

---

# **Micro Focus**

# **Fortify Software Security Center**

Software Version: 18.20

## **User Guide**

Document Release Date: November 2018

Software Release Date: November 2018



## Legal Notices

Micro Focus  
The Lawn  
22-30 Old Bath Road  
Newbury, Berkshire RG14 1QN  
UK

<https://www.microfocus.com>

## Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

## Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

## Copyright Notice

© Copyright 2008 - 2018 Micro Focus or one of its affiliates

## Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

## 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

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-and-services/documentation>

# Contents

Preface .....	14
Contacting Micro Focus Fortify Customer Support .....	14
For More Information .....	14
About the Documentation Set .....	14
Change Log .....	15
Chapter 1: Introduction .....	24
Intended Audience .....	24
Document Structure .....	24
What's New in Micro Focus Fortify Software Security Center 18.20 .....	25
AUDIT Page Redesign .....	25
Security Training Link .....	25
Audit Assistant Auto-Prediction .....	26
Audit Assistant Auto-Apply .....	26
Submitting Dynamic Scan Requests to Fortify WebInspect Enterprise .....	26
Launching Fortify WebInspect .....	26
Related Documents .....	26
All Products .....	27
Micro Focus Fortify CloudScan .....	28
Micro Focus Fortify Software Security Center .....	28
Micro Focus Fortify Static Code Analyzer .....	29
Micro Focus Fortify WebInspect .....	31
Micro Focus Fortify WebInspect Enterprise .....	32
Part I: Deploying Fortify Software Security Center .....	34
Chapter 2: Providing for Secure Deployment .....	35
Securing Access to Facilities .....	35
Securing Tomcat Server .....	35
Setting Tomcat Server Attributes to Protect Sensitive Data in Cookies .....	35
About Using HTTPS and SSL Communications .....	36

Configuring and Fortify Static Code Analyzer Tools to Communicate with Fortify Software Security Center Using HTTPS .....	36
About Securing Passwords and User Roles .....	37
Managing Computer Services and Accounts .....	37
Chapter 3: Preparing for Fortify Software Security Center Deployment .....	38
High-Level Deployment Tasks .....	38
Deployment Overview .....	39
The Fortify Software Security Center Installation Environment .....	41
Downloading Fortify Software Security Center Files .....	43
Unpacking and Deploying Fortify Software Security Center Software .....	43
About the Fortify Software Security Center Database .....	44
About JDBC Drivers .....	45
Adding the JDBC Driver to Fortify Software Security Center .....	45
About Fortify Software Security Center Database Character Set Support .....	46
Installing and Configuring the Database Server Software .....	46
Database User Account Privileges .....	46
Database-Specific Configuration Requirements .....	47
Using a Microsoft SQL Server Database .....	47
Configuring a MySQL Database .....	48
Configuring an Oracle Database .....	50
Preventing the “No more data to read from socket” Error .....	50
Partitioning an Oracle Database for Improved Performance .....	50
Preparing to Partition an Oracle Database .....	50
Partitioning the Database .....	51
Increasing the Number of Job Execution Threads .....	51
About the Fortify Software Security Center Database Tables and the Schema .....	51
About Seeding the Fortify Software Security Center Database .....	52
Permanently Deleting a Fortify Software Security Center Database .....	52
LDAP User Authentication .....	53
About Fortify Software Security Center User Authentication .....	53
Preparing to Configure LDAP Authentication .....	54
About the LDAP Server Referrals Feature .....	55
Disabling LDAP Referrals Support .....	55
Chapter 4: Deploying Fortify Software Security Center in Tomcat Server .....	56
About the fortify.home Directory .....	57
Directory Structure .....	57
About Secure Deployment .....	58

About Deploying Fortify Software Security Center in Apache Tomcat .....	58
Tomcat Memory Settings .....	58
About Configuring the Tomcat Connectors .....	59
Configuring Tomcat to Unpack WAR Files .....	59
Deploying Fortify Software Security Center in Tomcat Server .....	59
Chapter 5: Configuring Fortify Software Security Center for the First Time .....	60
Chapter 6: Logging in to Fortify Software Security Center .....	65
Chapter 7: Additional Fortify Software Security Center Configuration .....	66
Accessing the Configuration Settings in the ADMINISTRATION View .....	66
Configuring Issue Stats Thresholds .....	67
How Average Days to Review and Average Days to Remediate are Calculated ....	67
Setting the Issue Stats Thresholds .....	67
Configuration Options Available in the ADMINISTRATION View .....	68
Configuring Application Security Training .....	71
About Audit Assistant .....	71
Audit Assistant Workflow .....	72
Getting a Fortify Scan Analytics Authentication Token .....	73
Configuring Audit Assistant .....	74
About Audit Assistant Auto-Prediction .....	75
Mapping Audit Assistant Analysis Tag Values to Fortify Software Security Center Custom Tag Values .....	76
Configuring Fortify Software Security Center for BIRT Reporting .....	79
Enabling Java Security Manager .....	79
Creating a Database Account for Reporting .....	79
Allocating Memory for Report Generation .....	80
Setting Report Generation Timeout .....	81
Configuring CloudScan Monitoring in Fortify Software Security Center .....	81
Configuring Core Settings .....	82
About Configuring a Proxy for Rulepack Updates .....	85
Configuring Email Alert Notification Settings .....	85
Setting the Strategy for Resolving Issue Audit Conflicts .....	87
Configuring Java Message Service Settings .....	88
Configuring LDAP Servers .....	89
Editing an LDAP Server Configuration .....	98
Importing an LDAP Server Configuration .....	98
Registering LDAP Entities .....	99
Refreshing LDAP Entities Manually .....	102

Deleting an LDAP Server Configuration .....	102
Configuring a Proxy for Fortify Software Security Center Integrations .....	103
Configuring Job Scheduler Settings .....	104
Setting Job Execution Priority .....	108
Canceling Scheduled Jobs .....	108
Configuring Browser Access Security for Fortify Software Security Center .....	109
Configuring Fortify Software Security Center to Work with Single Sign-On .....	110
Configuring Fortify Software Security Center to Work with a Central Authorization Server .....	111
Setting up Kerberos Authentication with Fortify Software Security Center .....	112
Configuring Fortify Software Security Center to Work with SAML 2.0- Compliant Single Sign-On Solutions .....	113
Troubleshooting .....	115
Configuring Fortify Software Security Center to Work with Single Sign-On and Single Logout Solutions that use HTTP Headers .....	116
Configuring Fortify Software Security Center to use X.509 Certification- based SSO .....	117
Enabling Debug Logging for Single Sign-On Authentication .....	117
Configuring Web Services to Require Token Authentication .....	117
Changing Log Levels for Fortify Software Security Center .....	118
Chapter 8: Additional Installation-Related Tasks .....	119
Blocking Data Export to CSV Files .....	119
About Bug Tracker Integration .....	119
Managing Bug Tracker Plugins .....	120
Adding Bug Tracker Plugins .....	120
Removing Bug Tracker Plugins .....	120
Securing Logon Credentials for Bug Tracking Systems .....	121
Bug Tracker Parameters .....	121
ALM Parameters .....	122
Configuring an Eclipse Plugin Update Site .....	122
Adding and Managing Parser Plugins .....	123
About Fortify Software Security Center User Administration .....	124
Administrator Accounts .....	124
Fortify Software Security Center User Accounts .....	124
About Creating User Accounts .....	125
Preventing Destructive Library and Template Uploads to Fortify Software Security Center .....	126
Viewing Permission Information for Fortify Software Security Center Roles .....	126

Unlocking User Accounts (Local Users Only) .....	127
About Managing LDAP User Roles .....	128
Group Membership in Fortify Software Security Center .....	128
Handling Failed LDAP User Logins .....	128
About Mapping Fortify Software Security Center Roles to LDAP Groups .....	129
Creating Custom Attributes .....	129
Global Search Functionality in Fortify Software Security Center .....	132
About Global Search Functionality .....	132
Troubleshooting Search Index Issues .....	133
Placing Fortify Software Security Center in Maintenance Mode .....	133
About Fortify Software Security Content .....	134
Updating Rulepacks from the Micro Focus Fortify Update Server .....	135
Exporting Rulepacks .....	136
Importing Security Content .....	136
Deleting Rulepacks .....	136
Extending a Current Mapping .....	137
Creating a New Mapping .....	138
Chapter 9: Upgrading Fortify Software Security Center .....	140
Fortify Software Security Center Database Upgrade Tasks .....	140
Preparing to Upgrade the Fortify Software Security Center Database .....	141
Setting the Innodb Buffer Pool Size when Upgrading a MySQL Server Database .....	142
Preparing to Run the Database Upgrade Script .....	142
Updating and Deploying the WAR File .....	142
Configuring Fortify Software Security Center After an Upgrade .....	142
Upgrading Fortify Static Code Analyzer from Fortify Audit Workbench .....	145
Enabling Fortify Static Code Analyzer Suite Upgrades from Audit Workbench .....	145
Updating Expired Licenses .....	146
Quarterly Security Content Releases .....	146
Seeding the Database with Report Seed Bundles Delivered with Quarterly Security Content Releases .....	147
Part II: Using Micro Focus Fortify Software Security Center .....	148
Chapter 10: Using Fortify Software Security Center .....	149
About the Central Role of Fortify Software Security Center .....	149
Security Management Workflow .....	150
User Accounts and Access .....	151
Active Directory/LDAP Integration .....	151

Logging in to Fortify Software Security Center for the First Time .....	151
Requesting Access to Fortify Software Security Center .....	152
Changing Your Password .....	155
Enabling and Disabling Receipt of Email Alerts .....	156
Disabling Keyboard Shortcuts (Hotkeys) .....	157
About the Fortify Software Security Center Dashboard .....	158
Issue Stats Page .....	158
Exporting Data to Comma-Separated Values Files .....	160
Deactivating Application Versions .....	161
Reactivating Application Versions .....	162
Accessing the Fortify Software Security Center API Documentation .....	163
Viewing Fortify Software Security Center Keyboard Shortcuts .....	164
Chapter 11: Managing User Accounts .....	165
Fortify Software Security Center User Account Management .....	165
About Tracking Teams .....	165
About Roles .....	165
Pre-configured Roles .....	165
Creating Custom Roles .....	166
Deleting Custom Roles .....	167
Fortify Software Security Center Account Administration .....	168
Creating Local User Accounts .....	168
Editing Local User Accounts .....	170
Unlocking User Accounts (Local Users Only) .....	172
Registering LDAP Entities .....	173
Chapter 12: Applications and Application Versions .....	177
About Tracking Development Teams .....	179
About the Application Creation Process .....	179
Strategies for Creating Application Versions .....	179
Strategies for Packaged Software .....	180
Strategies for Continuous Deployment .....	180
About Annotating Application Versions for Reporting .....	180
Viewing a List of Fortify Software Security Center Applications .....	180
About Creating Application Versions .....	181
Application Version Attributes .....	181
Creating Custom Attributes .....	182
Specifying New Custom Attributes in Existing Application Versions .....	185
About Issue Templates .....	185



Adding Issue Templates to the System .....	186
Template Selection .....	186
Creating the First Version of a New Application .....	187
Adding a New Version to an Application .....	189
Enabling Auto-Apply and Auto-Predict for an Application Version .....	193
Searching Applications and Application Versions from the Applications View .....	195
Updating the Application Overview Page .....	195
Editing Application Version Details .....	195
Using Bug Tracking Systems to Help Manage Security Vulnerabilities .....	196
Bug Tracker Configuration .....	196
Velocity Templates for Bug Filing .....	196
Adding Velocity Templates to Bug Tracker Plugins .....	197
Editing Velocity Templates for Bug Tracker Plugins .....	198
Deleting Velocity Templates .....	199
Assigning a Bug Tracking System to an Application Version .....	200
Submitting a Bug for One or More Issues .....	203
Bug State Management .....	204
Changing the Template Associated with an Application Version .....	205
Setting Analysis Results Processing Rules for Application Versions .....	206
Configuring Audit Assistant Options for an Application Version .....	211
Custom Tags .....	211
Adding Custom Tags to the System .....	212
Modifying Custom Tag Attributes .....	214
Globally Hiding Custom Tags .....	215
Deleting Custom Tags .....	215
Adding Custom Tag Values .....	216
Editing Custom Tags .....	216
Deleting Custom Tag Values .....	217
Associating Custom Tags with Issue Templates .....	217
Removing Custom Tags from Issue Templates .....	218
Assigning Custom Tags to Application Versions .....	219
Disassociating a Custom Tag from an Application Version .....	220
Managing Custom Tags Through Issue Templates .....	221
Managing Custom Tags Through an Issue Template in an FPR File .....	221
About Deleting Application Versions .....	221
Deactivating Application Versions .....	222
Reactivating Application Versions .....	222
Deleting an Application Version .....	223

Chapter 13: Variables, Performance Indicators, and Alerts .....	225
Working with Variables .....	225
Creating Variables .....	226
Variable Syntax .....	226
Performance Indicators .....	227
Creating Performance Indicators .....	227
Alert Definitions .....	228
Creating Alerts .....	229
Editing Alerts .....	231
Deleting Alerts .....	231
Viewing and Marking Alerts .....	232
Chapter 14: About Working with Scan Artifacts .....	234
Uploading Scan Artifacts .....	234
Viewing File Processing Errors .....	236
Viewing Scan Errors and Warnings .....	236
Downloading Scan Artifacts .....	237
Downloading the Merged FPR File for an Application Version .....	237
Downloading Individual Scan Results .....	237
Approving Scan Artifacts .....	238
Viewing High-Level Summary Results .....	238
Viewing Summary Metrics on the Issue Stats Page .....	238
Viewing Summary Metrics on the CHART Page .....	239
Viewing Summary Metrics on the Overview Page .....	240
Viewing Issue Metadata .....	241
Mapping Scan Results to External Lists .....	242
Purging Scan Artifacts .....	243
Deleting Artifacts .....	244
Chapter 15: Collaborative Auditing .....	246
About Auditing .....	247
About Current Issues State .....	247
Setting the Strategy for Resolving Issue Audit Conflicts .....	248
Auditing Issues .....	249
Accessing the AUDIT Page from the Issue Stats Page of the Dashboard .....	255
Accessing the AUDIT Page from the Applications View .....	255
Viewing Issues Based on Fortify Priority .....	255
Filtering Issues for Display on the OVERVIEW and AUDIT Pages .....	257
Viewing Issues Assigned to You .....	259

Searching Issues .....	259
Search Modifiers .....	260
Search Query Examples .....	263
About Suppressed, Removed, and Hidden Issues .....	264
Changing Displayed Issues Using Filter Sets .....	265
Viewing Bugs Submitted for Issues .....	265
About Audit Assistant .....	265
Audit Assistant Workflow .....	266
About Classifiers and Prediction Policies .....	267
Defining Classifiers .....	268
Defining a Catch-All Classifier .....	271
Defining Prediction Policies .....	271
Enabling Metadata Sharing .....	273
Submitting Training Data to Audit Assistant .....	274
Reviewing Audit Assistant Results .....	274
Setting Issue Viewing Preferences .....	276
Viewing Suppressed Issues .....	276
Viewing Removed Issues .....	276
Viewing Hidden Issues .....	277
Searching Globally in Fortify Software Security Center .....	277
Fortify Software Security Center and WebInspect Integration .....	279
Viewing Fortify WebInspect Scan Results in Fortify Software Security Center .....	279
WebInspect Audit Data .....	282
False Positives .....	282
Submitting Dynamic Scan Requests to Fortify WebInspect Enterprise .....	283
Processing Dynamic Scan Requests from Fortify WebInspect Enterprise .....	285
Editing and Cancelling Dynamic Scan Requests .....	286
Dynamic Scan Request States .....	286
Editing Dynamic Scan Requests .....	286
Cancelling Dynamic Scan Requests .....	286
Chapter 16: Integrating with Fortify CloudScan .....	288
CloudScan Permissions .....	288
Viewing CloudScan Scan Request Details .....	289
Canceling CloudScan Scan Requests .....	290
Viewing CloudScan Sensor Information .....	290
Viewing CloudScan Controller Information .....	291
About Fortify CloudScan Sensor Pools .....	292

Pre-defined Sensor Pools .....	292
Creating CloudScan Sensor Pools .....	292
Deleting CloudScan Pools .....	295
Chapter 17: BIRT Reports .....	296
Generating and Viewing Reports .....	296
Preventing Destructive Libraries and Templates from Being Uploaded .....	299
BIRT Libraries .....	299
Importing Report Libraries .....	300
Customizing BIRT Reports .....	300
Acquiring the BIRT Report Designer .....	301
Downloading Report Definitions .....	301
Importing Report Definitions .....	302
Chapter 18: Authentication Tokens .....	304
Generating Authentication Tokens .....	304
Generating a Token from the ADMINISTRATION View .....	304
Generating a Token from the Command Line .....	305
Editing Authentication Tokens .....	307
Deleting Authentication Tokens .....	307
Appendix A: Using the fortifyclient Utility .....	309
fortifyclient Requirements .....	309
About Specifying the Fortify Software Security Center URL .....	310
fortifyclient Authentication Tokens .....	310
Listing fortifyclient Options and Parameters .....	310
About Uploading Authentication Tokens .....	310
Acquiring an Upload Authentication Token Using fortifyclient .....	311
Specifying DaysToLive for fortifyclient Authentication Tokens .....	311
Listing fortifyclient Authentication Tokens .....	312
Invalidating Tokens .....	312
Listing Application Versions .....	313
Purging Application Versions .....	314
About Uploading FPRs .....	314
Using an Application Identifier to Upload FPR Files .....	314
Using an Application Name and Version to Upload FPR Files .....	315
About Downloading FPRs .....	316

Downloading an FPR Using an Application Identifier .....	316
Downloading an FPR Using an Application Name and Version .....	317
Importing Content Bundles .....	317
Downloading Audit Attachment Files .....	318
Appendix B: Authoring Bug Tracker Plugins .....	320
Use Case .....	320
Application Setup .....	321
Implementation .....	321
Plugin Methods and Method Calls .....	322
Plugin Helper .....	325
Error Handling .....	325
Almost Stateless .....	326
Debugging a Bug Tracker Plugin .....	326
Deploying a Customized Bug Tracker Plugin .....	326
Appendix C: Automating Fortify Software Security Center Configuration .....	328
Send Documentation Feedback .....	330

# Preface

## Contacting Micro Focus Fortify Customer Support

If you have questions or comments about using this product, contact Micro Focus Fortify Customer Support using one of the following options.

### **To Manage Your Support Cases, Acquire Licenses, and Manage Your Account**

<https://softwaresupport.softwaregrp.com>

### **To Call Support**

1.844.260.7219

## For More Information

For more information about Fortify software products:

<https://software.microfocus.com/solutions/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-and-services/documentation>

# Change Log

The following table lists changes made to this document.

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

<b>Software Release / Document Revision</b>	<b>Changes</b>
18.20	<p><b>New topics:</b></p> <ul style="list-style-type: none"><li>• <a href="#">"Configuring Application Security Training" on page 71</a></li><li>• <a href="#">"About Audit Assistant Auto-Prediction" on page 75</a></li><li>• <a href="#">"Extending a Current Mapping" on page 137</a></li><li>• <a href="#">"Creating a New Mapping" on page 138</a></li><li>• <a href="#">"Enabling Auto-Apply and Auto-Predict for an Application Version" on page 193</a></li><li>• <a href="#">"Configuring Audit Assistant Options for an Application Version" on page 211</a></li><li>• <a href="#">"Viewing Issues Based on Fortify Priority" on page 255</a></li><li>• <a href="#">"Submitting Dynamic Scan Requests to Fortify WebInspect Enterprise" on page 283</a></li><li>• <a href="#">"Processing Dynamic Scan Requests from Fortify WebInspect Enterprise" on page 285</a></li></ul> <p><b>Modified topics:</b></p> <ul style="list-style-type: none"><li>• In the topic <a href="#">"Configuration Options Available in the ADMINISTRATION View" on page 68</a> the reference to SAP NetWeaver was removed and information about the AppSec Training section was added.</li><li>• Information about the new <b>REFRESH POLICIES</b> button was added to <a href="#">"Configuring Audit Assistant" on page 74</a>.</li><li>• Information about the <b>Disable 4.30 legacy UI</b> field was removed from the topic <a href="#">"Configuring Core Settings" on page 82</a>.</li><li>• The path to the <code>securityContext.xml</code> file was corrected in <a href="#">"Enabling Fortify Static Code Analyzer Suite Upgrades from Audit Workbench" on page 145</a>.</li></ul>

<b>Software Release / Document Revision</b>	<b>Changes</b>
	<ul style="list-style-type: none"><li>• The procedure for seeding the database with the report seed bundle from a quarterly security content release was modified in "<a href="#">Seeding the Database with Report Seed Bundles Delivered with Quarterly Security Content Releases</a>" on page 147.</li><li>• The note that indicated that you can edit your own account information from the legacy user interface was removed from "<a href="#">User Accounts and Access</a>" on page 151.</li><li>• All references to the legacy interface were removed from "<a href="#">Changing Your Password</a>" on page 155.</li><li>• Information about going to the legacy user interface to reactivate a missing application version was removed from "<a href="#">Reactivating Application Versions</a>" on page 222.</li><li>• The description of the <b>Check external metadata file versions in scan against versions on server</b> rule was changed in "<a href="#">Setting Analysis Results Processing Rules for Application Versions</a>" on page 206.</li><li>• "<a href="#">Alert Definitions</a>" on page 228 was changed to reflect the fact that it is no longer necessary for an administrator to enable email notifications from the legacy user interface (which is no longer available).</li><li>• "<a href="#">Auditing Issues</a>" on page 249 was changed to reflect the addition of Fortify priority links to the AUDIT page, the removal of the <b>Overview</b> section from the <b>CODE</b> tab, and the addition of the application security training feature.</li><li>• "<a href="#">Viewing Fortify WebInspect Scan Results in Fortify Software Security Center</a>" on page 279 was changed to reflect changes to the user interface for issue details.</li></ul> <p><b>Removed topics:</b></p> <ul style="list-style-type: none"><li>• Disabling the Legacy User Interface</li><li>• Setting the Legacy User Interface as the Default User Interface</li><li>• About the SAP NetWeaver Plugin for Fortify Software Security Center</li><li>• Adding the SAP JCo Driver to Fortify Software Security Center</li></ul>



