security Center provides, but you use the same plugin classname, do not change the short display name of the plugin. It is used for the name of the bugfield template group. (For consistency, also avoid changing the long display name.) If you *do* change the name of the main implementation class, then you must also change the display name(s) for the plugin.
For information about how to build a library that includes all bug tracker plugin dependencies, see the `<ssc_install_dir>/Samples/<bugtracker>/README` file.

See Also

"Authoring Bug Tracker Plugins" on page 423

Appendix C: Automating Fortify Software Security Center Configuration

You can automate Fortify Software Security Center configuration before deployment using the autoconfig file. This file includes sections for each configurable aspect of Fortify Software Security Center. The autoconfig file enables automated deployment by providing settings and seed bundles for silent Fortify Software Security Center update and installation. You can use the autoconfig file to automate all Setup wizard tasks. The Setup wizard picks this file up at server startup and automates the entire installation.

Note: The `datasource.properties` file and some database fields contain encrypted entries that rely on the `secret.key` file. So, if you are moving your Fortify Software Security Center instance from one computer to another, you must also move the `secret.key` file (not just your properties file).

To automate Fortify Software Security Center configuration:

1. Open a text editor and create a file named `<app_context>.autoconfig`, where *<app_context>* is the application server context in which Fortify Software Security Center is deployed (the name of the directory created under `fortify.home`). The file name *must* match the application context name (for Fortify Software Security Center, `<app_context>.autoconfig`) with the exception of ROOT context (`_default_.autoconfig`).
2. Add the following to the `<app_context>.autoconfig` file, in the YAML format shown.

   Note: Copy only the properties for the database engine you use, and make sure that you remove the hash symbol (#) before each property.

```
 appProperties:
   # Include any property found in <fortify.home>/<app_context
   >/conf/app.properties.
   # For example, host.url: 'http://ssc.example.org:8888/ssc'
   # searchIndex.location: '/home/ssc/search_index'
   # host.validation: false

datasourceProperties:
   # Include any property found in <fortify.home>/<app_
   context>/conf/datasource.properties.
   # For example:
   # db.username: ssc_db_admin_username
   # db.password: ssc_db_admin_password

   # MSSQL database
   # jdbc.url: 'jdbc:sqlserver://mssql-host:1433;database=ssc_
   db;sendStringParametersAsUnicode=false'

    # MySQL database
   # jdbc.url: 'jdbc:mysql://mysql-host:3306/ssc_db?
   sessionVariables=collation_connection=latin1_general_
   cs&rewriteBatchedStatements=true'

    # Oracle database
   # jdbc.url: 'jdbc:oracle:thin:oracle-host:1521:ssc_db'

 dbMigrationProperties:
   # Enable automatic database migration
   migration.enabled: true
   # Optionally specify alternative migration credentials
   # migration.username: ssc_db_admin_username
   # migration.password: ssc_db_admin_password

seeds:
   # modify the path to the appropriate location for your
   environment
   - '/home/ssc/bundles/Fortify_Process_Seed_Bundle-2023_Q1_
   <build>.zip'
   - '/home/ssc/bundles/Fortify_PCI_Basic_Seed_Bundle-2023_Q1_
   <build>.zip'
   - '/home/ssc/bundles/Fortify_PCI_SSF_Basic_Seed_Bundle-2023_Q1_
   <build>.zip'
   - '/home/ssc/bundles/Fortify_Report_Seed_Bundle-2023_Q1_<build>.zip'
```

3. Save the file in `<fortify.home>` (`%USERPROFILE%\.fortify` on Windows systems).
4. Place a copy of the `fortify.license` file in your `<fortify.home>` folder.
5. Start Tomcat Server.
6. Save the `<app_context>.autoconfig` file and then restart Fortify Software Security Center.

At the end of auto-configuration, Fortify Software Security Center computes the effective configuration checksum and saves it in the `version.properties` file as the value for the `autoconfig.checksum` property.

When Fortify Software Security Center starts with the `<app_context>.autoconfig` file present, it computes an effective configuration checksum and compares it to the checksum stored in the `version.properties` file. If the checksums do not match, Fortify Software Security Center runs a lightweight auto-configuration, and updates the `autoconfig.checksum` value.