Software Release / Document Revision	Changes
	<ul style="list-style-type: none"> <li>• Connecting to SAP NetWeaver</li> <li>• Uploading SAP NetWeaver Data to an Application Version</li> <li>• Switching Between the Current User Interface and the Legacy User Interface (The legacy version 4.30 user interface is no longer available.)</li> </ul>
18.10 / July 16, 2018	<p><b>New topics:</b></p> <ul style="list-style-type: none"> <li>• <a href="#">"Enabling Debug Logging for Single Sign-On Authentication" on page 117</a></li> <li>• <a href="#">"Changing Log Levels for Fortify Software Security Center" on page 118</a></li> <li>• <a href="#">"Automating Fortify Software Security Center Configuration" on page 328</a></li> </ul> <p><b>Modified topics:</b></p> <ul style="list-style-type: none"> <li>• Added to the procedure described in <a href="#">"Importing Security Content" on page 136</a></li> </ul>
18.10 / June 21, 2018	<p><b>New topics:</b></p> <ul style="list-style-type: none"> <li>• <a href="#">"Editing Local User Accounts" on page 170</a></li> </ul> <p><b>Modified topics:</b></p> <ul style="list-style-type: none"> <li>• <a href="#">"Configuring Issue Stats Thresholds" on page 67</a> was revised to include information about how values are calculated.</li> <li>• <a href="#">"Setting Analysis Results Processing Rules for Application Versions" on page 206</a> now includes the rule "Require the issue audit permission to upload audited analysis files."</li> <li>• In <a href="#">"Seeding the Database with Report Seed Bundles Delivered with Quarterly Security Content Releases" on page 147</a>, the introductory text was modified for increased clarity.</li> </ul>
18.10	<ul style="list-style-type: none"> <li>• Most topics were edited to reflect branding and style changes in the user interface.</li> <li>• All references to IBM DB2 database software, which is no longer supported, were removed.</li> </ul>

<b>Software Release / Document Revision</b>	<b>Changes</b>
	<ul style="list-style-type: none"><li>• All references to IBM WebSphere, and Oracle WebLogic, which are no longer supported, were removed.</li><li>• All references to application servers other than Apache Tomcat were removed.</li></ul> <p><b>New topics:</b></p> <ul style="list-style-type: none"><li>• <a href="#">"Partitioning an Oracle Database for Improved Performance" on page 50</a></li><li>• <a href="#">"Configuring a Proxy for Fortify Software Security Center Integrations" on page 103</a></li><li>• <a href="#">"Editing Authentication Tokens" on page 307</a></li><li>• <a href="#">"Deleting Authentication Tokens" on page 307</a></li></ul> <p><b>Modified topics:</b></p> <ul style="list-style-type: none"><li>• <a href="#">"What's New in Micro Focus Fortify Software Security Center 18.20" on page 25</a></li><li>• <a href="#">"Deployment Overview" on page 39</a> now includes a note to advise users that the product does not support load balancing across multiple Fortify Software Security Center servers.</li><li>• In <a href="#">"The Fortify Software Security Center Installation Environment" on page 41</a>, the graphic and table were updated, and the references to Fortify Runtime were removed.</li><li>• <a href="#">"Configuring a MySQL Database" on page 48</a> now includes instructions for setting the sql_mode option.</li><li>• <a href="#">"About the fortify.home Directory" on page 57</a></li><li>• <a href="#">"Configuring Fortify Software Security Center for the First Time" on page 60</a> was revised to reflect the fact that reading configuration settings from a previous WAR file is no longer supported.</li><li>• <a href="#">"Configuring Audit Assistant" on page 74</a> was changed to reflect the addition of the <b>Enable Audit Assistant</b> auto-apply field.</li><li>• In <a href="#">"Configuring Core Settings" on page 82</a>, information regarding the Rulepack proxy server settings was removed.</li><li>• <a href="#">"About Configuring a Proxy for Rulepack Updates" on page 85</a> was</li></ul>

Software Release / Document Revision	Changes
	<p>revised to reflect the introduction of a single proxy for access to all external resources.</p> <ul style="list-style-type: none"> <li>• <a href="#">"Configuring LDAP Servers" on page 89</a> was changed to reflect the addition of the SECURITY section and the new <b>Show Password</b> check box to the CREATE NEW LDAP CONFIGURATION dialog box.</li> <li>• <a href="#">"Configuring Job Scheduler Settings" on page 104</a> was changed to reflect the addition of the new <b>Token management</b> and <b>Data export maintenance</b> settings.</li> <li>• Upgrade tasks were revised in <a href="#">"Fortify Software Security Center Database Upgrade Tasks" on page 140</a>.</li> <li>• The steps <a href="#">"Configuring Fortify Software Security Center After an Upgrade" on page 142</a> in were revised.</li> <li>• <a href="#">"Updating Expired Licenses" on page 146</a></li> <li>• <a href="#">"Seeding the Database with Report Seed Bundles Delivered with Quarterly Security Content Releases" on page 147</a></li> <li>• <a href="#">"Generating Authentication Tokens" on page 304</a> now includes instructions on how to generate tokens from the ADMINISTRATION view.</li> <li>• <a href="#">"Acquiring an Upload Authentication Token Using fortifyclient" on page 311</a></li> </ul> <p><b>Removed topics:</b></p> <ul style="list-style-type: none"> <li>• Correcting a Case-Insensitive SQL Server Database Deployment</li> <li>• Correcting a Case-Insensitive MySQL Database Deployment</li> <li>• Role-Based Permissions for Fortify Software Security Center</li> <li>• Modifying Your User Account</li> <li>• Configuring an IBM DB2 Database</li> <li>• Troubleshooting an Error Received While Seeding an IBM DB2 Database</li> <li>• Deploying Fortify Software Security Center in WebLogic 12c</li> <li>• About Deploying Fortify Software Security Center in IBM WebSphere</li> <li>• About Fortify Website Certificates for WebSphere</li> </ul>

Software Release / Document Revision	Changes
	<ul style="list-style-type: none"> <li>• Exporting a Fortify Website Certificate Using Firefox</li> <li>• Exporting a Fortify Website Certificate Using Internet Explorer</li> <li>• Adding a Website Certificate to IBM WebSphere</li> <li>• Preparing IBM WebSphere Application Server for Fortify Software Security Center Deployment</li> <li>• Deploying Fortify Software Security Center in IBM WebSphere</li> <li>• Troubleshooting Database Migration Problems</li> <li>• Role-Based Permissions for Fortify Software Security Center</li> <li>• Viewing the Custom Tags Associated with an Issue Template</li> <li>• About Archiving and Restoring Runtime Events</li> <li>• Archived Runtime Events</li> <li>• Listing Runtime Applications</li> <li>• Archiving Runtime Events</li> <li>• About Restored Runtime Events</li> <li>• Restoring Runtime Events</li> <li>• Listing Runtime Archives</li> <li>• Uploading a Source Archive to an Application Version</li> <li>• Downloading Runtime Event Archive Files</li> <li>• Appendix A: LDAP Configuration Property Descriptions</li> </ul>
17.20	<p>All references to the Configuration Wizard were removed. Settings that existed in the configuration wizard in earlier versions are now accessed through the Fortify Software Security Center ADMINISTRATION view.</p> <p><b>New topics:</b></p> <ul style="list-style-type: none"> <li>• <a href="#">"What's New in Micro Focus Fortify Software Security Center 18.20" on page 25</a></li> <li>• <a href="#">"Adding the JDBC Driver to Fortify Software Security Center" on page 45</a></li> <li>• <a href="#">"About the fortify.home Directory" on page 57</a></li> <li>• <a href="#">"Configuring Fortify Software Security Center for the First Time" on</a></li> </ul>

Software Release / Document Revision	Changes
	<p>page 60</p> <ul style="list-style-type: none"> <li>• "Blocking Data Export to CSV Files" on page 119</li> <li>• "Managing Bug Tracker Plugins" on page 120</li> <li>• "Adding and Managing Parser Plugins" on page 123</li> <li>• "Placing Fortify Software Security Center in Maintenance Mode" on page 133</li> <li>• "Configuring Fortify Software Security Center After an Upgrade" on page 142</li> <li>• "Seeding the Database with Report Seed Bundles Delivered with Quarterly Security Content Releases" on page 147</li> <li>• "Exporting Data to Comma-Separated Values Files" on page 160</li> <li>• "Debugging a Bug Tracker Plugin" on page 326</li> <li>• "Mapping Audit Assistant Analysis Tag Values to Fortify Software Security Center Custom Tag Values" on page 76</li> </ul> <p><b>Modified topics:</b></p> <ul style="list-style-type: none"> <li>• Switching Between the Current User Interface and the Legacy User Interface</li> <li>• "Preparing for Fortify Software Security Center Deployment" on page 38</li> <li>• "About JDBC Drivers" on page 45</li> <li>• "Configuration Options Available in the ADMINISTRATION View" on page 68</li> <li>• The procedure described in "Configuring Audit Assistant" on page 74 was changed to reflect the addition of the <b>Prediction policy name</b> list to the Audit Assistant page.</li> <li>• "Configuring Core Settings" on page 82</li> <li>• "About Bug Tracker Integration" on page 119</li> <li>• "Global Search Functionality in Fortify Software Security Center" on page 132</li> <li>• "Upgrading Fortify Software Security Center" on page 140</li> <li>• "Preparing to Upgrade the Fortify Software Security Center</li> </ul>

<b>Software Release / Document Revision</b>	<b>Changes</b>
	<p data-bbox="553 384 837 415"><a href="#">Database" on page 141</a></p> <ul data-bbox="524 436 1049 468" style="list-style-type: none"><li>• <a href="#">"Updating Expired Licenses" on page 146</a></li></ul> <p data-bbox="524 489 737 520"><b>Removed topics:</b></p> <ul data-bbox="524 552 1308 1854" style="list-style-type: none"><li>• Starting the HPE Security Fortify Software Security Center Configuration Wizard</li><li>• Running the Configuration Wizard from the Command Line</li><li>• Setting Properties Using the Configuration Wizard</li><li>• Configuring the Core Parameters</li><li>• Saving the Configuration Wizard Settings</li><li>• About Database Setup</li><li>• Seeding a New Fortify Software Security Center Database</li><li>• Reseeding the Upgraded Database</li><li>• Configuring the Database Connection Parameters</li><li>• About Configuring Connectivity to an Upgraded Database</li><li>• Migrating from a Previous Version of Fortify Software Security Center</li><li>• Generating and Running the Database Migration Script</li><li>• Testing the JDBC Connection</li><li>• Configuring the Defect Tracker Plugins</li><li>• Additional Bug Tracker Configuration Information</li><li>• Developer Workbook Report</li><li>• DISA STIG Reports</li><li>• CWE/SANS Top 25 Reports</li><li>• FISMA Compliance: FIPS - 200 Report</li><li>• OWASP Mobile Top 10 Reports</li><li>• OWASP Top 10 Reports</li><li>• PCI DSS Compliance: Application Security Report</li><li>• Penetration Testing Correlation Report</li><li>• Seven Pernicious Kingdoms Report</li></ul>

<b>Software Release / Document Revision</b>	<b>Changes</b>
	<ul style="list-style-type: none"><li>• Vulnerability Report</li><li>• Hierarchical Summary Report</li><li>• Issue Trending Report</li><li>• Key Performance Indicators Report</li><li>• Security at a Glance Report</li></ul>

# Chapter 1: Introduction

The Fortify Software Security Center family of products performs sophisticated analyses of an enterprise's source code that results in concise summaries of source code security vulnerabilities.

If you are not installing Fortify Software Security Center for the first time, see the instructions on how to upgrade from an earlier version (["Upgrading Fortify Software Security Center" on page 140](#)).

## 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 163](#).

## Document Structure

This document is divided into two main parts. Part 1 (["Deploying Fortify Software Security Center" on page 34](#)) includes chapters that describe the deployment environment and provide instructions for installing and configuring Fortify Software Security Center. Part 2 (["Using Micro Focus Fortify Software Security Center" on page 148](#)) includes chapters that describe how to use Fortify Software Security Center.

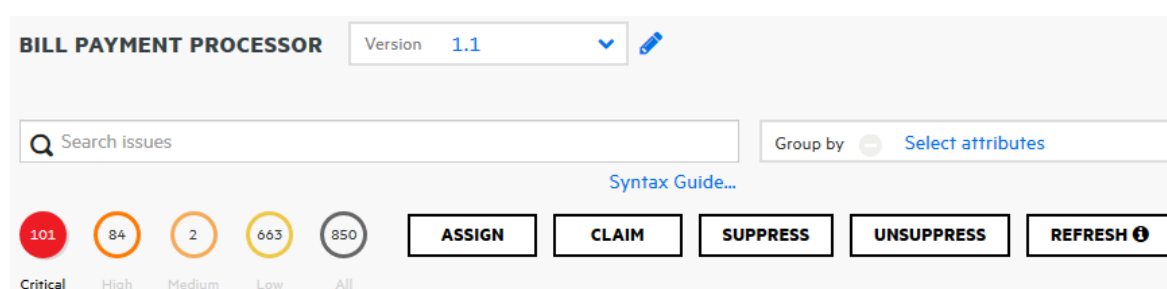


# What's New in Micro Focus Fortify Software Security Center 18.20

The Fortify Software Security Center 18.20 release introduces several new features, which are described here.

## AUDIT Page Redesign

### Fortify Priority Links on the AUDIT and OVERVIEW Pages



The **Critical**, **High**, **Medium**, **Low**, and **All** options that were in the **Filter by** list in previous releases are now displayed on the OVERVIEW and AUDIT pages as links, which you can use to view issues based on the potential risk they pose to the enterprise. For more information, see ["Viewing Issues Based on Fortify Priority" on page 255](#).

On the AUDIT bar, the button previously labeled the **REFRESH TABLE** button is now simply **REFRESH**.

### Relocated Metadata

Previously, to view the metadata associated with an issue, you clicked **METADATA** at the bottom of the expanded issue section. This information is now visible at the bottom of the new **DETAILS** tab located in the right panel of the expanded issue section.

## Security Training Link

If you have a relationship with a secure code training provider such as Secure Code Warrior, you can integrate that training with Fortify Software Security Center. After you do, your users can access context-appropriate guidance as they audit issues in Fortify Software Security Center. For details, see ["Configuring Application Security Training" on page 71](#).

The **CODE** tab on the AUDIT page now includes the **GET TRAINING** button, which you can use to access security training during audits. For information about how to enable or disable secure code training, see ["Configuring Application Security Training" on page 71](#). For information about how to use the feature, see ["About Audit Assistant" on page 265](#).

## Audit Assistant Auto-Prediction

Administrators can now configure Audit Assistant to automatically predict unpredicted issues uncovered during FPR processing. For details, see ["About Audit Assistant Auto-Prediction" on page 75](#).

## Audit Assistant Auto-Apply

You can now enable auto-apply for an application version (after an administrator enables it system-wide). If you do, then whenever you use Audit Assistant to request a prediction on your static analysis issues, Fortify Software Security Center applies those predictions to Fortify Software Security Center Analysis tag values. For details, see ["Enabling Auto-Apply and Auto-Predict for an Application Version" on page 193](#).

## Submitting Dynamic Scan Requests to Fortify WebInspect Enterprise

If Fortify Software Security Center is integrated with Fortify WebInspect, you can now submit dynamic scan requests to WebInspect Enterprise. This feature was previously available in the Fortify Software Security Center legacy (v 4.30) user interface, which is now unavailable. For more information, see ["Submitting Dynamic Scan Requests to Fortify WebInspect Enterprise" on page 283](#).

## Launching Fortify WebInspect

If you are in the role of Fortify Software Security Center Administrator or Application security tester, you can use the new **LAUNCH WIE** button to start Fortify WebInspect Enterprise, and then process dynamic scan requests submitted by Fortify Software Security Center users. For details, see ["Processing Dynamic Scan Requests from Fortify WebInspect Enterprise" on page 285](#).

## Related Documents

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

**Note:** You can find the Micro Focus Fortify Product Documentation at <https://www.microfocus.com/support-and-services/documentation>.

## 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
<p><i>About Micro Focus Fortify Product Software Documentation</i></p> <p>About_Fortify_Docs_&lt;version&gt;.pdf</p>	<p>This paper provides information about how to access Micro Focus Fortify product documentation.</p> <p><b>Note:</b> This document is included only with the product download.</p>
<p><i>Micro Focus Fortify Software System Requirements</i></p> <p>Fortify_Sys_Reqs_&lt;version&gt;.pdf</p> <p>Fortify_Sys_Reqs_Help_&lt;version&gt;</p>	<p>This document provides the details about the environments and products supported for this version of Fortify Software.</p>
<p><i>Micro Focus Fortify Software Release Notes</i></p> <p>FortifySW_RN_&lt;version&gt;.txt</p>	<p>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.</p>
<p><i>What's New in Micro Focus Fortify Software &lt;version&gt;</i></p> <p>Fortify_Whats_New_&lt;version&gt;.pdf</p> <p>Fortify_Whats_New_Help_&lt;version&gt;</p>	<p>This document describes the new features in Fortify Software products.</p>
<p><i>Micro Focus Fortify Open Source and Third-Party License Agreements</i></p> <p>Fortify_OpenSrc_&lt;version&gt;.pdf</p> <p>Fortify_OpenSrc_&lt;version&gt;</p>	<p>This document provides open source and third-party software license agreements for software components used in Fortify Software.</p>

## Micro Focus Fortify CloudScan

The following documents provide information about Fortify CloudScan. Unless otherwise noted, these documents are available on the [Micro Focus Product Documentation](#) website.

Document / File Name	Description
<i>Micro Focus Fortify CloudScan Installation, Configuration, and Usage Guide</i> CloudScan_Guide_<version>.pdf CloudScan_Help_<version>	This document provides information about how to install, configure, and use Fortify CloudScan to streamline the static code analysis process. It is written for anyone who intends to install, configure, or use Fortify CloudScan for offloading the scanning phase of their Fortify Static Code Analyzer process.

## Micro Focus Fortify Software Security Center

The following documents provide information about Fortify Software Security Center. Unless otherwise noted, these documents are available on the [Micro Focus Product Documentation](#) website.

Document / File Name	Description
<i>Micro Focus Fortify Software Security Center User Guide</i> SSC_Guide_<version>.pdf SSC_Help_<version>	<p>This document provides Fortify Software Security Center users with detailed information about how to deploy and use Software Security Center. It provides all of the information you need to acquire, install, configure, and use Software Security Center.</p> <p>It is intended for use by system and instance administrators, database administrators (DBAs), enterprise security leads, development team managers, and developers. Software Security Center provides security team leads with a high-level overview of the history and current status of a project.</p>

## Micro Focus 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.

Document / File Name	Description
<i>Micro Focus Fortify Static Code Analyzer Installation Guide</i> SCA_Install_<version>.pdf SCA_Install_Help_<version>	This document contains installation instructions for Fortify Static Code Analyzer and Applications.
<i>Micro Focus Fortify Static Code Analyzer User Guide</i> SCA_Guide_<version>.pdf SCA_Help_<version>	This document describes how to 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.
<i>Micro Focus Fortify Static Code Analyzer Performance Guide</i> SCA_Perf_Guide_<version>.pdf SCA_Perf_Help_<version>	This document provides guidelines for selecting hardware to scan different types of codebases and offers tips for optimizing memory usage and performance.
<i>Micro Focus Fortify Static Code Analyzer Custom Rules Guide</i> SCA_Cust_Rules_Guide_<version>.zip SCA_Cust_Rules_Help_<version>	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.  <b>Note:</b> This document is included only with the product download.
<i>Micro Focus Fortify Audit Workbench User Guide</i> AWB_Guide_<version>.pdf AWB_Help_<version>	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.
<i>Micro Focus Fortify Plugins for Eclipse Installation and Usage Guide</i>	This document provides information about how to install and use the Fortify Complete and the Fortify Remediation Plugins for Eclipse.

Document / File Name	Description
Eclipse_Plugins_Guide_<version>.pdf  Eclipse_Plugins_Help_<version>	
<i>Micro Focus Fortify Plugins for IntelliJ, WebStorm, and Android Studio Installation and Usage Guide</i>  IntelliJ_AndStud_Plugins_Guide_<version>.pdf  IntelliJ_AndStud_Plugins_Help_<version>	This document describes how to install and use both the Fortify Analysis Plugin for IntelliJ IDEA and Android Studio and the Fortify Remediation Plugin for IntelliJ IDEA, Android Studio, and WebStorm.
<i>Micro Focus Fortify Jenkins Plugin Installation and Usage Guide</i>  Jenkins_Plugin_Guide_<version>.pdf  Jenkins_Plugin_Help_<version>	This document provides how to install, configure, and use the plugin.
<i>Micro Focus Fortify Security Assistant Plugin for Eclipse User Guide</i>  SecAssist_Eclipse_Guide_<version>.pdf  SecAssist_Eclipse_Help_<version>	This document describes how to install and use Fortify Security Assistant plugin for Eclipse to provide alerts to security issues as you write your Java code.
<i>Micro Focus Fortify Extension for Visual Studio User Guide</i>  VS_Ext_Guide_<version>.pdf  VS_Ext_Help_<version>	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.
<i>Micro Focus Fortify Static Code Analyzer Tools Properties Reference Guide</i>  SCA_Tools_Props_Ref_<version>.pdf	This document describes the properties used by Fortify Static Code Analyzer tools.

Document / File Name	Description
SCA_Tools_Props_Ref_Help_<version>	

## Micro Focus Fortify WebInspect

The following documents provide information about Fortify WebInspect. Unless otherwise noted, these documents are available on the [Micro Focus Product Documentation](#) website.

Document / File Name	Description
<i>Micro Focus Fortify WebInspect Installation Guide</i> WI_Install_<version>.pdf WI_Install_Help_<version>	This document provides an overview of Fortify WebInspect and instructions for installing Fortify WebInspect and activating the product license.
<i>Micro Focus Fortify WebInspect User Guide</i> WI_Guide_<version>.pdf	This document describes how to configure and use Fortify WebInspect to scan and analyze Web applications and Web services. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p><b>Note:</b> This document is a PDF version of the Fortify WebInspect 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.</p> </div>
<i>Micro Focus Fortify WebInspect Tools Guide</i> 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.
<i>Micro Focus Fortify WebInspect Runtime Agent Installation Guide</i>	This document describes how to install the Fortify WebInspect Runtime Agent for applications running under a supported Java Runtime

Document / File Name	Description
WI_RT_Agent_Install_<version>.pdf WI_RT_Agent_Install_Help_<version>	Environment (JRE) on a supported application server or service and applications running under a supported .NET Framework on a supported version of IIS.
<i>Micro Focus Fortify WebInspect Agent Rulepack Kit Guide</i> WI_Agent_Rulepack_Guide_<version>.pdf WI_Agent_Rulepack_Help_<version>	This document describes the detection capabilities of Fortify WebInspect Agent Rulepack Kit. Fortify WebInspect Agent Rulepack Kit runs atop the Fortify Runtime 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.

## Micro Focus 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.

Document / File Name	Description
<i>Micro Focus Fortify WebInspect Enterprise Installation and Implementation Guide</i> WIE_Install_<version>.pdf WIE_Install_Help_<version>	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.
<i>Micro Focus Fortify WebInspect Enterprise User Guide</i> 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.  <b>Note:</b> This document is a PDF version of the Fortify WebInspect Enterprise help. This PDF file is provided so you can easily print multiple topics from the help



Document / File Name	Description
	<p>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.</p>
<p><i>Micro Focus Fortify WebInspect Tools Guide</i> WI_Tools_Guide_&lt;version&gt;.pdf</p>	<p>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.</p>

# 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.

### 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.

**Important!** If you use SSL, keep in mind that Fortify *does not* support deploying Fortify Software Security Center to a container that uses self-signed certificates.

### Configuring and Fortify Static Code Analyzer Tools 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 -import -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 -export -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 65](#).

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 165](#).

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 53](#).

## **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 140](#).

Task	Description	Information and Instructions
1	Download the Fortify Software Security Center software files and the <code>fortify.license</code> file.	<a href="#">"Downloading Fortify Software Security Center Files" on page 43</a>
2	Prepare Tomcat Server for Fortify Software Security Center deployment.	<a href="#">"Deploying Fortify Software Security Center in Tomcat Server" on page 56</a>
3	Unpack and deploy the installation bundle. Then deploy Fortify Software Security Center in Tomcat Server.	<a href="#">"Unpacking and Deploying Fortify Software Security Center Software" on page 43</a>
4	Install and configure the software for the database server you plan to use for the Fortify Software Security Center database.	<a href="#">"About the Fortify Software Security Center Database" on page 44</a>
5	Configure the JDBC driver you plan to use so that Tomcat Server can access it.	<a href="#">"Adding the JDBC Driver to Fortify</a>

Task	Description	Information and Instructions
		<a href="#">"Software Security Center" on page 45</a>
6	Log in to Fortify Software Security Center. (See <a href="#">"Logging in to Fortify Software Security Center" on page 65</a> )	<a href="#">"Logging in to Fortify Software Security Center" on page 65</a>
7	Use the Fortify Software Security Center Setup wizard to perform initial configuration. (Locate your Fortify license, create the Fortify Software Security Center database tables and initialize the database schema, seed the database, and so on.)	<a href="#">"Configuring Fortify Software Security Center for the First Time" on page 60</a>
8	Restart the Fortify Software Security Center server.	
9	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 <a href="#">"Configuration Options Available in the ADMINISTRATION View" on page 68.</a> )	<a href="#">"Additional Fortify Software Security Center Configuration" on page 66</a>
10	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.	<a href="#">"Additional Installation-Related Tasks" on page 119</a>

This section also contains information about the JDBC drivers that are required to interface with the database.

If you no longer need the Fortify Software Security Center database, you can find instructions on how to permanently delete it in this section (["Permanently Deleting a Fortify Software Security Center Database" on page 52](#)).

## 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 CloudScan, 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.

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 66.

**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.

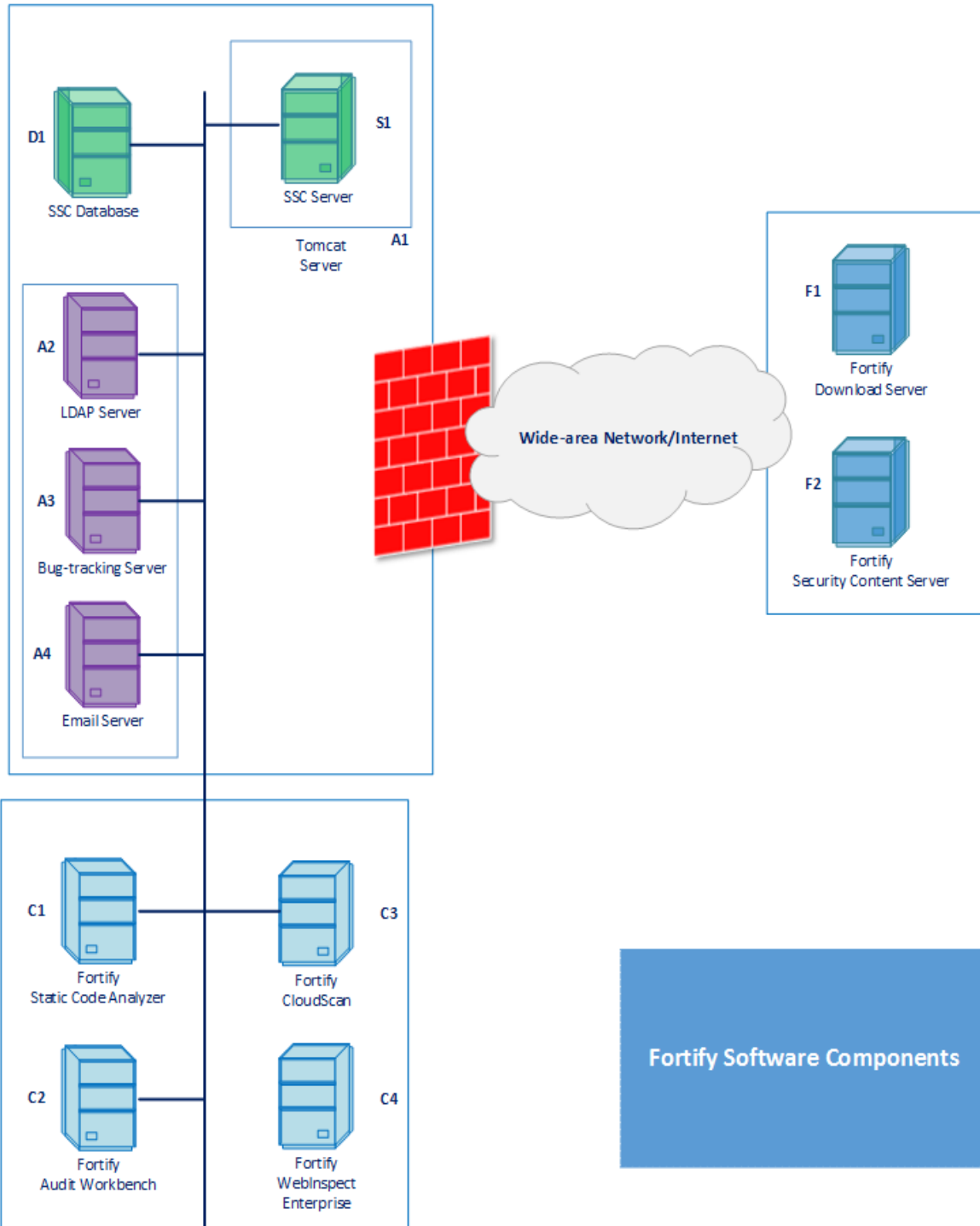
To provide centralized management, Fortify Software Security Center inter-operates with the following external components:

- 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



### 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 39.



The following table provides descriptions of the required and optional Fortify Software Security

Center installation components illustrated here.

ID	Description
S1	<p>Fortify Software Security Center</p> <p>Fortify Software Security Center is delivered as a Web Archive (WAR) file run by Tomcat Server (A1).</p>
D1	<p>Third-party database that Fortify Software Security Center requires to store user and artifact data.</p> <p>Before you put Fortify Software Security Center into production, you must install a supported third-party database.</p>
A1	<p>Tomcat Server</p> <p>Fortify Software Security Center (S1) is delivered as a Web Archive (WAR) file and run by Tomcat.</p>
A2	<p>Optional third-party LDAP authentication server</p> <p>You can configure Fortify Software Security Center to use LDAP authentication.</p>
A3	<p>Optional defect-tracking server</p> <p>You can configure Fortify Software Security Center to enable bug submission directly to Bugzilla, JIRA, ALM, Team Foundation Server (TFS), or a customized bug-tracking system.</p>
A4	<p>Optional third-party email server</p> <p>You can configure Fortify Software Security Center to use an external SMTP email server to send alerts to application collaborators.</p>
C1	<p>Optional Fortify Static Code Analyzer analysis agent</p> <p>Fortify Static Code Analyzer scans source code and identifies issues.</p>
C2	<p>Audit Workbench source code auditing tool</p> <p>Although it is technically optional, most Fortify Software Security Center installations use Audit Workbench to audit issues and categorize vulnerabilities.</p>
C3	<p>Fortify CloudScan</p> <p>Cloud of machines used to handle the processor-intensive scanning phase of static code analysis.</p>

ID	Description
C4	Optional analysis agent - Fortify WebInspect Enterprise Connects with Fortify WebInspect agents to retrieve issue audit information.
F1	Fortify download server Used to acquire installation programs.
F2	Fortify Security Content update server Used to acquire and update Security Content.

Fortify Software Security Center must be configured to work with the external components shown in the previous figure. The external components must also be configured to work with Fortify Software Security Center.

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

## Downloading Fortify Software Security Center Files

Fortify software is available only as an electronic download from the [Fortify Customer Portal](#). For descriptions of the Fortify software installation packages available there, see the *Micro Focus Fortify Software System Requirements* document.

Download the Fortify Software Security Center installation files and the `fortify.license` file following the instructions in the *Micro Focus Fortify Software System Requirements* document.

### 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_Seed_Bundle-2018_Q3.zip	Process template seed bundle used to seed your third-party database tables. It provides a default admin user account and issue template data.
Fortify_Report_Seed_Bundle-2018_Q3.zip	Report seed bundle used to seed the third-party database tables. It provides the default set of Fortify Software Security Center reports.
Fortify_PCI_Basic_Seed_Bundle-2018_Q3.zip	(Optional) PCI Basic seed bundle adds a Payment Card Industry process template and its associated report to the default set of issue templates and reports.

The process templates seed bundle and the reports seed bundle are required for Fortify Software Security Center deployment. The PCI Basic seed bundle is 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 *Micro Focus Fortify Software System Requirements* document.)

## 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 47](#) or ["Configuring a MySQL Database" on page 48](#).

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 60.](#))

Topics covered in this section:

<a href="#">About JDBC Drivers</a>	45
<a href="#">About Fortify Software Security Center Database Character Set Support</a>	46
<a href="#">Installing and Configuring the Database Server Software</a>	46
<a href="#">Database User Account Privileges</a>	46
<a href="#">Database-Specific Configuration Requirements</a>	47
<a href="#">About the Fortify Software Security Center Database Tables and the Schema</a>	51
<a href="#">About Seeding the Fortify Software Security Center Database</a>	52
<a href="#">Permanently Deleting a Fortify Software Security Center Database</a>	52

## About JDBC Drivers

Licensing prohibits Fortify Software Security Center from including the JDBC drivers that are required to interface with the supported third-party databases. You must obtain the JDBC JAR files required to support the type and version of third-party database you plan to use with Fortify Software Security Center.

**Important!** Before you deploy Fortify Software Security Center for the first time or upgrade an existing instance, you must first verify that the Tomcat Server classpath includes the location of the JDBC driver.

For information about the database driver classes that Fortify Software Security Center supports, see the *Micro Focus Fortify Software System Requirements* document. For instructions on how to add the JDBC driver to the system, see ["Adding the JDBC Driver to Fortify Software Security Center" below.](#)

### Adding the JDBC Driver to Fortify Software Security Center

To add the JDBC driver to Fortify Software Security Center, do one of the following:

- (Recommended) Add the JDBC JAR file location to the Tomcat Server classpath. For instructions on how to include the library on the classpath, see the Tomcat Server documentation.
- Do the following only if adding the JDBC driver file location to the classpath might interfere with another application deployed on Tomcat:
  - a. Unzip the Fortify Software Security Center installation bundle for your application server (Fortify\_<version>\_Server\_WAR\_Tomcat.zip).
  - b. Unzip the ssc.war file.

- c. Open the **WEB-INF** folder, and then place the JDBC JAR file in the **lib** folder.
- d. Save the SSC WAR file, and then re-zip the installation bundle.

## 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.

## 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 SELECT, UPDATE, INSERT, and DELETE operations in all the database tables
- 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 SELECT, UPDATE, INSERT, and DELETE operations in all the database tables
- Execute stored procedures
- 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 Fortify Software Security Center for BIRT Reporting" on page 79](#)).

## 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:

- 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 installation is *case-insensitive*, Fortify Software Security Center does not work correctly.

- 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.
- For Windows domain authentication, make sure that you add `integratedSecurity=true` to the JDBC URL.

## 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 *Micro Focus 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 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 5.7 is `c:\ProgramData\MySQL\MySQL Server 5.7`.

- 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
<code>innodb_log_file_size</code>	512M (Fortify recommends 2.5GB or more) Set this to approximately 25 to 100 percent of your <code>innodb_buffer_pool_size</code> value. Note, however, that increasing this value increases recovery time.
<code>innodb_lock_wait_timeout</code>	300 (recommended) Expressed in seconds



Setting	Value
wait_timeout	
query_cache_type	Any non-zero value
query_cache_size	Between 64M and 228M
innodb_buffer_pool_size	512M (Fortify recommends 10GB or more)  <b>Note:</b> If you increase this value without also increasing the innodb_log_file_size value, uploads of large FPR files can fail.
default-storage-engine	INNODB
innodb_file_format	Barracuda
innodb_large_prefix	1
sql_mode	TRADITIONAL  <b>Note:</b> MySQL 5.7.5 and later versions have a default sql_mode setting that includes the ONLY_FULL_GROUP_BY flag. This option is incompatible with the queries that Fortify Software Security Center issues.

6. Make sure that MySQL is set up with Barracuda or a newer file format to enable the dynamic row format feature. For more information, see the MySQL documentation for the innodb file format and for dynamic row formats.
7. 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
  - 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 the 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 60](#)), 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 46](#)
- ["Database-Specific Configuration Requirements" on page 47](#)

## 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 43):

- The issue template seed bundle (Fortify\_Process\_Seed\_Bundle-2018\_Q3.zip) provides a default admin user account and issue template data.
- The report seed bundle (Fortify\_Report\_Seed\_Bundle-2018\_Q3.zip) provides the default set of Fortify Software Security Center reports.

You can also install the optional PCI Basic Bundle (Fortify\_PCI\_Basic\_Seed\_Bundle-2018\_Q3.zip), which adds a Payment Card Industry process template and an associated report 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.)

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 66.

### See Also

["Seeding the Database with Report Seed Bundles Delivered with Quarterly Security Content Releases"](#) on page 147

## Permanently Deleting a 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
```

## 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!** Although Fortify supports the use of multiple LDAP servers, it does not support the use of multiple LDAP servers behind a load balancer.

**Note:** For information about how to manage LDAP entities and user roles in Fortify Software Security Center, see ["Registering LDAP Entities" on page 173](#) and ["About Managing LDAP User Roles" on page 128](#).

Topics covered in this section:

<a href="#">About Fortify Software Security Center User Authentication</a> .....	53
<a href="#">Preparing to Configure LDAP Authentication</a> .....	54
<a href="#">About the LDAP Server Referrals Feature</a> .....	55
<a href="#">Disabling LDAP Referrals Support</a> .....	55

### 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. The default database-only authentication method can be augmented by using LDAP to authenticate users. Most

administrators prefer to augment the Fortify Software Security Center default database-only authentication with LDAP. LDAP authentication enables a single administrative process to manage user authentication for multiple network entities, including Fortify Software Security Center. You can configure Fortify Software Security Center to augment its native database-only user authentication with LDAP user authentication.

## 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.

If your LDAP server does not permit anonymous binding, create a read-only LDAP account for Fortify Software Security Center to use. Fortify Software Security Center requires an account with permissions necessary to read user attributes and authenticate users. (Even if your LDAP server supports anonymous binding, you may prefer to create an LDAP read-only account for Fortify Software Security Center.)

**Note:** For information about how to configure the primary source looking up users, see "[Configuring Core Settings](#)" on page 82.

**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 the next page.

### See Also

["Configuring LDAP Servers" on page 89](#)

## 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](#)" below.

**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 panel, 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**.

## Chapter 4: Deploying Fortify Software Security Center in Tomcat Server

The topics in this section provide instructions on how to prepare Tomcat Server for Fortify Software Security Center deployment, and then deploy Fortify Software Security Center in Tomcat Server.

After you deploy Fortify Software Security Center, complete the configuration tasks in the ADMINISTRATION view in Fortify Software Security Center. For information and instructions, see ["Additional Fortify Software Security Center Configuration" on page 66](#).

**Note:** By default, Fortify Software Security Center log files are written to the `<fortify.home>/<appcontext>/logs` directory. To change the location of Fortify Software Security Center logs, set the `com.fortify.ssc.logPath` JVM system property to point to a different path.

**Important!** Fortify Software Security Center has not been tested against clustered application servers. Information about how Fortify Software Security Center performs for application servers running in clustered mode is unavailable. Contact your administrator if you require a clustered server configuration.

Topics covered in this section:

<a href="#">About the fortify.home Directory</a> .....	57
<a href="#">Directory Structure</a> .....	57
<a href="#">About Secure Deployment</a> .....	58
<a href="#">About Deploying Fortify Software Security Center in Apache Tomcat</a> .....	58
<a href="#">Tomcat Memory Settings</a> .....	58
<a href="#">About Configuring the Tomcat Connectors</a> .....	59
<a href="#">Configuring Tomcat to Unpack WAR Files</a> .....	59
<a href="#">Deploying Fortify Software Security Center in Tomcat Server</a> .....	59



## About the fortify.home Directory

The `fortify.home` directory is where the configuration file and other Fortify Software Security Center resources reside. After Fortify Software Security Center deployment, you can find it in:

- `C:\Users\<username>\.fortify` on a Windows system
- `C:\Windows\System32\config\systemprofile\.fortify` if Tomcat is running as a Windows service
- `<user.home>/.fortify` on a Linux system

**Note:** Although these are the default directories, you can specify a different directory using the Setup wizard during configuration. (See "[Configuring Fortify Software Security Center for the First Time](#)" on page 60.)

## Directory Structure

The `fortify.home` directory is structured as follows:

```
<fortify.home>/
  <app_context>/
    conf/
      app.properties
      datasource.properties
      log4j2.xml
      version.properties
    logs/
      ssc.log
      ...
    init.token
  fortify.license
  plugin-framework/
```

where

<code>log4j2.xml</code>	is the log configuration, which you can change on the fly.
<code>init.token</code>	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 <code>&lt;host&gt;:&lt;port&gt;/init</code> URL.
<code>app.properties</code>	is a file that contains the application properties that the customer can configure (extracted from <code>ssc.properties</code> ).

<code>datasource.properties</code>	is a file that contains the database connection properties.
<code>version.properties</code>	is a file that stores information about current and previous versions of Fortify Software Security Center for application upgrade purposes.
<code>plugin-framework</code>	is the plugin framework configuration and temporary storage (internal).
<code>fortify.license</code>	is the license file for Fortify Software Security Center.

## About Secure Deployment

Secure deployment is particularly important for Tomcat Server configuration, operation, and communications. For more information, see ["Securing Tomcat Server" on page 35](#) and ["Setting Tomcat Server Attributes to Protect Sensitive Data in Cookies" on page 35](#).

## About Deploying Fortify Software Security Center in Apache Tomcat

The following topics describe what you need to do to deploy Fortify Software Security Center in Tomcat Server.

### Tomcat Memory Settings

To enable Fortify Software Security Center to use several frameworks that dynamically subclass an application's core classes, you must specify the memory settings for Tomcat Server. Dynamic subclassing requires an increased number of class definitions in the Java runtime's permanent memory heap.

**Note:** Configuring Tomcat memory does not impair server runtime performance or runtime environment behavior.

Configure the java heap size for Fortify Software Security Center based on the requirement stated in the *Micro Focus Fortify Software System Requirements* document. If you are working with very large number of artifacts and applications, you might need to set the java heap size higher than the stated requirement.

## About Configuring the Tomcat Connectors

Configure the Tomcat connectors and ports, as necessary. See the Tomcat documentation for instructions on how to configure the connectors and set up SSL/TLS (if required).

If you only need to modify the default ports, edit the `<tomcat>/conf/server.xml` file.

### See Next

["Deploying Fortify Software Security Center in Tomcat Server" below](#)

## Configuring Tomcat to Unpack WAR Files

Fortify Software Security Center does not run correctly in Tomcat if Tomcat is configured *not* to unpack WARs.

The Tomcat `unpackWars` attribute must be set to `true` on Tomcat's host configuration, and on its context configuration. (The values are set to `true` by default.)

For information about how to set the `unpackWars` attribute, see Apache Tomcat documentation.

**Note:** Setting the value for the context configuration takes precedence over the value for the host configuration.

## Deploying Fortify Software Security Center in Tomcat Server

To deploy Fortify Software Security Center in Tomcat Server:

1. After you prepare the database schema and run `create-tables.sql`, stop Tomcat Server.
2. Navigate to the `<tomcat>/webapps` directory.
3. If the `<tomcat>/webapps` directory contains the `ssc` subdirectory, delete the subdirectory.
4. Copy the `ssc.war` file to the `<tomcat>/webapps` directory.

**Note:** You can change the default context root name (`ssc`) by renaming the `ssc.war` file, or by setting the context root in deployment parameters.

5. Start Tomcat Server:

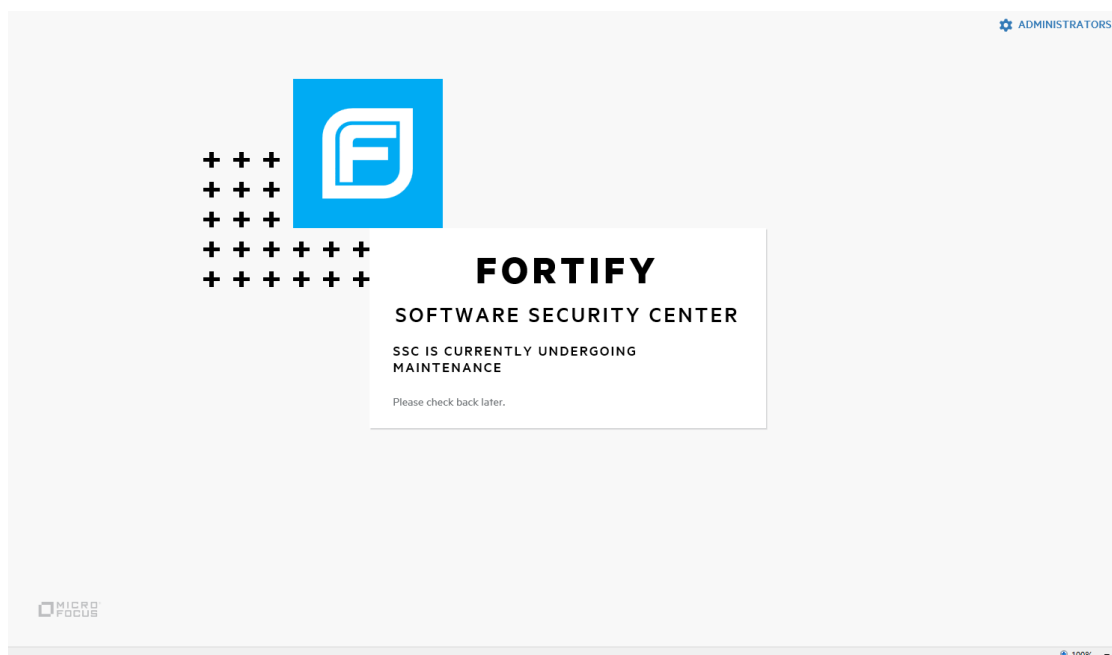
**Important!** Fortify only supports the deployment of a single Fortify Software Security Center instance. Furthermore, that instance must not be behind a load balancer.

## Chapter 5: Configuring Fortify Software Security Center for the First Time

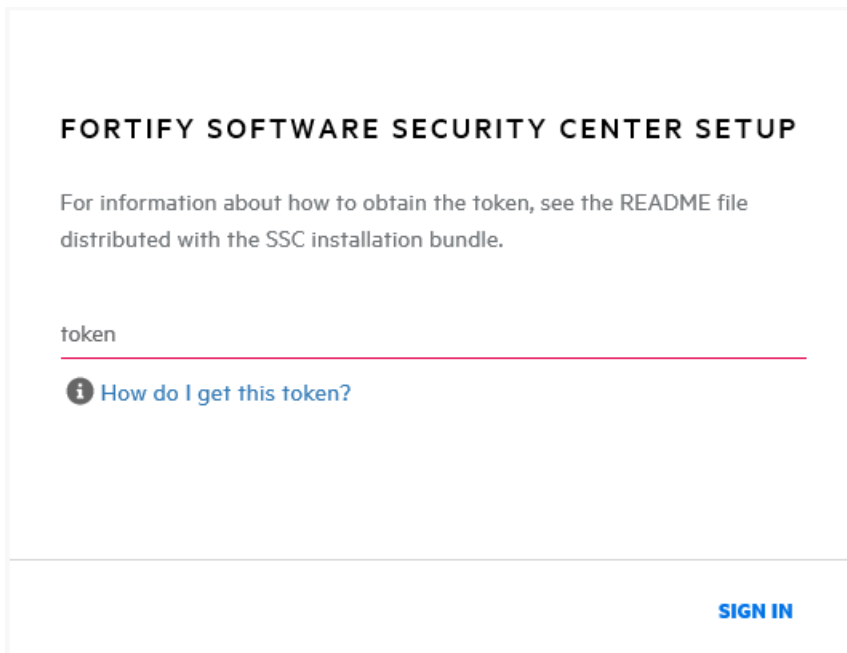
After you deploy Fortify Software Security Center for the first time and then enter the Fortify Software Security Center URL in a browser window, the Fortify Software Security Center Setup wizard (Setup wizard) opens. Here, you can complete the steps for the initial server configuration. The Setup wizard 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 133](#)).

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>/`).



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 57), 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**.

The Fortify Software Security Center Setup wizard opens.

6. Read the information on the **START** page of the 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 panel 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. If you want to save your configuration properties file in a directory other than the default shown, on Tomcat Server, specify a different path for the JVM system property `fortify.home`.

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

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 panel, 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 panel, 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 panel, 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 46](#).
  - 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 46](#).

- d. In the **JDBC URL** box, type the URL for the Fortify Software Security Center database.

If you are using a MySQL Server database, you must append the following property setting to the end of the URL:

```
connectionCollation=COLLATION  
where COLLATION is the collation type of your database.
```

**Examples:**

```
jdbc:mysql://localhost:3306/ssc?connectionCollation=utf8_bin
jdbc:mysql://localhost:3306/ssc?connectionCollation=latin1_
general_cs
```

**Important!** If you are using a MSSQL Server database, you must append the following property setting to the end of the URL:

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

- 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.
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 the Schema" on page 51](#).
14. After you initialize the database, click **NEXT**.
15. On the **DATABASE SEEDING** step, do the following:
- a. In the left panel, use **BROWSE** to locate and select your `Fortify_Process_Seed_Bundle-2018_Q3.zip` file, and then click **SEED DATABASE**.
  - b. Use **BROWSE** to locate and select your `Fortify_Report_Seed_Bundle-2018_Q3.zip` file, and then click **Seed Database**.
  - c. (Optional) Use **BROWSE** to locate and select your `Fortify_PCI_Basic_Seed_Bundle-2018_Q3.zip` file, and then click **SEED DATABASE**.
16. Click **NEXT**.
17. Click **FINISH**.
18. 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 66](#).)

**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 133](#).



## Chapter 6: 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, 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 124](#).

To log in to Fortify Software Security Center:

1. In a web browser, type the URL for your Fortify Software Security Center instance:
  - If Fortify Software Security Center is configured to use secure HTTPS protocol, type the following URL:

```
https://<host_IP>:<port>/<ssc>/
```

where *<port>* represents the port number used by Tomcat Server and *<ssc>* is the context root name.

- 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 used by Tomcat Server and *<ssc>* is the context root name.

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

["Additional Fortify Software Security Center Configuration" on page 66](#)

## Chapter 7: 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.

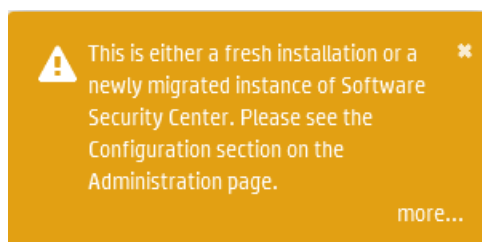
You can configure and update other settings in the ADMINISTRATION view later, as necessary.

### 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 65](#).
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**.

The ADMINISTRATION view opens. The navigation panel 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 panel, select **Configuration**.

The panel displays the configuration category options. For information about these options, see ["Configuration Options Available in the ADMINISTRATION View" on page 68](#).

## 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 than 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 panel, 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.

The screenshot shows a configuration window titled "THRESHOLDS". It contains three main sections:

- Max Issue Age**: A text input field containing the value "365".
- Average Days to Review**: A slider control with a green segment on the left and a yellow segment on the right. Below the slider are two text input fields: "Min." with the value "100" and "Max." with the value "365".
- Average Days to Remediate**: A slider control identical to the one above. Below it are "Min." and "Max." text input fields, both containing "100" and "365" respectively.

At the bottom of the window are two buttons: "CANCEL" and "SAVE".

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 panel, 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 make the <b>GET TRAINING</b> button available on the issue details section of the AUDIT page.	<a href="#">"Configuring Application Security Training" on page 71</a>
Audit Assistant	Use to enable and configure Audit Assistant, which uses Fortify Scan Analytics to automatically audit Fortify Static Code Analyzer scans.	<a href="#">"Configuring Audit Assistant" on page 74</a>
BIRT Reports	Use to apply enhanced security to reporting in Fortify Software Security Center.	<a href="#">"Configuring Fortify Software Security Center for BIRT Reporting" on page 79</a>
CloudScan	Use to configure Fortify Software Security Center to monitor CloudScan and to display CloudScan results in Fortify Software Security Center.	<a href="#">"Configuring CloudScan Monitoring in Fortify Software Security Center" on page 81</a>
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.	<a href="#">"Configuring Core Settings" on page 82</a>
Email	Use to configure the server settings used to send email alerts to users.	<a href="#">"Configuring Email Alert Notification Settings" on page 85</a>
Issue Audit	Use to select the setting that determines how issue audit conflicts are resolved.	<a href="#">"Setting the Strategy for Resolving Issue Audit Conflicts" on page 248</a>
JMS	Use to configure Fortify Software Security Center to publish system events to the Java Message Service (JMS).	<a href="#">"Configuring Java Message Service Settings" on page 88</a>
LDAP Servers	Use to configure LDAP authentication	<a href="#">"Configuring LDAP Servers" on</a>

Option	Description	Instructions
	and LDAP server options for one or more LDAP servers.	<a href="#">page 89</a>
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.	<a href="#">"Placing Fortify Software Security Center in Maintenance Mode" on page 133</a>
Proxy	Use to configure a single proxy for Rulepack updates, the connection to Audit Assistant, and for bug tracker plugins.	<a href="#">"Configuring a Proxy for Fortify Software Security Center Integrations" on page 103</a>
Scheduler	Use to configure the Fortify Software Security Center job scheduler settings.	<a href="#">"Configuring Job Scheduler Settings" on page 104</a>
Security	Use to configure the Fortify Software Security Center security features.	<a href="#">"Configuring Browser Access Security for Fortify Software Security Center" on page 109</a>
Seed Bundles	Use to seed the database with seed bundles distributed in a quarterly security content release.	<a href="#">"Seeding the Database with Report Seed Bundles Delivered with Quarterly Security Content Releases" on page 147</a>
SSO	Use to configure Fortify Software Security Center to work with one of the following SSO solutions: <ul style="list-style-type: none"> <li>• CAS SSO</li> <li>• SPNEGO/Kerberos SSO</li> <li>• SAML SSO</li> <li>• HTTP SSO</li> <li>• X.509 SSO</li> </ul>	<a href="#">"Configuring Fortify Software Security Center to Work with Single Sign-On" on page 110</a>
Web Services	Use to configure Fortify Software Security Center web services.	<a href="#">"Configuring Web Services to Require Token Authentication" on page 117</a>

## 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 panel, 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 Micro Focus Fortify Customer Support (<https://softwaresupport.softwaregrp.com>).
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 Issues" on page 249](#)

## 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 Community Intelligence data (pooled, anonymized data from Fortify users), audit data that your security team has completed, or data from both sources. This data provision is referred to as *training*. Audit Assistant's assessments of the actual threats that issues represent become more accurate as it receives more training data.

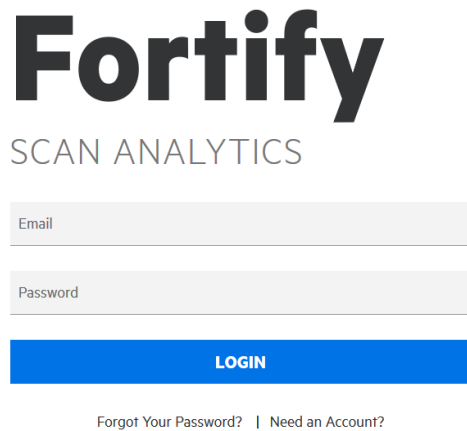
You can submit training data (metadata derived from historical human-audited scan results) without having submitted anything for prediction. This gives you access to the Fortify Community Intelligence data set. If you choose *not* to share your training data, and so do not have access to the Fortify Community Intelligence data set (default configuration), then you must submit your own training data before you can get valid assessments from Audit Assistant.

Audit Assistant can also learn through corrections that are included in the training 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.

## 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>.



Fortify

SCAN ANALYTICS

Email

Password

LOGIN

[Forgot Your Password?](#) | [Need an Account?](#)

- 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 classifiers.
3. From Fortify Scan Analytics, create one or more policies.
4. (Optional) Choose to share anonymous metadata.
5. Obtain a Fortify Scan Analytics token.
6. 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 74).
  - 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.
7. 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*.
8. From Fortify Software Security Center, open an application version and submit its Fortify Static Code Analyzer scan results to Audit Assistant.
9. After Audit Assistant completes its assessment, view those results and, if necessary, adjust



them.

10. 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**

["Configuring Audit Assistant" on the next page](#)

["About Classifiers and Prediction Policies" on page 267](#)

["Defining Classifiers" on page 268](#)

["Defining a Catch-All Classifier" on page 271](#)

["Defining Prediction Policies" on page 271](#)

["Enabling Metadata Sharing" on page 273](#)

["Enabling Auto-Apply and Auto-Predict for an Application Version" on page 193](#)

["Submitting Training Data to Audit Assistant" on page 274](#)

["Reviewing Audit Assistant Results" on page 274](#)


**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" on the next page](#).)

### 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 panel, select **Configuration**, and then select **Audit Assistant**.
3. Configure the settings on the Audit Assistant page as described in the following table.

Field	Description
* Required	
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 <b>How do I get a token?</b> or, see <a href="#">"Getting a Fortify Scan Analytics Authentication Token"</a> on the previous page.
*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 <a href="#">"Configuring a Proxy for Fortify Software Security Center Integrations"</a> on page 103, 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 default policy for an application version from the APPLICATION PROFILE dialog box. For instructions, see ["Configuring Audit Assistant Options for an Application Version" on page 211](#).

8. To enable Audit Assistant to automatically send unaudited issues 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" below](#).)
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.

**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 following 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.

## Auto-prediction enablement

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 74.) 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 193.)

## 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 74), 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, the mapped custom tag must be designated as the primary custom tag.

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 panel of the ADMINISTRATION view, select **Templates**, and then select **Custom Tags**.

Or

 Before you use this feature, you **must** map Audit Assistant analysis tag values to SSC Analysis tag values. To start, save your settings here, then click [here](#).

- At the bottom of the Audit Assistant page, click the **here** link.

The Custom Tags page opens.

2. At the top right of the page, select the **Show Audit Assistant-compatible** check box.
3. Expand the row for a list-type custom tag (such as Analysis) for which you want to map values.

**Name** ◯      **Description** ◯      **Type** ◯   **Extensible** ◯   **Restricted** ◯   **Hidden** ◯

Analysis      The analysis tag must be set for an issue to be counted as 'Audited.' This is encouraged to be the final action performed by an auditor.      LIST

**Name**

**Description**

Restricted ⓘ       Extensible ⓘ       Hidden ⓘ

Value	Description	AA Mapping	Hidden
Not an Issue			
Reliability Issue			
Bad Practice			
Suspicious			
Exploitable			

**Default Value**

**Audit Assistant Guidance**

**Non-Issue**

**True Issue**

DELETE    EDIT

4. At the bottom right of the expanded row, click **EDIT**.

**Name** ◯      **Description** ◯      **Type** ◯   **Extensible** ◯   **Restricted** ◯   **Hidden** ◯

Analysis      The analysis tag must be set for an issue to be counted as 'Audited.' This is encouraged to be the final action performed by an auditor.      LIST

**Name** ◯

**Description**

Restricted ⓘ       Extensible ⓘ       Hidden ⓘ

+ ADD VALUE

Value	Description	AA Mapping	Hidden
Not an Issue			<input checked="" type="checkbox"/> <input type="text"/>
Reliability Issue			<input checked="" type="checkbox"/> <input type="text"/>
Bad Practice			<input checked="" type="checkbox"/> <input type="text"/>
Suspicious			<input checked="" type="checkbox"/> <input type="text"/>
Exploitable			<input checked="" type="checkbox"/> <input type="text"/>

**Default Value**

**Audit Assistant Guidance**

To specify which custom tag values signify issues that are of real concern, and which signify issues that are benign and can be ignored, place each tag value in either **Non-Issue** or **True Issue** box. Audit Assistant uses this information to classify issues as false positives or real issues.

**Non-Issue**           

**True Issue**           

CANCEL    SAVE

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

Value	Description	AA Mapping	Hidden	Edit value
Not an Issue				
Reliability Issue				
Bad Practice				
Suspicious				
Exploitable				

5. Select the **Edit value** icon () for a listed value.

EDIT VALUE

**Name\***

Not an Issue
×

**Description**

**AA Custom Tags**

Not an Issue

Indeterminate (Below Not An Issue threshold)

Exploitable

Hidden

CANCEL

APPLY

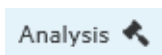
The EDIT VALUE dialog box opens.

6. Under **AA Custom Tags**, select the check box for the value you issues that have this custom tag value.
7. Click **APPLY**.

Value	Description	AA Mapping	Hidden	Edit value
Not an Issue		Not an Issue		
Reliability Issue				
Bad Practice				
Suspicious				
Exploitable				

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

8. Complete steps 5 through 7 for all of the values that you want to map for automated autiding.
9. 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 Guidance** section is used for data training purposes. For information about how to configure this section, see ["Adding Custom Tags to the System" on page 212](#).

## Configuring Fortify Software Security Center 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 panel, 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**.

### 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	filterset	requirement
activitycomment	folder	requirementcomment
activityinstance	foldercountcache	requirementinstance

attr	issuecache	requirementtemplate
auditattachment	measurement	requirementtemplatecomment
auditcomment	measurementhistory	requirementtemplateinstance
catpackexternalcategory	metadef	sdlhistory
catpackexternallist	metadef_t	sourcefile
catpacklookup	metaoption	snapshot
datablob	metaoption_t	userpreference
documentinfo	metavalue	variable
eventlogentry	projecttemplate	variablehistory
<b>Views</b>		
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 panel, 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 **TEST CONNECTION**.
8. Click **SAVE**.

**See Also**

["Allocating Memory for Report Generation" below](#)

["Setting Report Generation Timeout" on the next page](#)

**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 panel, 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 panel, 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 CloudScan Monitoring in Fortify Software Security Center

With Fortify CloudScan, 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 Fortify CloudScan and display its results in Fortify Software Security Center. You can also create and manage CloudScan sensor pools. To enable this functionality, you must configure the integration in Fortify Software Security Center.

To configure the integration between Fortify Software Security Center and Fortify CloudScan:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, click **ADMINISTRATION**.
2. In the left panel of the ADMINISTRATION view, select **Configuration**, and then select **CloudScan**.  
The CloudScan page opens.
3. Select the **Enable CloudScan** check box.
4. In the **CloudScan Controller URL** box, type the URL for your CloudScan controller.

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

5. In the **CloudScan poll period (seconds)** box, type the number of seconds to elapse between sessions of data polling from CloudScan.
6. In the **SSC and CloudScan controller shared secret** box, type the password for Fortify Software Security Center to use when it requests data from the CloudScan Controller.  
The CloudScan Controller verifies the password when requested for administration console data. This string must match the value stored in the CloudScan Controller `config.properties` file for the `ssc_cloudctr1_secret` key.

7. Click **SAVE**.
8. Restart the Fortify Software Security Center server.

## 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 85](#).

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 panel of the ADMINISTRATION view, select **Configuration**, and then select **Core**. The **Core** page opens.
3. 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 before lockout	Number of times a 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 <b>Lockout time (minutes)</b> box. <b>Note:</b> For information about how to unlock a user account, see <a href="#">"Unlocking User Accounts (Local Users Only)" on page 172</a> . The default value is 3.

Field	Description
Lockout time (minutes)	If a user attempts and fails to log in to Fortify Software Security Center the number of times specified for <b>Login Attempts before Lockout</b> , Fortify Software Security Center locks the user account for the number of minutes specified in the <b>Lockout time (minutes)</b> box.  The default value is 30.
User lookup strategy	If LDAP is enabled, select one of the following user lookup strategies from this list: <ul style="list-style-type: none"> <li> <span data-bbox="505 642 1260 674">• <b>Local users first, fallback to LDAP users (compatibility)</b></span>                          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.                     </li> <li> <span data-bbox="505 842 1052 873">• <b>LDAP users first, fallback to local users</b></span>                          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.                     </li> <li> <span data-bbox="505 1041 1224 1073">• <b>LDAP users exclusive, fallback to local administrator</b></span>                          (Recommended strategy for SSO) Search LDAP users only, and allow local administrator access.                     </li> </ul>
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 WebInspect Agent Issue	Determines the maximum number of events to log within a single Fortify WebInspect Agent issue. After that threshold is reached, new events related to the same issue are ignored.  The default value is 5.
Inactive session timeout	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.

Field	Description
(minutes)	
Locale for Rulepacks	Type one of the following: <ul style="list-style-type: none"> <li>• en (English)</li> <li>• ja (Japanese)</li> <li>• zh_CN (simplified Chinese)</li> <li>• zh_TW (traditional Chinese)</li> <li>• es (Spanish)</li> <li>• pt_BR (Portuguese Brazilian)</li> </ul>
Rulepack update URL	URL for the Fortify Rulepack update site. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Important!</b> Do not change the default value of the <b>Rulepack Update URL</b> field unless your Fortify Customer Support (<a href="https://softwaresupport.softwaregrp.com">https://softwaresupport.softwaregrp.com</a>) representative directs you to do so.</p> </div> <p>The default value is <code>https://update.fortify.com</code></p>
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. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> The Fortify Software Security Center must be enabled and correctly configured.</p> </div>
Base URL for runtime event description server	The runtime event details include a link to a description of the event category, which is hosted on a Fortify Software Security Center instance. If you do not want your Fortify Software Security Center instance to access the Internet, change the base URL for the event category descriptions. <p>The default value is <code>https://content.fortify.com/products/360/rta/descriptions/</code>.</p>
User Administrator's email	Type the email address of the user who is to receive system email alerts and notifications when email notifications are enabled. <p>Requests for new user accounts are sent to this address when the <b>Can't</b></p>

Field	Description
address (for user account requests)	<b>access or need an account?</b> link is available on the Fortify Software Security Center login page.
Enable export to CSV	Select this check box to enable users to export Fortify Software Security Center data to comma-separated values files.  <b>Note:</b> 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 User Accounts \(Local Users Only\)" on page 172](#)

### 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 103](#).

After you configure a single proxy for use with all HTTP(s) protocol-based integrations, you can enable that proxy for Rulepack update. For instructions, see ["Configuring Core Settings" on page 82](#).

### 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.

For information about alerts and how to configure Fortify Software Security Center to send alerts as email alert notifications, see ["Enabling and Disabling Receipt of Email Alerts" on page 156](#).

To configure the settings used for sending email alert notifications:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, select **ADMINISTRATION**.
2. In the left panel, select **Configuration**, and then select **Email**.  
The Email page opens.
3. 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 the SMTP password.
Enable SSL/TLS encryption	Select this check box to enable communications security using SSL and TLS protocols.
Trust the certificate provided by the SMTP server	Select this check box to always treat the specified SMTP server certificate as trusted.

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

## 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 panel, 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**
- **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 247](#)

## 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 panel of the ADMINISTRATION view, select **Configuration**, and then select **JMS**.  
The JMS page opens.
3. 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, <code>tcp://123.0.1.2:12345</code> .
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 <code>Fortify.Advisory.EventNotification</code> .

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



## Configuring LDAP Servers

Configure LDAP authentication servers for your Fortify Software Security Center server to use from the **Configuration** section of the ADMINISTRATION view.

**Important!** Before you configure the properties on the LDAP page, you must prepare for LDAP authentication as described in "[LDAP User Authentication](#)" on page 53.

**Note:** 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 one or more LDAP server connections for Fortify Software Security Center:

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

Field	Description
<b>BASIC SERVER PROPERTIES</b>	
Enable this LDAP Integration	Select this check box to make this LDAP server available for Fortify Software Security Center to use.
Server Name  <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> <b>Important!</b> If you configure multiple LDAP servers, you must make sure that you specify a unique server name for each.                     </div>	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 use secured LDAPS, enter the URL in the following format:  ldaps://<hostname>:<port> LDAPS ensures that only encrypted user

Field	Description
<p>Base DN</p> <div data-bbox="302 426 808 737" style="background-color: #f0f0f0; padding: 10px;"> <p><b>Important!</b> If you configure more than one LDAP server for Fortify Software Security Center, then you must set a unique Base DN for each of them.</p> </div>	<p>credentials are transmitted.</p> <p>Type the Base Distinguished Name (DN) for LDAP directory structure searches.</p> <p>For example, the Base DN for <code>companyName.com</code> is <code>dc=companyName,dc=com</code>.</p> <p>All DN values are case-sensitive, must not contain extra spaces, and must exactly match LDAP server entries.</p> <p>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.</p>
<p>Bind User DN</p> <div data-bbox="302 1108 808 1482" style="background-color: #f0f0f0; padding: 10px;"> <p><b>Note:</b> If your LDAP server supports anonymous binding, you are not required to specify values for <b>Bind User DN</b> and <b>Bind User Password</b>. Check with your LDAP administrator to find out whether your LDAP server supports anonymous binding.</p> </div>	<p>Type the full distinguished name (DN) of the account Fortify Software Security Center uses to connect to the authentication server.</p> <p>The general format for an account specifier is as follows:</p> <pre>cn=&lt; accountName &gt;,ou=users,dc=&lt;domainName&gt;,dc=com</pre> <p>where <code>&lt;accountName&gt;</code> represents the minimum privilege, read-only authentication server account you created for exclusive use by Fortify Software Security Center.</p> <div data-bbox="849 1619 1369 1780" style="background-color: #f0f0f0; padding: 10px;"> <p><b>Caution!</b> For security reasons, never use a real user account name in a production environment.</p> </div> <p>If you use Active Directory, specify the</p>

Field	Description
	domain name and username in the following format:  <code>&lt;domain_name&gt;\&lt;username&gt;</code>
Bind User Password  <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note:</b> If your LDAP server supports anonymous binding, you are not required to specify values for <b>Bind User DN</b> and <b>Bind User Password</b>. Check with your LDAP administrator to find out whether your LDAP server supports anonymous binding.</p> </div>	Type the password for the Bind User DN account.
Show Password	Select this check box to show entered passwords.
Relative Search DN's (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 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.  For example: To search within the base DN <code>companyName.com</code> and all entries under that base DN, specify the following to recursively search all entries under that path:  <code>cn=users</code> or

Field	Description
	cn=users,ou=divisionName
Ignore Partial Result Exception	<p>To avoid search failures when search results include more records than the LDAP server can return, leave this check box selected.</p> <p>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.</p>
<p>Because most people use Microsoft Active Directory, the remaining LDAP attributes on the page are configured to work with the default Active Directory configuration. However, if your LDAP server is set up differently, you can change these attribute values.</p>	
<p><b>BASE SCHEMA</b></p>	
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

Field	Description
	value is group.
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 <code>distinguishedName</code> .
<b>USER LOOKUP SCHEMA</b>	
User first name attribute	Type the user object attribute that specifies a user's first name. The default value is <code>givenName</code> .
User lastname attribute	Type the user object attribute that specifies a user's last name. The default value is <code>sn</code> .
Group name attribute	Type the group attribute that specifies the group name. The default value is <code>cn</code> .
User username attribute	Type the user object attribute that specifies a username. The default value is <code>sAMAccountName</code> .
User password attribute	Type the user object attribute that specifies a user's password. The default value is <code>userPassword</code> .
Group member attribute	Type the group attribute that defines the members of the group. The default value is <code>member</code> .
User email attribute	Type the user object attribute that specifies a user's email address. The default value is <code>mail</code> .
UsermemberOf attribute	Type the name of an LDAP attribute that includes the LDAP group names for LDAP

Field	Description
	users.
<b>USER PHOTO</b>	
User photo enabled	Select this check box to enable the retrieval of user photos from the LDAP server.
User thumbnail photo attribute	ThumbnailPhoto attribute for Active Directory.
User thumbnail mime default attribute	Thumbnail mime default attribute
<b>ADVANCED INTEGRATION PROPERTIES</b>	
<p>Cache LDAP User Data</p> <p><b>Note:</b> Fortify recommends that you leave LDAP user caching enabled. Changes to user information made directly in the LDAP server may not be reflected in Fortify Software Security Center for up to an hour. However, a slow connection between Fortify Software Security Center and the LDAP server or a large LDAP directory with slow searches could degrade Fortify Software Security Center performance. User data are seldom changed directly in the LDAP server.</p>	<p>Select this check box to enable LDAP user data caching in Fortify Software Security Center.</p> <p>You can refresh the LDAP cache manually from the ADMINISTRATION view in Fortify Software Security Center. For instructions, see <a href="#">"Refreshing LDAP Entities Manually" on page 102.</a></p>
Cache: Max threads per cache	<p>Type the maximum number of threads dedicated for each update process (user action). Each time a user clicks <b>Update</b>, a new update process starts.</p> <p>The default value is 4.</p>
Cache: Max object lifetime (ms, "-1" to turn off)	If you want objects in the cache refreshed more frequently than the default refresh time (typically 1 hour), type the maximum

Field	Description
	amount of time (in milliseconds) that an object can be in the cache before it is refreshed with new information from the LDAP server.  The default value is -1.
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. The default value is 12.
Enable paging in LDAP search queries	Select this check box to enable paging in LDAP search queries.  <div style="background-color: #f0f0f0; padding: 5px;"> <b>Note:</b> Not all LDAP servers support paging. Check to make sure that your LDAP server supports this feature.                     </div>
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 <b>Enable paging in LDAP search queries</b> 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	If you have only one LDAP server, Fortify recommends that you select <b>ignore</b> so that LDAP works faster. If you have a multi-domain LDAP configuration and you use LDAP referrals, select <b>follow</b> . The default value is <b>ignore</b> .  <div style="background-color: #f0f0f0; padding: 5px;"> <b>Note:</b> If referrals are not used on your LDAP server, see "<a href="#">About the LDAP Server Referrals Feature</a>" on page 55."                     </div>

Field	Description
LDAP Authenticator type	<p>From this list, select one of the following LDAP authentication types to use:</p> <ul style="list-style-type: none"> <li>• <b>BIND_AUTHENTICATOR</b>— Authentication directly to the LDAP server ("bind" authentication).</li> <li>• <b>PASSWORD_COMPARISON_AUTHENTICATOR</b>— The password the user supplies is compared to the one stored in the repository.</li> </ul> <p>For more information about LDAP authentication types, see <a href="http://docs.spring.io/spring-security/site/docs/3.1.x/reference/ldap.html">http://docs.spring.io/spring-security/site/docs/3.1.x/reference/ldap.html</a>.</p>
LDAP Password Encoder type	<p>Select a value from this list only if the LDAP authentication method is password comparison.</p> <p>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 <b>MD4_PASSWORD_ENCODER</b>, password comparisons will fail.</p>
<p>Enable Nested LDAP Groups</p> <div data-bbox="302 1472 808 1829" style="background-color: #f0f0f0; padding: 10px;"> <p><b>Note:</b> 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</p> </div>	<p>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).</p>



Field	Description
not plan to use nested groups.	
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.
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	Specify the base security identifier (SID) of LDAP directory objects.
Object SID (objectSid) attribute	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.
SSL Trust Check	
Hostname Validation	

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.

### See Also

["Importing an LDAP Server Configuration" below](#)

["LDAP User Authentication" on page 53](#)

["Registering LDAP Entities" on page 173](#)

["About Managing LDAP User Roles" on page 128](#)

["Editing an LDAP Server Configuration" below](#)

["Deleting an LDAP Server Configuration" on page 102](#)

### Editing an LDAP Server Configuration

To edit an LDAP server connection:

1. On the Fortify header, click **ADMINISTRATION**.
2. In the left panel, 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 89](#).
6. To check the validity of the configuration, click **VALIDATE CONNECTION**.
7. To save the configuration after successful validation, click **SAVE**.

### See Also

["LDAP User Authentication" on page 53](#)

["Registering LDAP Entities" on page 173](#)

["About Managing LDAP User Roles" on page 128](#)

### 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 panel, select **Configuration**, and then scroll down and select **LDAP Servers**.
3. On the LDAP Servers header, click **IMPORT**.

The IMPORT LEGACY LDAP CONFIGURATION dialog box opens.

4. 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 in ["Configure the attributes described in the table in step 4 in "Configuring LDAP Servers" on page 89."](#) below.

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 89](#).
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

["LDAP User Authentication" on page 53](#)

["Registering LDAP Entities" on page 173](#)

["About Managing LDAP User Roles" on page 128](#)

#### 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 panel, click **Users**, and then select **LDAP**.
3. On the **LDAP** toolbar, click **+ADD**.

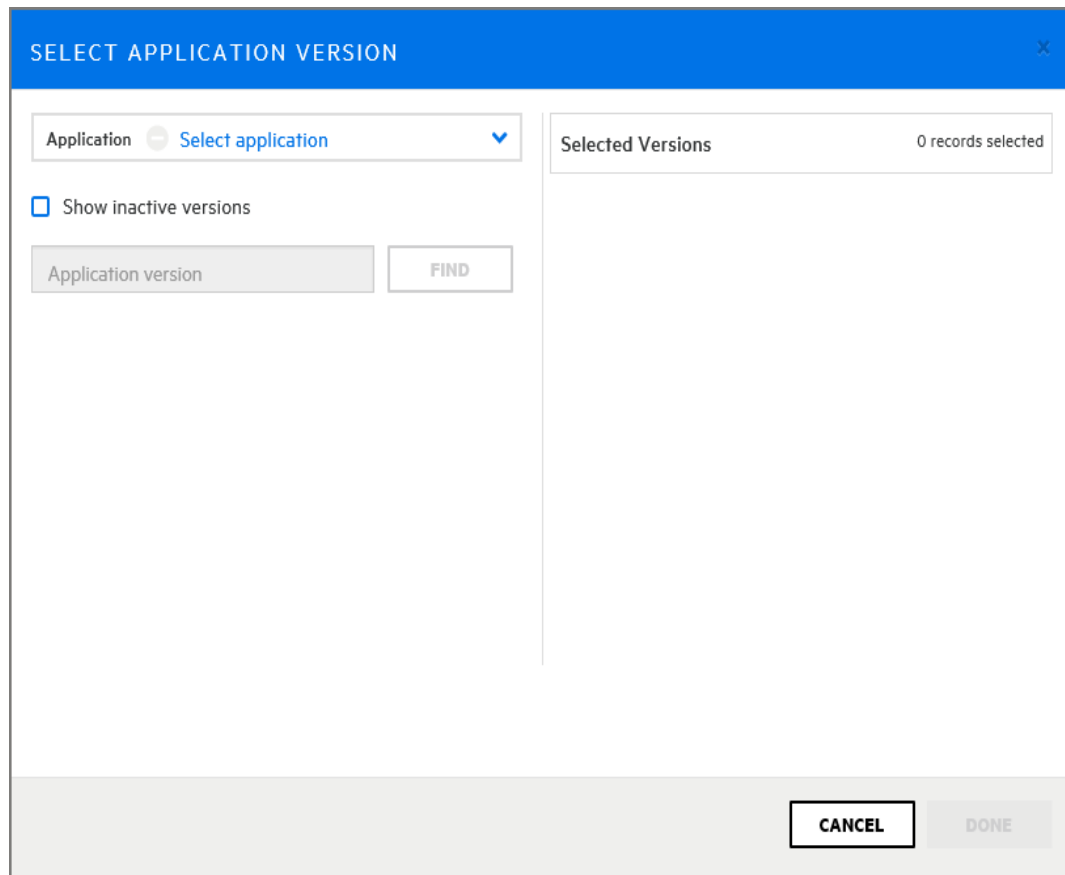
The **ADD NEW LDAP ENTITY** window opens.

4. 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**.



The screenshot shows a dialog box titled "SELECT APPLICATION VERSION". At the top left, there is a dropdown menu labeled "Application" with the text "Select application" and a blue arrow. To the right of this is a "Selected Versions" section with the text "0 records selected". Below the dropdown is a checkbox labeled "Show inactive versions". At the bottom left, there is a text input field for "Application version" and a "FIND" button. At the bottom right, there are "CANCEL" and "DONE" buttons.

The **SELECT APPLICATION VERSION** dialog box opens.

- b. From the **Application** list, select the name of an application that you want the LDAP entry 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.

9. To initiate the LDAP refresh process manually so that your changes are evident sooner than

they would be otherwise:

- a. On the LDAP page, select the check box for the LDAP entity you want to refresh.
- b. On the LDAP toolbar, click **REFRESH**.

For information about how to configure LDAP servers, see ["Configuring LDAP Servers" on page 89](#).

#### **See Also**

["LDAP User Authentication" on page 53](#)

["About Managing LDAP User Roles" on page 128](#)

#### **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 panel, select **Users**, and then select **LDAP**.
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 89](#).

#### **See Also**

["LDAP User Authentication" on page 53](#)

["Registering LDAP Entities" on page 173](#)

["About Managing LDAP User Roles" on page 128](#)

#### **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 panel, 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 upper 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 53](#)

["Registering LDAP Entities" on page 173](#)

["About Managing LDAP User Roles" on page 128](#)

## 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 74](#)), the Rulepack update URL (["Configuring Core Settings" on page 82](#)), and bug tracker plugins (["Assigning a Bug Tracking System to an Application Version" on page 200](#)).

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 panel, 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.
<b>HTTP proxy</b>	
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	If HTTP authentication is required, type a password.

Setting	Description
password	
<b>HTTPS proxy</b>	
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.
HTTSP 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 74](#)
- ["Configuring Core Settings" on page 82](#)
- ["Assigning a Bug Tracking System to an Application Version" on page 200](#)

**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 panel, select **Configuration**, and then select **Scheduler**.  
 The **Scheduler** page opens.
3. Configure the settings as described in the following table.



Field	Description
Number of days after which executed jobs will be removed	The number of days after which finished jobs are removed from Fortify Software Security Center. The default value is 2 (days).
Job execution strategy	Select the job execution strategy to use. Options are as follows: <ul style="list-style-type: none"> <li>• <b>Conservative:</b> Enables highly concurrent FPR processing. With this option, the job scheduler can run FPR processing on all workers available to the scheduler and up to two report jobs at a time. Low concurrency jobs such as artifact and application version deletion are executed in sequence.</li> <li>• <b>Aggressive:</b> 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.</li> <li>• <b>Exclusive jobs:</b> Enables jobs to run in sequence, one at a time.</li> </ul> The default value is Conservative. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <b>Note:</b> Two worker threads are dedicated to exporting to comma-separated values (CSV) jobs for both conservative and aggressive strategies. (See <a href="#">"Exporting Data to Comma-Separated Values Files" on page 160.</a>)                     </div>
<b>Token management</b>	
Warn days before expiry	Number of days before token expiration that users are notified of the upcoming expiration. Valid values range from 3 to 30 days, inclusive. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <b>Note:</b> The start of the day is 12 AM in the Fortify Software Security Center server locale.                     </div>
<b>Snapshot refresh</b> - Use the fields in this section to schedule the snapshot job.	
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 <b>SUN, WED, FRI</b> or <b>1, 4, 6</b> .

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

Field	Description
	<p>To enter consecutive days, separate the entries with a dash. For example, type <b>MON-FRI</b> to run the scheduler on week days only.</p> <p>Type <b>*</b> if the scheduler is to run every day.</p> <p>The default value is <b>*</b>.</p>
Hours	<p>Type the hour, using 24-hour time notation, at which the recurring index maintenance job is to start running. For example, type <b>1</b> to start the job at 1 A.M.</p> <p>Type <b>*</b> if the scheduler is to run every hour.</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> The values you enter in the <b>Days of Week</b>, <b>Hours</b>, and <b>Minutes</b> fields are concatenated to create the CRON expression used by the scheduler.</p> </div> <p>The default value is 0 (midnight).</p>
Minutes	<p>Type the minute at which the recurring index maintenance job is to start running. For example, type <b>24</b> to start the job at 24 minutes past the hour that you entered in the <b>Hours</b> box.</p> <p>The default value is 0 (indicating the job starts running in the first minute).</p>
<b>Events maintenance</b>	
Days to preserve	<p>Type the number of days after which Micro Focus removes past events. To specify no event removal, type <b>0</b> (zero).</p> <p>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.</p>
<b>Data export maintenance</b>	
Days to preserve	<p>Type the number of days after which Fortify Software Security Center removes exported data.</p>

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

**See Also**

["Canceling Scheduled Jobs" on the next page](#)

### 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 panel 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

["Configuring Job Scheduler Settings" on page 104](#)

["Canceling Scheduled Jobs" below](#)

### 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 panel 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 104](#)

**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 panel, select **Configuration**, and then select **Security**.  
The Security page opens.
3. Configure the settings as described in the following table.

Field	Description
Content-Security-Policy	<p>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.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• To restrict access to only the base URL configured using the <code>host.url</code> property (set using the Fortify Software Security Center configuration wizard), select <b>Strict</b>.</li> <li>• To enable a less restrictive policy than strict CSP, select <b>Relaxed</b>. This is the default setting. It allows access to the Fortify Software Security Center domain from any <code>host:port</code>.</li> <li>• To disable the Content-Security-Policy header, select <b>Disabled</b>. Although Fortify recommends that you <i>not</i> disable the Content-Security-Policy header, this option is</li> </ul>

Field	Description
	available if CSP causes unexpected problems.
Set value for Strict-Transport-Security header	<p>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.</p> <p><b>Important!</b> 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 (<a href="https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet">https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet</a>).</p> <p>The Strict-Transport-Security header is sent only through a secure channel determined by Tomcat Server.</p>
Set value for Public-Key-Pins header	<p>Type the value for the Public-Key-Pins header. This decreases the risk of man-in-the-middle (MitM) attacks.</p> <p><b>Important!</b> 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 (<a href="https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet">https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet</a>).</p> <p>The Public-Key-Pins header is sent only through a secure channel determined by Tomcat Server.</p>

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
Central Authorization Server (CAS)	<a href="#">"Configuring Fortify Software Security Center to Work with a Central Authorization Server" on the next page</a>
SPNEGO-based Kerberos	<a href="#">"Setting up Kerberos Authentication with Fortify Software</a>

SSO Solution	Instructions
	<a href="#">"Security Center" on page 112</a>
SAML 2.0-compliant single sign-on	<a href="#">"Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single Sign-On Solutions" on page 113</a>
HTTP headers	<a href="#">"Configuring Fortify Software Security Center to Work with Single Sign-On and Single Logout Solutions that use HTTP Headers" on page 116</a>
X.509 certification	<a href="#">"Configuring Fortify Software Security Center to use X.509 Certification-based SSO" on page 117</a>

**Notes:**

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.

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 or information about how to enable debug logging for SSO, see information about Fortify Audit Workbench support for SSO, see the *Micro Focus Fortify Audit Workbench User Guide*.

For information about how to enable debug logging for SSO, see ["Enabling Debug Logging for Single Sign-On Authentication" on page 117](#).

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

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 panel of the ADMINISTRATION view, select **Configuration**, and then select **SSO**. The SINGLE SIGN ON page opens to the **CAS SSO** tab.
3. Configure the settings described in the following table.

Field	Description
Enable Central Authentication Server integration	Select this check box to enable integration with CAS.
Fortify Software Security Center Location	Type the Fortify Software Security Center server URL.  The default is

Field	Description
	http://localhost:8180/ssc.
Central Authentication Server URL	Type the URL for the CAS server. The default is http://localhost:8080/cas.

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

### Setting up Kerberos Authentication with Fortify Software Security Center

To set up Kerberos authentication with Fortify Software Security Center:

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 SSKerberos
```

2. Create a keytab file.

**Example:**

```
ktpass -out c:\SSCSERVER.keytab -princ HTTP/  
SSCServer.mydomain.lan@mydomain -mapUser mydomain\SSKerberos -  
mapOp set -pType KRB5_NT_PRINCIPAL /crypto all /kvno0 -pass  
3o(t&gSp&3hZ4#t9
```

3. Log in to Fortify Software Security Center as an administrator, and then, on the Fortify header, select **ADMINISTRATION**.
4. In the left panel of the ADMINISTRATION view, select **Configuration**, and then select **SSO**. The SSO page opens.
5. Click the **SPNEGO/KERBEROS SSO** tab.
6. Select the **Enable SPNEGO/Kerberos integration** check box.
7. In the **Service principal name** box, type the service principal name (SPN) of Fortify Software Security Center in the Kerberos realm.
8. In the **Keytab location** box, type the location of the keytab file (created in step 2), which contains Fortify Software Security Center principal keys.  
Make sure that you use the correct resource prefix. Example: file:///.
9. (Optional) In the **Krb5.conf location** box, type the Krb5.conf file location.  
This sets the java.security.krb5.conf property.
10. To enable debug mode, select the **Enable debug mode** check box.
11. Click **SAVE**.