If auto-configuration fails for any reason, Fortify Software Security Center is set to maintenance mode (`maintenance.mode=true` in the `version.properties` file) and forces either full auto-configuration or the display of the Setup wizard on the next server startup.

The checksum includes:

- Effective properties from autoconfig appProperties
- Effective properties from autoconfig datasourceProperties
- Filenames from effective autoconfig seeds
- All properties in the `conf/app.properties` file
- All properties in the `conf/datasource.properties` file

Properties from `dbMigrationProperties` are not included in the checksum.

Fortify Software Security Center performs full auto-configuration only if it is not fully configured. Fortify Software Security Center performs lightweight auto-configuration only if the checksums do not match but it is otherwise already configured.

Lightweight auto-configuration skips database migration (regardless of what is set in the `ssc.autoconfig` file) and it skips the initial internal bundle seeding. Seeding of bundles provided by autoconfig seeds is still performed.

Appendix D: Webhook Payloads

Every webhook payload contains the following fields:

- events – webhook event list (information about events triggered)
- sscUrl – URL address of the server
- webhookId – associated webhook ID
- triggeredAt – date on which the payload was created in (created and stored in the database)

Example:

```
{
  “events”:[
    {
      “event”:”ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS”,
      “artifactId”:1,
      “projectVersionId”:1,
      “filename”:”file.fpr”,
      “username”:”testUser1”
    }
  ],
  “triggeredAt”:”2020-08-21T12:19:24.502+0000”,
  “sscUrl”:” http://localhost:8180/ssc”,
  “webhookId”:1
}
```

Event Payloads

An “events” array is filled with actual event payloads, which are described below. Every event has an “event” field, which describes the event type.

Note: Currently, there is just one event in an array. Event aggregation is not supported.

Artifact Upload Payload

Payloads generated for artifact events include the following fields:

- artifactId – ID of uploaded artifact
- projectVersionId – ID of the application version to which the artifact was uploaded
- filename – artifact filename
- username –username of the user who uploaded the event
- event – artifact upload event type
  Possible upload event types:
  - ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS
  - ANALYSIS_RESULT_UPLOAD_FAILURE
  - ANALYSIS_RESULT_UPLOAD_REQUIRES_APPROVAL
  - ANALYSIS_RESULT_INDEXING_COMPLETED

Example:

```
{
  “event”:”ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS”,
  “artifactId”:1,
  “projectVersionId”:1,
  “filename”:”file.fpr”,
  “username”:”testUser1”
}
```

Artifact Upload Approved Payload

This is an extension of Artifact Upload Payload, and contains additional fields to identify the approving user and the approval comment.

Fields:

- artifactId – ID of uploaded artifact
- projectVersionId – ID of application version to which the artifact was uploaded
- filename – artifact filename
- username – username of uploading user
- approvalUsername – approving user's username
- approvalComment – comment submitted with approval

Example:

```
{
  "event":"ANALYSIS_RESULT_UPLOAD_APPROVED",
  "artifactId":1,
  "projectVersionId":1,
  "filename":"file.fpr",
  "username":"testUser1",
  "approvalUsername":"testUser2",
  "approvalComment":"upload has been approved"
}
```

Project Version Payload

Payloads generated for application version events include the following fields:

- projectId –application ID
- projectName – application name
- projectVersionId – application version ID
- projectVersionName –application version name
- event – application version event type
  Possible event types:

- APP_VERSION_CREATED
- APP_VERSION_UPDATED
- APP_VERSION_DELETED

Example:

```
{
  “event”:”APP_VERSION_CREATED”,
  “projectId”:1,
  “projectName”:”Test application”,
  “projectVersionId”:1,
  “projectVersionName”:”v1”
}
```

Project Version Updated Payload

This is an extension of Project Version Payload, with additional fields to identify changes made.