12. Check to make sure that the **User username attribute** setting for your LDAP server is correct. (See ["Configuring LDAP Servers" on page 89.](#))
13. Restart the server.
14. Verify that the LDAP user names resolve correctly. Format the LDAP user name values as follows:

```
username@domain
```

15. 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 Internet Explorer and 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.

#### See Also

["Configuring Fortify Software Security Center to Work with Single Sign-On" on page 110](#)

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

**Note:** SAML single logout is not implemented in Fortify Software Security Center.

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 53.](#))
2. If your IdP runs with SSL (https), configure Fortify Software Security Center to run with SSL. Otherwise, protocol switching during authenticating against IdP could interfere with authentication.
3. Get SAML metadata from the IdP server and store it on the Fortify Software Security Center file system.
4. Open the metadata file and make a note of the entityID for your IdP EntityDescriptor (<EntityDescriptor entityID="THE\_VALUE\_YOU\_ARE\_LOOKING\_FOR">).
5. Log in to Fortify Software Security Center and, on the Fortify header, select **ADMINISTRATION**.
6. In the left panel of the ADMINISTRATION view, select **Configuration**, and then select **SSO**. The SSO page opens.

7. Click the **SAML SSO** tab.
8. Provide the information described in the following table.

Field	Description
Enable SAML 2.0 integration	Select this check box to enable the remaining configuration fields on the page.
IdP metadata location	Location of your identity provider metadata (the metadata obtained in step 3):  file:///location/of/idp-metadata.xml  <b>Note:</b> 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 <i>not</i> support getting metadata over http proxy.
Default IdP	entityID of your IdP EntityDescriptor (from IdP metadata)
SP entity ID	Service provider entity ID  You can specify the Fortify Software Security Center URL or a Uniform Resource Name (URN) such as urn:ssc:saml.
SP alias	Fortify Software Security Center alias  To simplify things, you can use the URN (urn:ssc:saml).
Keystore location	Location of your Java keystore for encrypting and signing SAML assertions
Keystore password	Java keystore file password
Signing & encryption key	Signing/encryption key
Signing & encryption key password	Signing/encryption key password
SAML name identifier	Username attribute (any string assertion attribute)

9. Click **SAVE**.
10. 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 Fortify Software Security Center SAML metadata.

**Note:** For Fortify Software Security Center 17.10 and earlier versions, you can find the

`host.url` property in `<WAR>/WEB-INF/config/ssc.properties` or use the configuration wizard to set up the URL.

11. Restart Fortify Software Security Center.
12. Generate the Fortify Software Security Center (SP) metadata at `<hostname>:<port>/<context>/saml/metadata`.
13. Open the metadata generated in previous step and verify that the values for the following are the same as the values you specified in the **SAML SSO** tab:
  - The entity ID value matches the one you specified in the **"SP entity ID" on the previous page** box.
  - The SP alias in the metadata is the one you specified in the **"SP alias" on the previous page** box.
  - The location URLs in `<AssertionConsumerService>` bindings are accessible from the IdP server.
14. Upload the Fortify Software Security Center metadata to the IDP server.
15. 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.

#### Troubleshooting

**Issue:** "I'm accessing the `<hostname>:<port>/<app-context>/login.jsp` page and I'm not redirected to IdP."

- The login page is excluded from SSO so that a local administrator can access the application if SSO is incorrectly configured.

**Issue:** "I'm authenticated with IdP, but Fortify Software Security Center doesn't authorize me."

- 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.
  - The user lookup strategy is correctly configured (see ["Configuring Core Settings" on page 82](#)).

**Issue:** "I would like to set the IdP metadata location as HTTP URL to IDP instead of referencing the IdP metadata locally."

- The configuration accepts also HTTP location but the IDP cannot be behind proxy.
- If 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 panel, select **Configuration**, and then select **SSO**.  
 The SSO page opens.
3. Select the **HTTP SSO** tab.
4. Configure the settings described in the following table.

Field	Description
Enable HTTP SSO integration	Select this check box to enable the remaining fields.
HTTP header for username	Type the HTTP header to use for SSO logons. The default value is <i>username</i> .
IdP login page	Type the URL for the identity provider login page.
<b>SSO Logout</b>	
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.
<b>SSO Logout Response Directive</b>	
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. See "[LDAP User Authentication](#)" on page 53.
7. Restart the server.

**See Also**

["Configuring Fortify Software Security Center to Work with Single Sign-On" on page 110](#)

**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. Log in to Fortify Software Security Center as an administrator, and then click the **ADMINISTRATION** tab.
2. In the left panel of the ADMINISTRATION view, select **Configuration**, and then click **SSO**. The SSO page opens.
3. Click the **X.509 SSO** tab.
4. Select the **Enable X.509 integration** check box.
5. In the **X.509 certificate username pattern** box, type a regular expression for Fortify Software Security Center to use to retrieve user names from the X.509 certificate.

**Note:** To match the CN attribute of the certificate's subject, you can specify `CN=(.*?)`.

6. Click **SAVE**.
7. To implement the configuration, restart the Fortify Software Security Center server.

**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>/ssc/WEB-INF/classes` directory, and then open the `log4j2.xml` file in an editing application.
2. Add the following logger definition to the `log4j2.xml` file:

```
<Logger name="com.fortify.manager.web.security.sso.SsoFilter"
level="debug"/>
```

**See Also**

["Configuring Fortify Software Security Center to Work with Single Sign-On" on page 110](#)

**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 310](#).

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 panel, select **Configuration**, and then select **Web Services**.  
The WEB SERVICE ATTRIBUTES page opens.
3. 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>/ssc/conf`, and then open the `log4j2.xml` file in a text editor.
2. In the `<Loggers>` section, change the root level setting to one of the following:
  - `<Root level="warn">`
  - `<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."

## Chapter 8: 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 selected Fortify Software Security Center data displayed on the Issue Stats and AUDIT pages 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 panel of the ADMINISTRATION view, select **Configuration**, and then select **Core**. The **Core** page opens.
3. Scroll to the bottom of the page, and then clear the **Enable export to CSV** check box.
4. Click **SAVE**.

#### See Also

["Configuring Core Settings" on page 82](#)

### 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
- JIRA
- ALM
- TFS/VSTS

**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 320](#).

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 196](#).

## Managing Bug Tracker Plugins

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

### 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 panel of the ADMINISTRATION view, select **Plugins**, and then select **Bug Tracking**.  
The Bug Tracking page opens.
3. On the page header, click **NEW**.  
Fortify Software Security Center displays the Upload Plugin Warning.
4. Read the warning and, if you accept the potential risk involved in uploading the plugin, click **OK**.  
The Upload Plugin Bundle dialog box opens.
5. Click **BROWSE**, and then locate and select the JAR file for your plugin.
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**.

### 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 panel of the ADMINISTRATION view, select **Plugins**, and then select **Bug Tracking**.  
The Bug Tracking page opens.
3. 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 119](#)

["Authoring Bug Tracker Plugins" on page 320](#)

["Adding and Managing Parser Plugins" on page 123](#)

## 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 320](#) or contact Fortify Support (<https://support.fortify.com>).

## 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.

## Configuring an Eclipse Plugin Update Site

You can use Fortify Software Security Center to host an Eclipse update site. This enables you to distribute the Fortify Plugin for Eclipse from a central location, eliminating the need for each individual developer to install plugins locally.

To configure an Eclipse update site:

1. Navigate to `<ssc_install_dir>/WEB-INF/internal`, and then open the `securityContext.xml` file in a text editor.

**Note:** `<ssc_install_dir>` is the directory in which Fortify Software Security Center is deployed.

2. Locate the following line of text:

```
<!--<security:intercept-url pattern="/update-site/**" access="PERM_
ANONYMOUS"/>-->
```

3. Remove the comment tags from the line of text so that it looks like the following:

```
<security:intercept-url pattern="/update-site/**" access="PERM_
ANONYMOUS"/>
```

4. Save the `securityContext.xml` file.
5. Enable the mapping for the Eclipse Update site.
6. Run the `Fortify_SCA_and_Apps` installer.
7. Copy the contents of `<sca_install_dir>/plugins/eclipse` (this consists of a `site.xml` file and jar files in the features and plugins directories) to the `update-site` directory on your web server. `<sca_install_dir>` is the location in which the Static Code Analyzer and Applications installer installed the files.

Your developers can now point to the URL from their Eclipse IDE. For complete client-side installation details, see the *Micro Focus Fortify Plugins for Eclipse Installation and Usage Guide*.

## 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 panel, select **Plugins**, and then select **Parsers**.  
The Parsers page opens.
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**.  
The Upload Plugin Bundle dialog box opens.
5. 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 120](#)

## 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:

<a href="#">Administrator Accounts</a> .....	124
<a href="#">Fortify Software Security Center User Accounts</a> .....	124
<a href="#">About Creating User Accounts</a> .....	125
<a href="#">Preventing Destructive Library and Template Uploads to Fortify Software Security Center</a> ....	126
<a href="#">Viewing Permission Information for Fortify Software Security Center Roles</a> .....	126

### 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 126](#)

### 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 151](#).

### Related Topics

["About Creating User Accounts" below](#)

["Unlocking User Accounts \(Local Users Only\)" on page 172](#)

## About Creating User Accounts

The Fortify Software Security Center Users module provides the tools you use to edit, delete, or suspend 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 168](#).

For information about how to configure Fortify Software Security Center user account timeout and lockout settings, see ["Configuring Core Settings" on page 82](#). For more information about user account privileges, see ["Fortify Software Security Center User Account Management" on page 165](#).

### See Also

["Viewing Permission Information for Fortify Software Security Center Roles" below](#)

["Unlocking User Accounts \(Local Users Only\)" on page 172](#)

## 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 commands 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 panel, 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.

Developer      Users of the Developer role can upload analysis results and view and audit issues for application versions that the user has access to.

**Name**  
Developer

**Description**  
Users of the Developer role can upload analysis results and view and audit issues for application versions that the user has access to.

**Type**  
System defined

Universal access

Fortify strongly recommends that you select universal access only for administrator-level users.

**Permissions**

Name	Description
Approve Analysis Results Upload	User can approve uploaded analysis results to application versions to which the user has access. This permission requires the View Application Versions permission.
Comment on Issues	User can comment on issues for application versions to which the user has access. This permission requires the View Application Versions permission.
Comment on SSA Governance Progress	User can comment on the process template, requirements, activities, and tasks for application versions to which the user has access. This permission requires the View Application Versions permission.
Delete Generated Reports	User can delete generated reports. Reports that expose application version/runtime application data will be restricted to the application versions/runtime applications to which the user has access.

For more information about user accounts, see ["Managing User Accounts" on page 165](#).

### Related Topics

["Pre-configured Roles" on page 165](#)

["About Creating User Accounts" on page 125](#)

["Unlocking User Accounts \(Local Users Only\)" on page 172](#)

## Unlocking User Accounts (Local Users Only)

After a local user tries unsuccessfully to log in to Fortify Software Security Center more than three times in a row, Fortify Software Security Center prevents the user from attempting more logons. 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.

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 panel of the ADMINISTRATION view, select **Users**, and then click **Local**.
3. Bring up the locked user account, expand the row to view account details, and then click **EDIT**.

At the bottom left, the message **User has reached the maximum login attempts** is displayed.

4. To the right of the message, click **Unlock user**.

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 168](#)

["Editing Local User Accounts" on page 170](#)

## About Managing LDAP User Roles

A relative distinguished name (RDN) further qualifies a base DN. For example, if the base distinguished name (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," you, as an administrator, must check to make sure that the user has been added to the correct LDAP group.



To make sure that the user has been added to the correct group in LDAP:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left panel in the ADMINISTRATION view, select **Users**, and then select **LDAP**.
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:** Refreshing the data blocks your access to Fortify Software Security Center. 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.

## 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 panel, under **Templates**, click **Attributes**.  
The Attributes page lists the attributes on the right.
4. Click **NEW**.  
The CREATE NEW ATTRIBUTE dialog box opens.

5. Provide the information described in the following table.

Field	Description
Name	Type a descriptive name for the attribute.
Description	Type a brief description. The description is displayed under the attribute field in the Create New Application 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 wizard.
Category	Select an attribute type. Depending on the category you select, the attribute is displayed on the <b>Business Attributes</b> step, the <b>Technical Attributes</b> step, or the <b>Organization Attributes</b> step of the CREATE NEW APPLICATION wizard.  <b>Note:</b> If your Fortify Software Security Center instance is integrated with Fortify WebInspect, the list also includes the <b>Dynamic Scan Request</b> category.
Scope	Select the value that indicates whether the attribute applies only to

Field	Description
	application versions, runtime applications, or to both.
Type	<p>Select one of the following control types:</p> <ul style="list-style-type: none"> <li>• To create a check box for the attribute, select <b>Boolean</b>.</li> <li>• To create a calendar selection control for the attribute, select <b>Date</b>.</li> </ul> <p><b>Note:</b> This type is not available for a Dynamic Scan Request attribute.</p> <ul style="list-style-type: none"> <li>• To create a list from which a user can select only a single value for the attribute, select <b>List of Values - Single Selection</b>.</li> </ul> <p><b>Note:</b> If you create a single-select type attribute, users can select it from the <b>Group by</b> and <b>Aggregate by</b> lists on the Dashboard to customize the data they view.</p> <ul style="list-style-type: none"> <li>• To create a list from which a user can select multiple values for the attribute, select <b>List of Values - Multiple Selection</b>.</li> <li>• To create a field that accepts an integer value, select <b>Integer</b>.</li> <li>• To create a text field into which a user can type a single line of text, select <b>Text - Single Line</b>.</li> <li>• To create a text field into which a user can type multiple lines of text, select <b>Text - Multiple Lines</b>.</li> </ul> <p><b>Note:</b> If you select one of the <b>List of Values</b> types, additional fields are displayed in which you add the values and their descriptions, and specify whether or not they are hidden.</p>

6. Click **SAVE**.

The new attribute is available the next time a user uses the CREATE NEW APPLICATION wizard.

For instructions on how to specify custom attributes in existing application versions, see ["Specifying New Custom Attributes in Existing Application Versions" on page 185](#).

**See Also**

["Application Version Attributes" on page 181](#)

## 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 60.](#))

**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 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 60](#) or ["Configuring Fortify Software Security Center After an Upgrade" on page 142.](#))

### 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" above](#)

["Troubleshooting Search Index Issues" on the next page](#)

## 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 104](#).

## Placing Fortify Software Security Center in Maintenance Mode

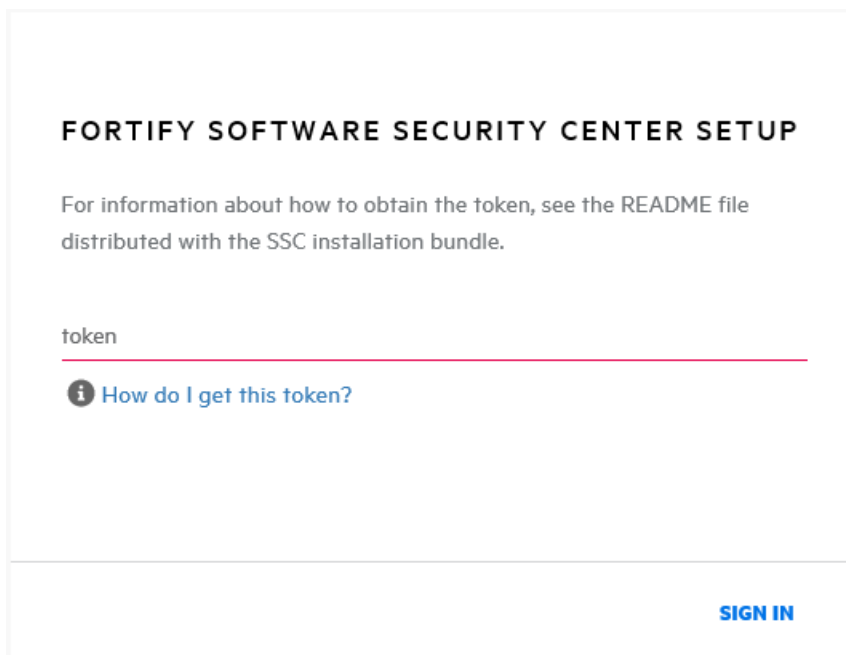
If, at any time, you need to change any server configuration settings, you can place Fortify Software Security Center in maintenance mode, and then make the necessary changes.

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 panel, select **Configuration**, and then select **Maintenance Mode**.  
The Maintenance Mode page opens.
3. 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 opens and displays all of the current configuration settings. For information about server configuration, see "[Configuring Fortify Software Security Center for the First Time](#)" on page 60.

## 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 information on how to manage Rulepacks, see:

- "[Updating Rulepacks from the Micro Focus Fortify Update Server](#)" on the next page
- "[Seeding the Database with Report Seed Bundles Delivered with Quarterly Security Content Releases](#)" on page 147
- "[Exporting Rulepacks](#)" on page 136
- "[Importing Security Content](#)" on page 136
- "[Deleting Rulepacks](#)" on page 136

- External metadata provides mappings from the Fortify vulnerability categories to alternative categories (such as CWE, OWASP Top 10, and PCI DSS).

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 147](#).) 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 *Micro Focus 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 137](#)
- ["Creating a New Mapping" on page 138](#)

**Note:** Fortify recommends that you periodically update your security content.

## Updating Rulepacks from the Micro Focus Fortify Update Server

If you want to make sure that you have the latest Rulepack, you can import the Rulepack 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 103](#).

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 panel of the ADMINISTRATION view, under **Metrics & Tracking**, select **Rulepacks**.
3. On the Rulepacks page, click **UPDATE FROM SERVER**.

Fortify Software Security Center displays a message as it checks for new Rulepacks.

### See Also

["Deleting Rulepacks" 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 panel, 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**.

## 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 panel, 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.

## Deleting Rulepacks

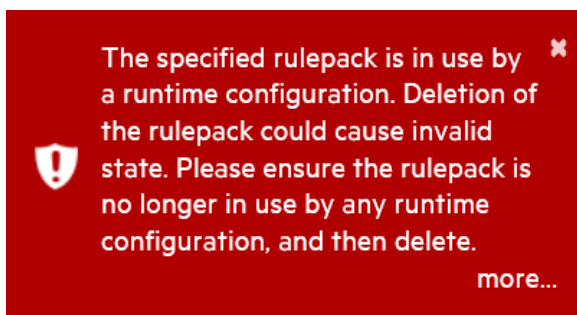
You can remove old Rulepacks from Fortify Software Security Center.

**Note:** You cannot delete Rulepacks that are in use.



### 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 panel, 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 Rulepacks.
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 the previous page](#)

["Importing Security Content" on the previous page](#)

["Updating Rulepacks from the Micro Focus Fortify Update Server" on page 135](#)

## Extending a Current Mapping

You can extend the mappings that Fortify Software Security Center delivers with the external metadata. 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 136](#).

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

["About Fortify Software Security Content" on page 134](#)

["Creating a New Mapping" below](#)

## 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 136](#).

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

["About Fortify Software Security Content" on page 134](#)

["Extending a Current Mapping" on page 137](#)

# Chapter 9: 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 two versions installed. For example, to upgrade to version 18.20, you must have either version 17.20 or 18.10 installed. If an earlier version is installed, you must upgrade to version 17.20 or 18.10 before you can upgrade to version 18.20.

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 CloudScan-related functionality in Fortify Software Security Center 16.10 and later versions requires updated CloudScan Controller and sensors. If you do not need sensor metrics, you can use existing sensors. You can use existing CloudScan clients without limiting functionality.

You must upgrade the CloudScan Controller before you upgrade the CloudScan sensors and clients, *and* before you upgrade the Fortify Software Security Center server. For information about how to upgrade CloudScan Components, see the *Micro Focus Fortify CloudScan Installation, Configuration, and Usage Guide*.

**Note:** If you plan to view Fortify WebInspect scan results in 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.

## 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.  <b>Important!</b> If the JDBC drivers exist in <tomcat>/webapps/<app>/lib, copy them to <tomcat_server>/lib before you delete the SSC folder.
3	Delete the <b>plugin framework</b> folder from your

Task	Description
	<code>c:\users\<username>\.fortify\plugin-framework</username></code> or <code>&lt;fortify.home&gt;/plugin-framework</code> folder.
4	Copy the new WAR file to the <code>&lt;tomcat&gt;/webapps</code> directory.
5	Start Tomcat Server.
6	Open a browser and enter your Fortify Software Security Center URL to start Fortify in initialization mode. (See <a href="#">"Configuring Fortify Software Security Center After an Upgrade" on the next page.</a> )  If you are migrating a version 17.20 or later instance, use the Setup wizard to verify the configuration settings.
7	Use the Setup wizard to generate the migration SQL script. (See <a href="#">"Configuring Fortify Software Security Center After an Upgrade" on the next page.</a> )
8	Run the migration script on your database. (See <a href="#">"Preparing to Run the Database Upgrade Script" on the next page.</a> )
9	Use the Setup wizard to reseed the database.
10	Restart Tomcat Server.
11	Bug tracker plugins are no longer part of the <code>ssc.war</code> file. After you upgrade and start Fortify Software Security Center, be sure to disable and remove old bug tracker plugins in, and then install new plugins from the current distribution file. For more information, see <a href="#">"About Bug Tracker Integration" on page 119.</a>

## 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.

**Note:** Fortify recommends that you delete the plugin framework folder from your `c:\users\\.fortify\plugin-framework` folder or `<fortify.home>/plugin-framework` folder before you upgrade.

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 48.

## 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 46.

## 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. (See ["Deploying Fortify Software Security Center in Tomcat Server"](#) on page 56.)

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 66.

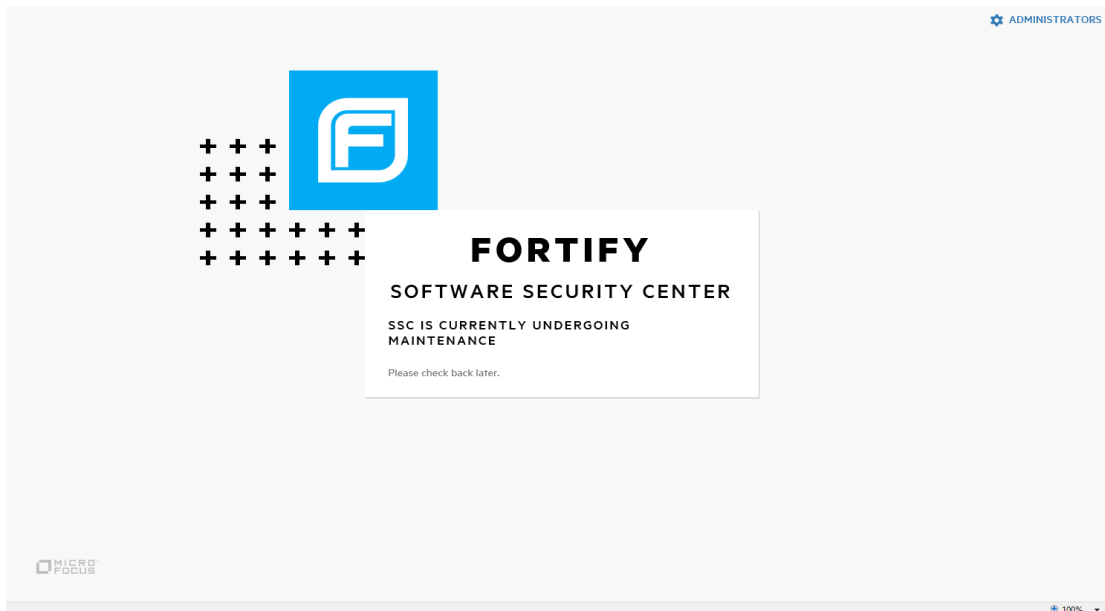
## Configuring Fortify Software Security Center After an Upgrade

After you upgrade Fortify Software Security Center and go to your Fortify Software Security Center URL in a browser window, the Setup wizard opens.

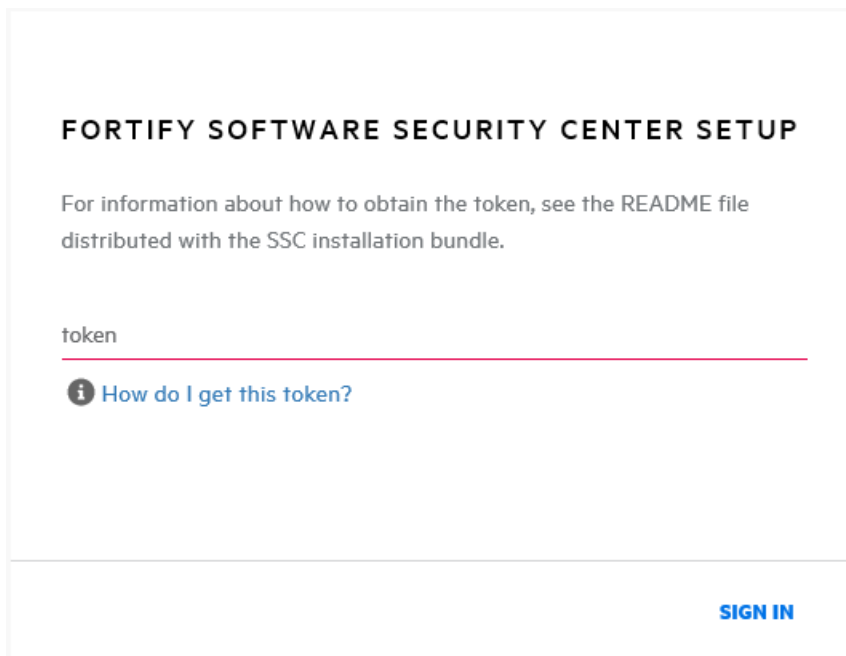
**Note:** The Setup wizard is available to administrators only, and only after first deployment of Fortify Software Security Center, after an upgrade, or after the server is placed in maintenance mode (see ["Placing Fortify Software Security Center in Maintenance Mode"](#) on

page 133).

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.**

The Fortify Software Security Center Setup wizard opens.

6. If you need to change any of the configuration settings on the **CONFIGURATION** or **CORE SETTINGS** steps, you can do so using the instructions provided in ["Configuring Fortify Software Security Center for the First Time" on page 60](#).
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 46](#).
  - 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.
  - e. To test the connection to your database, click **TEST CONNECTION**.
  - f. After the Setup wizard indicates that the connection was successful, in the right panel, 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 the Schema" on page 51](#).)
9. After you run the `ssc-migration.sql` script, click **NEXT**.
10. On the **DATABASE SEEDING** step, do the following:
  - a. In the left panel, 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.

**Note:** Depending on the size of the source database, data migration may take several hours to complete.

**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 133](#).

**See Also**

["Configuring Fortify Software Security Center for the First Time" on page 60](#)



## 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 associated 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 Suite Upgrades from Audit Workbench" below](#)

### Enabling Fortify Static Code Analyzer Suite Upgrades from Audit Workbench

To make new Fortify Static Code Analyzer installers available to Audit Workbench users for upgrades:

1. On the 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. Navigate to the `<ssc_install_dir>/update-site/installers` directory.
5. Open and read the `readme.txt` file.
6. In the `readme.txt` file, copy the sample `update.xml` file content (between and including the `<installerInformation>` and `</installerInformation>` tags).
7. Create a new text file and paste the copied text into it.
8. Update the version information for the installers to reflect your installation. For example:

```
<filename>Fortify_SCA_and_Apps_<version>_windows_x64.exe</filename>
```

9. Under the `<downloadLocationList>` tag, update the URL information to reflect your Software Security Center installation. For example:

```
<url>http://localhost:8080/ssc/update-site/installers/</url>
```

10. Name this file `update.xml` and save it to the `<ssc_install_dir>/update-site/installers` directory.
11. Restart Tomcat Server.
12. After you get a new SCA and Apps installer file (`Fortify_SCA_and_Apps_<version>_<OS>`), do the following:
  - a. Copy the new installer file to the `<ssc_install_dir>/update-site/installers` directory.
  - b. Open the `update.xml` file in a text editor.
  - c. Between the `versionId` tags, type the version ID for the new installer. (The version ID is the version number without the periods.)  
  
Check to make sure that the `<versionId>` tag value matches the Fortify Static Code Analyzer version in the installer.
  - d. Save the edited `update.xml` file.

Audit Workbench users can now check and install new Fortify Static Code Analyzer 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

Fortify Software Security Center licenses expire annually. For information about how to obtain a Fortify license file, see the *Micro Focus Fortify Software System Requirements* document. Place your downloaded `fortify.license` file in the `<ssc_install_dir>` directory.

## 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 Fortify Software Security Content" on page 134](#)

["Updating Rulepacks from the Micro Focus Fortify Update Server" on page 135](#)

["About Seeding the Fortify Software Security Center Database" on page 52](#)

## 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 52](#).

**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://support.fortify.com>).
  - 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. Before you proceed to seed the database, do the following:
  - a. Log in as an administrator, and then, on the Fortify header, select **ADMINISTRATION**.
  - b. In the left panel, under **Metrics and Tracking**, select **Rulepacks**.
  - c. On the Rulepacks page, select **IMPORT**.
  - d. In the IMPORT RULEPACK dialog box, click **+ADD FILES**.
  - e. Navigate to and select the `externalmetadata.xml` included with the downloaded content, and then click **START UPLOAD**.
  - f. After the import is completed, click **CLOSE**.
4. In the left panel, select **Configuration**, and then select **Seed Bundles**.
5. On the **Seed Bundles** page, click **BROWSE**, and then navigate to and select the `ReportBundle.zip` file.
6. 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 52](#)

# Part II: Using Micro Focus Fortify Software Security Center

The following chapters provide information about how to use Fortify Software Security Center.

# Chapter 10: 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 CloudScan, 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 .....	149
Security Management Workflow .....	150
User Accounts and Access .....	151
Active Directory/LDAP Integration .....	151
Logging in to Fortify Software Security Center for the First Time .....	151
Requesting Access to Fortify Software Security Center .....	152
Changing Your Password .....	155
Enabling and Disabling Receipt of Email Alerts .....	156
Disabling Keyboard Shortcuts (Hotkeys) .....	157
About the Fortify Software Security Center Dashboard .....	158
Issue Stats Page .....	158
Exporting Data to Comma-Separated Values Files .....	160
Deactivating Application Versions .....	161
Reactivating Application Versions .....	162
Accessing the Fortify Software Security Center API Documentation .....	163
Viewing Fortify Software Security Center Keyboard Shortcuts .....	164

## About the Central Role of Fortify Software Security Center

Fortify Software Security Center provides a location for collecting, correlating, 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:**

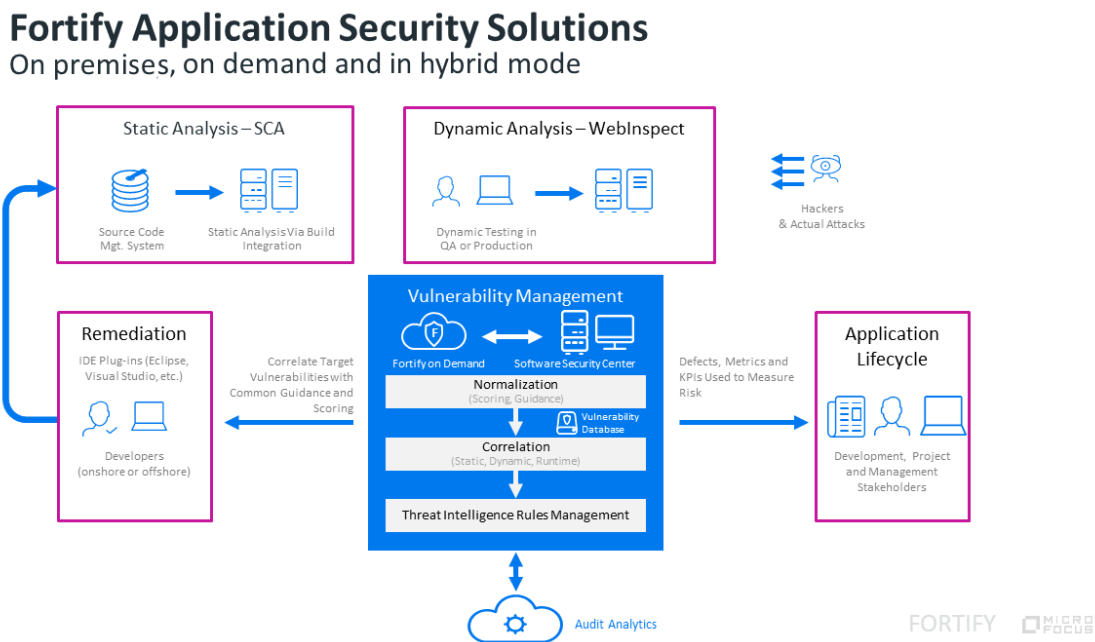
- Identify and prioritize a baseline of existing vulnerabilities
- Prevent new vulnerabilities from being introduced
- Remediate existing vulnerabilities and lower the baseline
- Ensure that your code is in compliance with internal and external security mandates

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, TFS/VSTS, 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:

<a href="#">Active Directory/LDAP Integration</a> .....	151
<a href="#">Logging in to Fortify Software Security Center for the First Time</a> .....	151
<a href="#">Requesting Access to Fortify Software Security Center</a> .....	152
<a href="#">Changing Your Password</a> .....	155
<a href="#">Enabling and Disabling Receipt of Email Alerts</a> .....	156
<a href="#">Disabling Keyboard Shortcuts (Hotkeys)</a> .....	157

### 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 89](#).

#### See Also

["Registering LDAP Entities" on page 173](#)

["Fortify Software Security Center User Account Management" on page 165](#)

### 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 155](#).

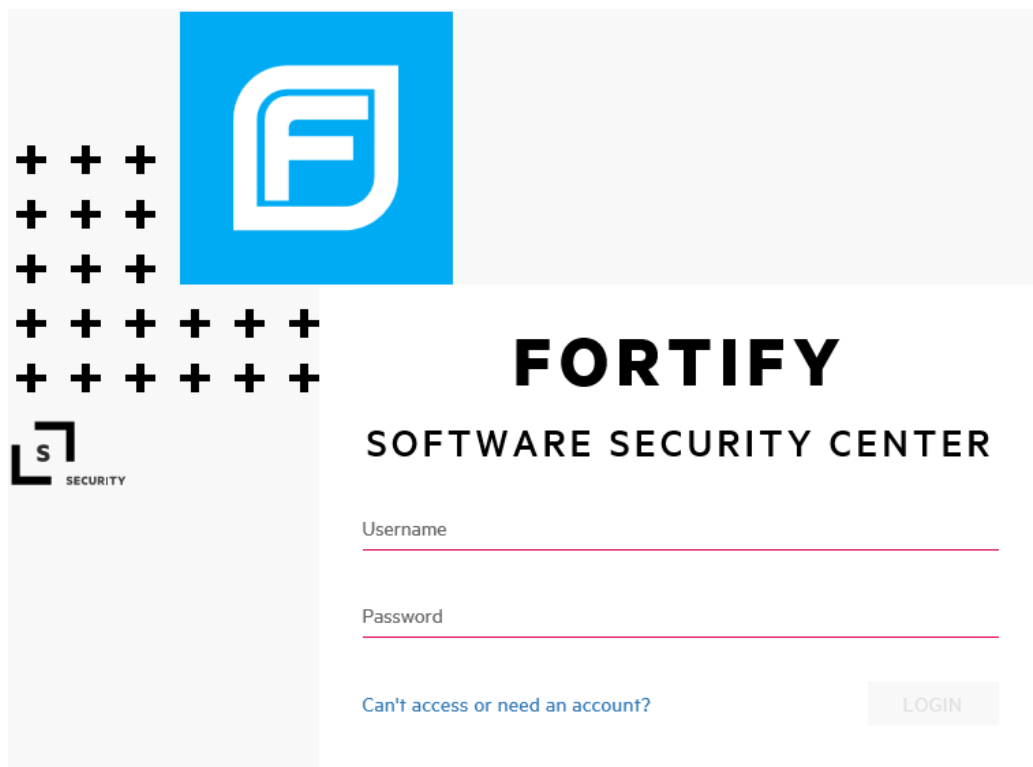
## Requesting Access to Fortify Software Security Center

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.

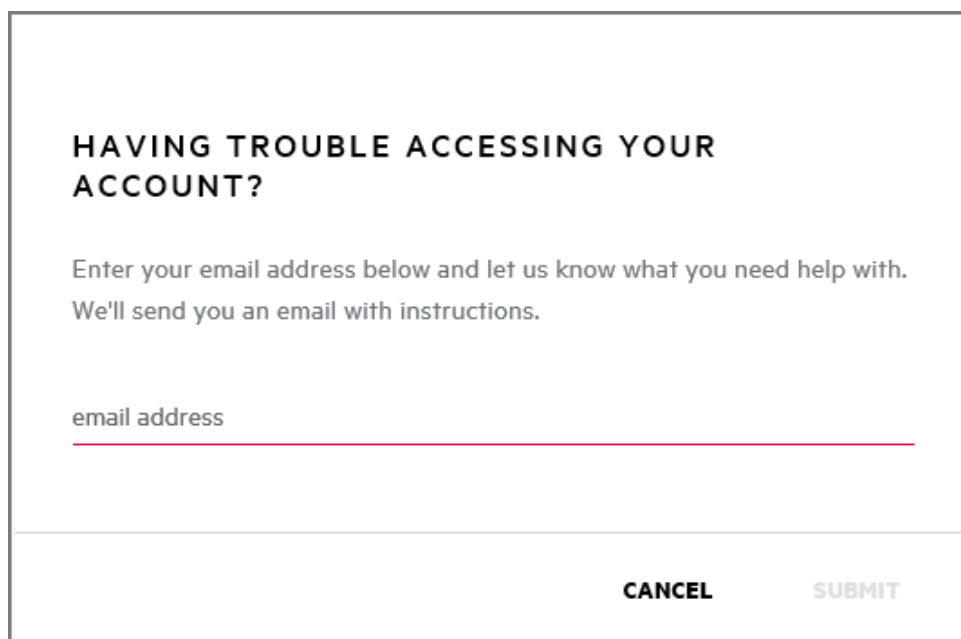
To request access to Fortify Software Security Center:



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 85.)

3. Type your email address, and then click **SUBMIT**.

### ACCOUNT REQUEST

To request an account with Fortify Software Security Center enter the account details and click 'Send'

First Name  
\_\_\_\_\_

Last Name  
\_\_\_\_\_

jdoe@microfocus.com  
\_\_\_\_\_

Application Version  
\_\_\_\_\_

Notes  
\_\_\_\_\_

**CANCEL**      **SEND**

The ACCOUNT REQUEST dialog box opens.

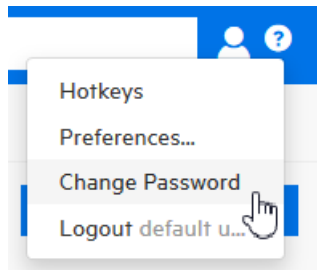
4. Provide the required information, and then click **SEND**.

Fortify Software Security Center sends your request to the Fortify Software Security Center administrator.

## Changing Your Password

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**.

A screenshot of the 'Change Password' dialog box. It has a title 'Change Password' and four input fields: 'Old Password', 'New Password', and 'Confirm New Password'. Below these is a 'Password Strength' indicator, which is a horizontal bar with an upward-pointing triangle. Below the bar is a paragraph of text: 'The SAVE button is enabled only after you type a 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.' At the bottom right are two buttons: 'CANCEL' and 'SAVE'.

The Change Password dialog box opens.

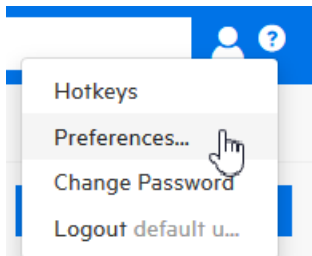
The **SAVE** button is enabled only after you type a strong new password that does not include your username or common phrases (names, movie or song titles, dates, or number or letter sequences). A combination of three or four unrelated words like "myredhorsedance" can work well. After your password 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**.

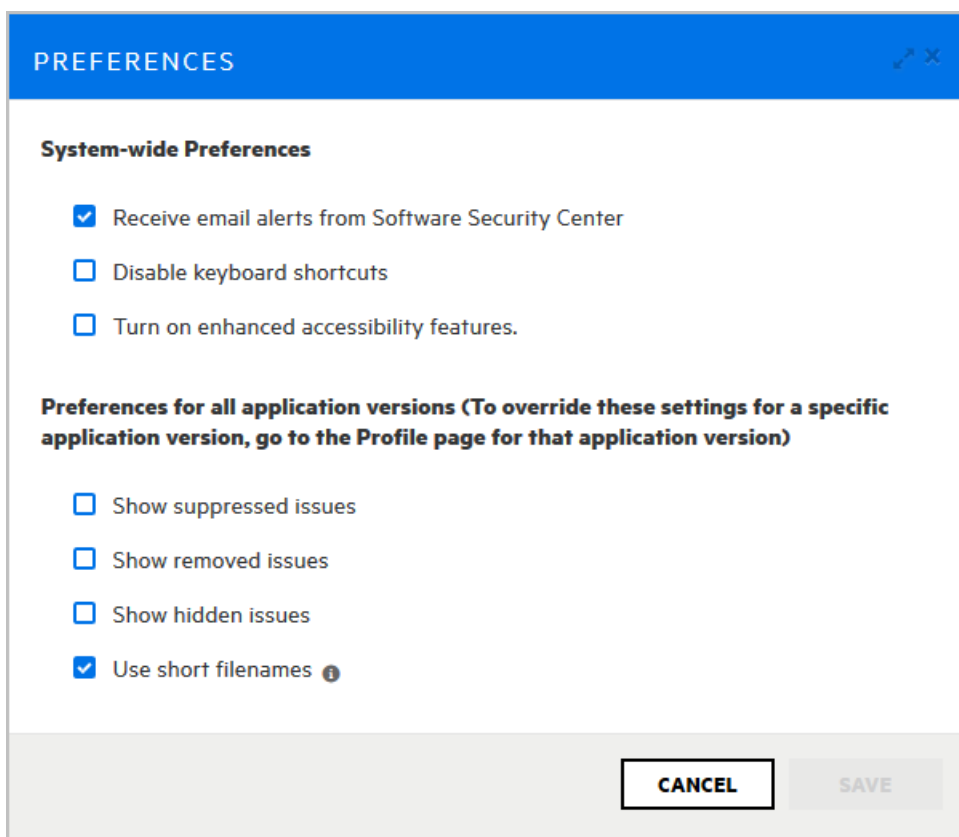
## Enabling and Disabling Receipt of Email Alerts

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**.



The PREFERENCES dialog box opens.

3. 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**.