Fields:

- projectId – application ID
- projectName – application name
- projectVersionId – application version id
- projectVersionName – application version name
- event – APP_VERSION_UPDATED
- changes – value list that defines what changed in application version
  Available values:
  - ACTIVE – if application version “active” status has changed
  - COMMITTED – if application version was committed or uncommitted
  - PROJECT_VERSION_NAME – if application version name changed
  - PROJECT_TEMPLATE – if issue template has changed
  - ATTRIBUTES – if business/technical attributes changed
  - USER_ACCESS_ADDED – if one or more users were added to application version

- USER_ACCESS_REMOVED – if one or more users were removed from application version
- CUSTOM_TAG – if application version had custom attribute added or removed
- PRIMARY_TAG – if primary tag of application version has changed

Example:

```
{
  “event”:”APP_VERSION_UPDATED”,
  “projectId”:1,
  “projectName”:”Test application”,
  “projectVersionId”:1,
  “projectVersionName”:”v1”,
  “changes”:[“ACTIVE”,”COMMITTED”]
}
```

Project Version Created From Previous Payload

This is an extension of the Project Version Updated Payload. In this case, the configuration values of an existing application version were copied over to a new application version. The payload contains additional information about the application version on which the new application version is based.

Fields:

- projectId – ID of the parent application
- projectName – name of the parent application
- projectVersionId – (child) application version ID
- projectVersionName –application version name
- previousProjectId – ID of the (parent) application
- previousProjectName – name of the (parent) application
- previousProjectVersionId – ID of the (parent) application version
- previousProjectVersionName - name of the (parent) application version
- event – APP_VERSION_CREATED

Example:

```
{
   “event”:”APP_VERSION_CREATED”,
   “projectId”:1,
   “projectName”:”Test application”,
   “projectVersionId”:2,
   “projectVersionName”:”v2”,
   “previousProjectId”:1,
   “previousProjectName”:”Test application”,
   “previousProjectVersionId”:1,
   “previousProjectVersionName”:”v1”
}
```

Report Generation Payload

Payloads generated for report events.

Fields:

- reportId – ID of the requested report
- reportName – name specified for report generation
- renderingEngine – report rendering engine
- reportType – report type
- event – type of the report generation event
  Available values:
  - REPORT_GENERATION_COMPLETE
  - REPORT_GENERATION_REQUESTED

Example:

```
{
   “event”:”REPORT_GENERATION_COMPLETE”,
   “reportId”:1,
   “reportName”:”Test report”,
   “renderingEngine”:”BIRT”,
   “reportType”:”PROJECT”
}
```

User Payload

Payloads generated for user lifecycle events.

Fields:

- id – user id
- username – user’s username
- event – user event
  - USER_CREATED - Authentication entity (LOCAL_USER, LOCAL_GROUP, LDAP_USER, LDAP_GROUP, or LDAP_ORGANIZATIONAL_UNIT) was created in Fortify Software Security Center.
  - USER_DELETED - Authentication entity (LOCAL_USER, LOCAL_GROUP, LDAP_USER, LDAP_GROUP, or LDAP_ORGANIZATIONAL_UNIT) was deleted from Fortify Software Security Center.
  - USER_UPDATED - Authentication entity (LOCAL_USER, LOCAL_GROUP, LDAP_USER, LDAP_GROUP, or LDAP_ORGANIZATIONAL_UNIT) was updated in Fortify Software Security Center.
  - LOCAL_USER_ACCOUNT_LOCKED
- userType – type of user
  Available types:
  - LOCAL_USER
  - LOCAL_GROUP
  - LDAP_USER
  - LDAP_GROUP
  - LDAP_ORGANIZATIONAL_UNIT

Example:

```
{
  “id”:1,
  “username”:”testUser”,
  “event”:” USER_CREATED”,
  “userType”:” LOCAL_USER”
}
```

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email.

Note: If you are experiencing a technical issue with our product, do not email the documentation team. Instead, contact Fortify Customer Support at https://www.microfocus.com/support so they can assist you.

If an email client is configured on this computer, click the link above to contact the documentation team and an email window opens with the following information in the subject line:

Feedback on User Guide (Fortify Software Security Center 23.1.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to fortifydocteam@microfocus.com.

We appreciate your feedback!