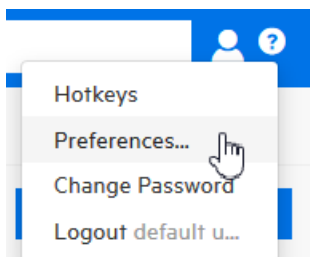
**See Also**

["Alert Definitions" on page 228](#)

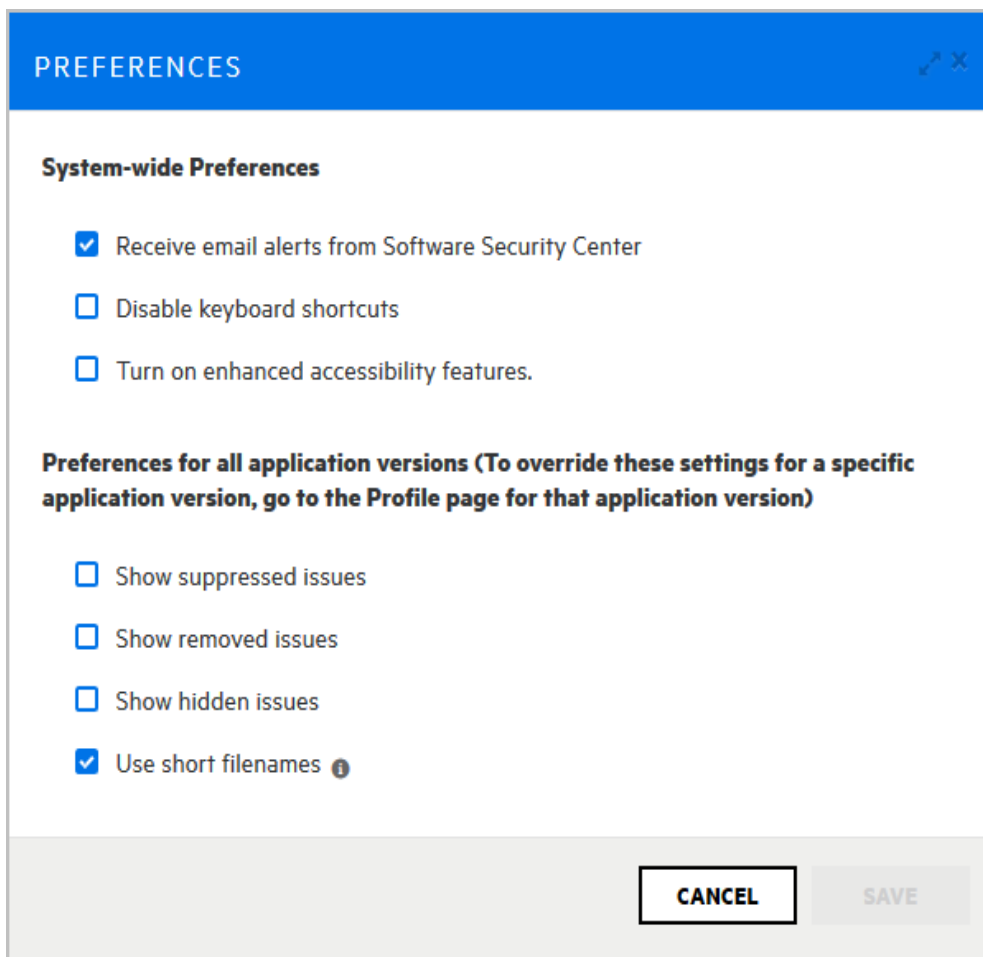
## Disabling Keyboard Shortcuts (Hotkeys)

To disable Fortify Software Security Center keyboard shortcuts:

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 **Preferences**.



3. In the PREFERENCES dialog box, under **System-wide Preferences**, select the **Disable keyboard shortcuts** check box, and then 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:

<a href="#">Issue Stats Page</a>	158
<a href="#">Exporting Data to Comma-Separated Values Files</a>	160
<a href="#">Deactivating Application Versions</a>	161
<a href="#">Reactivating Application Versions</a>	162
<a href="#">Accessing the Fortify Software Security Center API Documentation</a>	163
<a href="#">Viewing Fortify Software Security Center Keyboard Shortcuts</a>	164

### 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.

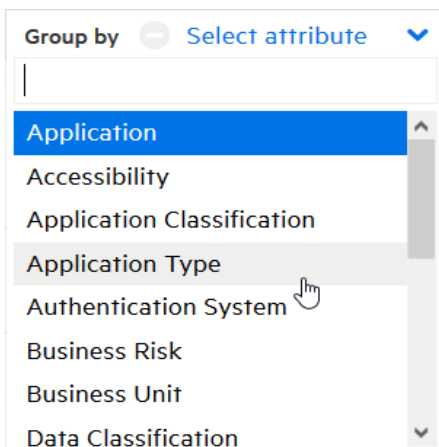
**Note:** If you are an administrator or security lead, you can set the thresholds that determine what users see when they review information on the Issue Stats page. For details, see ["Configuring Issue Stats Thresholds" on page 67](#).

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

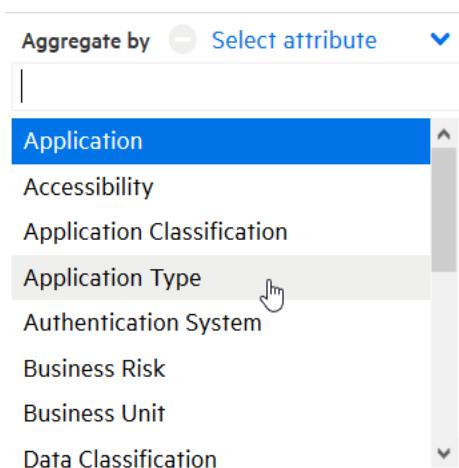


To group your data based on a single application version attribute, select the attribute from the **Group by** list. (The default grouping attribute is the application version.)

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 182](#).

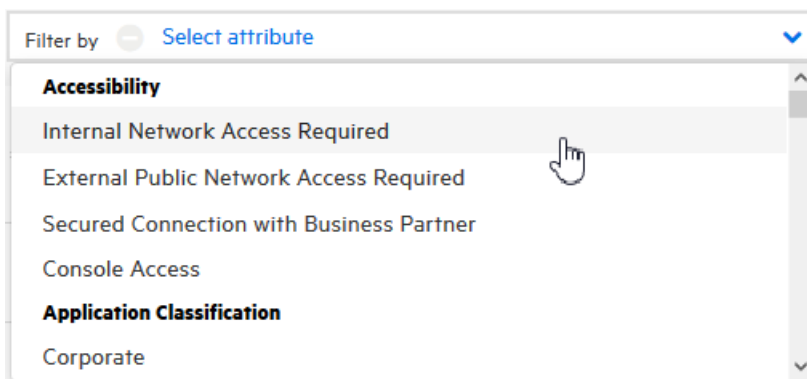
## Selecting an aggregating attribute



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 182](#).

### Selecting one or more filtering attributes

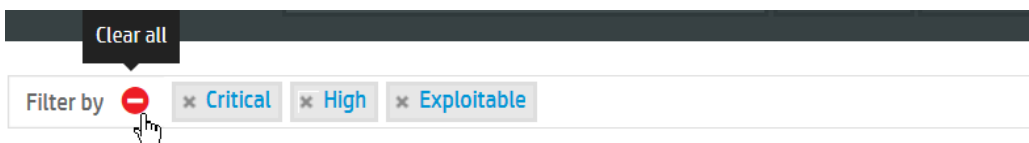


To selectively display data based on an application attributes, select an attribute from the **Filter by** list. You can select multiple attributes, but you must select them one at a time.



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 Fortify Software Security Center data displayed on the Issue Stats and AUDIT pages to comma-separated values (CSV) files.



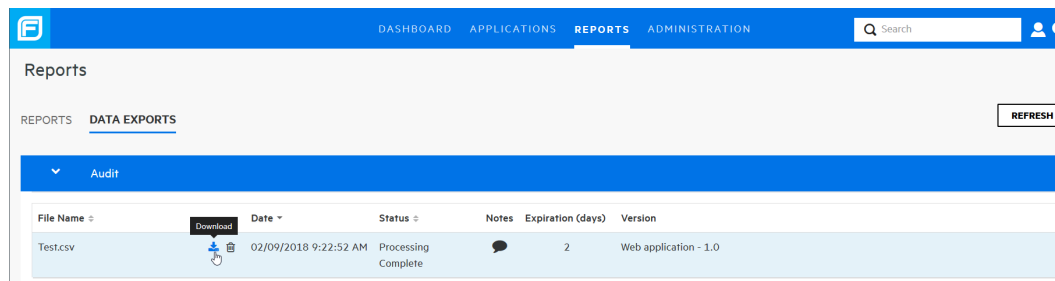
To export data from the Issue Stats or AUDIT page to a CSV file:


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**.  
The EXPORT CSV dialog box opens.
3. 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 .
- d. Specify whether to save or open the file.

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 104](#).

## Deactivating Application Versions

Deactivating an application version hides that version on 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, select the application version you want to deactivate.  
The AUDIT page for the selected version opens.
2. Click **PROFILE**.
3. In the APPLICATION PROFILE dialog box, click **APPLICATION SETTINGS**.
4. In the **Version Settings** panel, 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**

["Deleting an Application Version " on page 223](#)

### **Reactivating Application Versions**

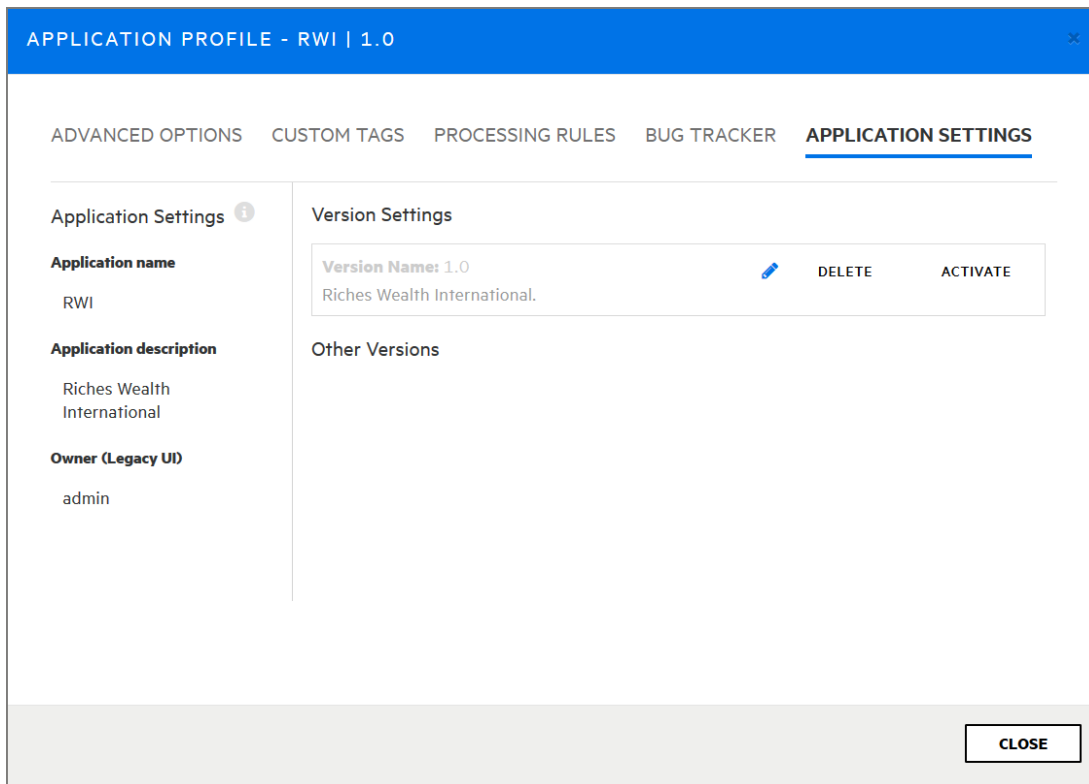
If a specific application version has been deactivated and is not listed on the DASHBOARD or in the Applications view, you can reactivate it to make it visible again.

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.  
The AUDIT page for the selected application version opens.
4. On the application version toolbar, click **PROFILE**.  
The APPLICATION PROFILE dialog box opens.
5. Click **APPLICATION SETTINGS**.



6. In the **Other Versions** section, next to the inactive version you want to reactivate, 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.

## 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 .  
The About Fortify Software Security Center <version> box opens.

i About Fortify Software Security Center 18.20.0104x

**SUPPORT**  
Please visit <https://softwaresupport.softwaregrp.com> to contact support.  
Main US Phone +1-844-260-7219

**DOCUMENTATION**  
Please visit <https://www.microfocus.com/documentation/fortify-software-security-center/>  
for access to all of our documentation.  
[API Documentation](#)

© 2008 - 2018 Micro Focus. All rights reserved.

**CLOSE**

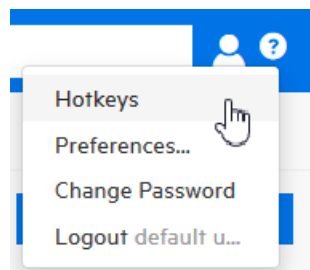
2. Click **API Documentation**.

The FORTIFY SOFTWARE SECURITY CENTER API DOCUMENTATION VERSION <version> web page opens.

## Viewing Fortify Software Security Center Keyboard Shortcuts

To view the keyboard shortcuts 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

["Disabling Keyboard Shortcuts \(Hotkeys\)" on page 157](#)

## Chapter 11: 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, and how to register AD/LDAP entities with Fortify Software Security Center.

### 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 the next page](#).

### 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 126](#).

Role	Description
Administrator	Has full access to the system and all results
Application Security Tester	Performs tasks required to execute dynamic scan requests, including: <ul style="list-style-type: none"><li>• View application versions</li><li>• View and generate reports</li><li>• Process dynamic scans</li><li>• Upload scan results</li><li>• Audit issues</li></ul>
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" below](#)

## 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 panel of the ADMINISTRATION page, select **Users**, and then select **Roles**.

3. In the **Roles** toolbar, click **NEW**.  
The CREATE NEW ROLE dialog box opens.
4. Provide the information described in the following table.

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.  <b>Note:</b> 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**.  
The ADD PERMISSIONS dialog box opens.
6. 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**.
8. In the CREATE NEW ROLE dialog box, click **SAVE**.

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 panel 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:

<a href="#">Creating Local User Accounts</a> .....	168
<a href="#">Editing Local User Accounts</a> .....	170
<a href="#">Unlocking User Accounts (Local Users Only)</a> .....	172
<a href="#">Registering LDAP Entities</a> .....	173

### 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.

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 panel of the ADMINISTRATION view, select **Users**, and then select **Local**.  
The **Local** page opens and lists local users.
3. In the **Local** toolbar, click **NEW**.  
The CREATE NEW USER dialog box opens.
4. Provide the information listed in the following table.

Field or Check Box	Description
Username	Username for Fortify Software Security Center logon.
First Name	First name of user.
Last Name	Last name of user.
Email	Email address of user.
Roles	Select the check boxes that correspond to the roles you want to



Field or Check Box	Description
	assign to the user.
Password	Password for the new user.
Confirm Password	Password for the new user.
User must change password at next login	Select this check box 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 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.

5. To specify the applications that the new user can access:
  - a. In the **Access** section, click **+ ADD**.  
The SELECT APPLICATION VERSION dialog box opens.
  - b. From the **Application** list, select the application to which you want the user to have access.  
The **Versions** list displays all existing versions of the selected application.
  - c. To select all versions, select the check box to the left of **Versions**. Otherwise select the check boxes for the versions that the user can access.
  - d. Click **DONE**.
  - e. To add another application version or versions, repeat steps a through d.
6. 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 users.

**See Also**

["Editing Local User Accounts" on the next page](#)

["Unlocking User Accounts \(Local Users Only\)" on page 172](#)

## Editing Local User Accounts

To edit a local user account:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left panel of the ADMINISTRATION view, select **Users**, and then click **Local**.
3. Locate the user account you want to edit, and then click the row to expand it and view account details.

The screenshot shows the user account editing interface for 'susan'. At the top, a header bar contains the user's details: a checkbox, 'susan', 'Richards', 'Susan', 'susan@fortify.com', and 'Developer'. Below this, the form is divided into several sections:

- First Name:** A text input field containing 'Susan'.
- Last Name:** A text input field containing 'Richards'.
- Roles:** A list box containing 'Developer' with a checked checkbox.
- Email:** A text input field containing 'susan@fortify.com'.
- Access:** A list box containing several application versions with unchecked checkboxes: 'Bill Payment Processor 1.1', 'Logistics 1.3', 'Logistics 2.5', 'RWI 1.0', and 'Web application 1.0'.
- Additional Options:** Three checkboxes are located to the right of the 'Roles' section: 'User must change password at next login' (unchecked), 'Password never expires' (checked), and 'Suspended' (unchecked).

At the bottom of the form, there are three buttons: 'EVENT LOG' (black), 'DELETE' (black), and 'EDIT' (blue).

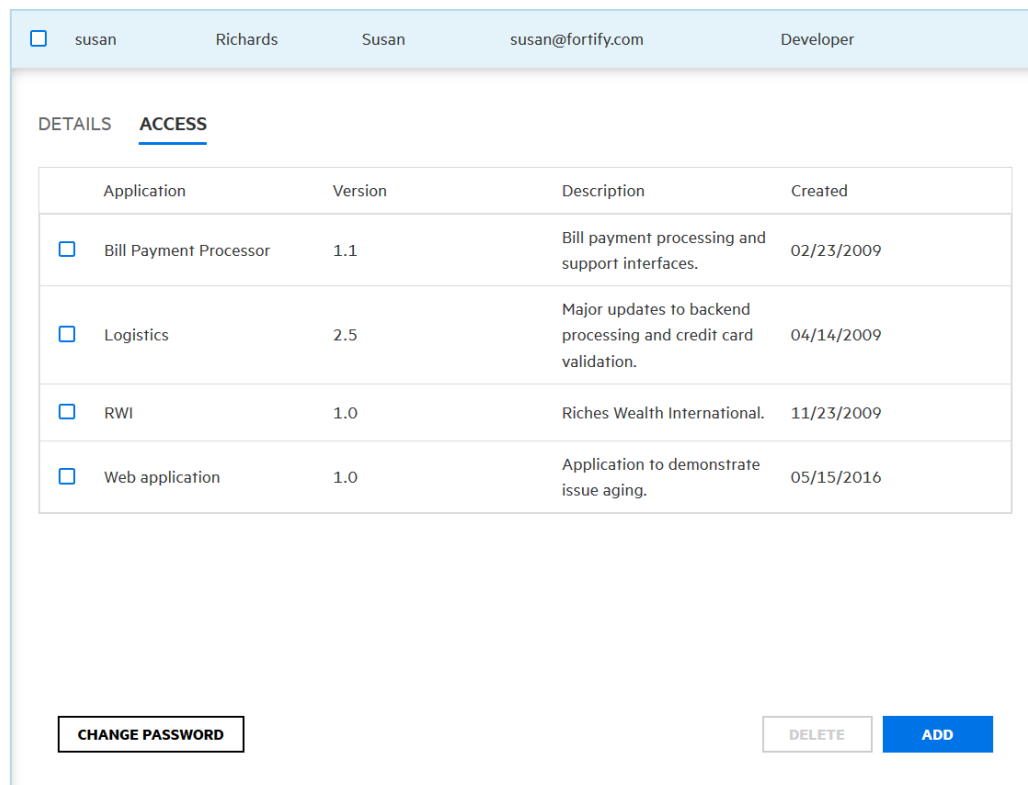
4. Click **EDIT**.

The screenshot shows a user management interface for a user named Susan Richards. At the top, a header bar contains a square icon, the first name 'susan', the last name 'Richards', the full name 'Susan', the email address 'susan@fortify.com', and the role 'Developer'. Below this, the 'DETAILS' tab is selected, with 'ACCESS' as an alternative tab. The form is divided into several sections: 'First Name\*' with a text input containing 'Susan'; 'Last Name\*' with a text input containing 'Richards'; 'Email\*' with a text input containing 'susan@fortify.com'; 'Roles\*' with a list of roles including Administrator, Security Lead, Manager, Developer (checked), View-Only, and Application Security Tester; and a password policy section with checkboxes for 'User must change password at next login', 'Password never expires' (checked), and 'Suspended'. At the bottom, there are three buttons: 'CHANGE PASSWORD', 'CANCEL', and 'SAVE'.

The **DETAILS** tab displays basic user information, including the name, email address, password expiration policy used for the account, and the roles to which the user is assigned.

5. Make any necessary changes to the fields.

6. To change the application versions (either remove or add) to which the user has access:
  - a. Select the **ACCESS** tab.



- b. To unassign the user from one or more application versions, select the corresponding check box(es), and then click **DELETE**.
    - c. To assign the user to another application version, click **ADD**, and then use the SELECT APPLICATION VERSION dialog box to locate and select the application version (s).

**Note:** Any changes you make on the **ACCESS** tab are saved automatically and immediately.

7. To save changes made on the **DETAILS** tab select the **DETAILS** tab, and then click **SAVE**.

### See Also

["Creating Local User Accounts" on page 168](#)

["Unlocking User Accounts \(Local Users Only\)" below](#)

### Unlocking User Accounts (Local Users Only)

After a local user tries unsuccessfully to log in to Fortify Software Security Center more than three times in a row, Fortify Software Security Center prevents the user from attempting more logons. 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.

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 panel of the ADMINISTRATION view, select **Users**, and then click **Local**.
3. Bring up the locked user account, expand the row to view account details, and then click **EDIT**.

At the bottom left, the message **User has reached the maximum login attempts** is displayed.

4. To the right of the message, click **Unlock user**.

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 168](#)

["Editing Local User Accounts" on page 170](#)

## 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 panel, click **Users**, and then select **LDAP**.
3. On the **LDAP** toolbar, click **+ADD**.

The **ADD NEW LDAP ENTITY** window opens.

ADD NEW LDAP ENTITY

To register an LDAP entity, select the LDAP entity type, enter the entity name, and then click FIND. Select the entity to register from the search results, specify the appropriate role(s), and then click SAVE.

LDAP Entity  Name  (wildcard (\*) allowed)

SPECIFY THE LDAP ENTITY AND NAME FIELDS, THEN CLICK FIND.

4. From the **LDAP Entity** list, select the type of LDAP entity you want to register (**Group, User**,

or **Organizational Unit**).

- In the list of returned entities, select the user, group, or organizational unit that you want to register.

**ADD NEW LDAP ENTITY**

To register an LDAP entity, select the LDAP entity type, enter the entity name, and then click FIND. Select the entity to register from the search results, specify the appropriate role(s), and then click SAVE.

LDAP Entity: User    Name: sscuser1 (wildcard (\*) allowed)    **FIND**

Name	Distinguished Name	Last Name	First Name	Email
sscuser1	CN=SSCUser1,CN=Users,DC=sscqa,DC=com	User1	SSCUser1	

**Roles**    **Access**    + ADD    - DELETE

Administrator

Security Lead

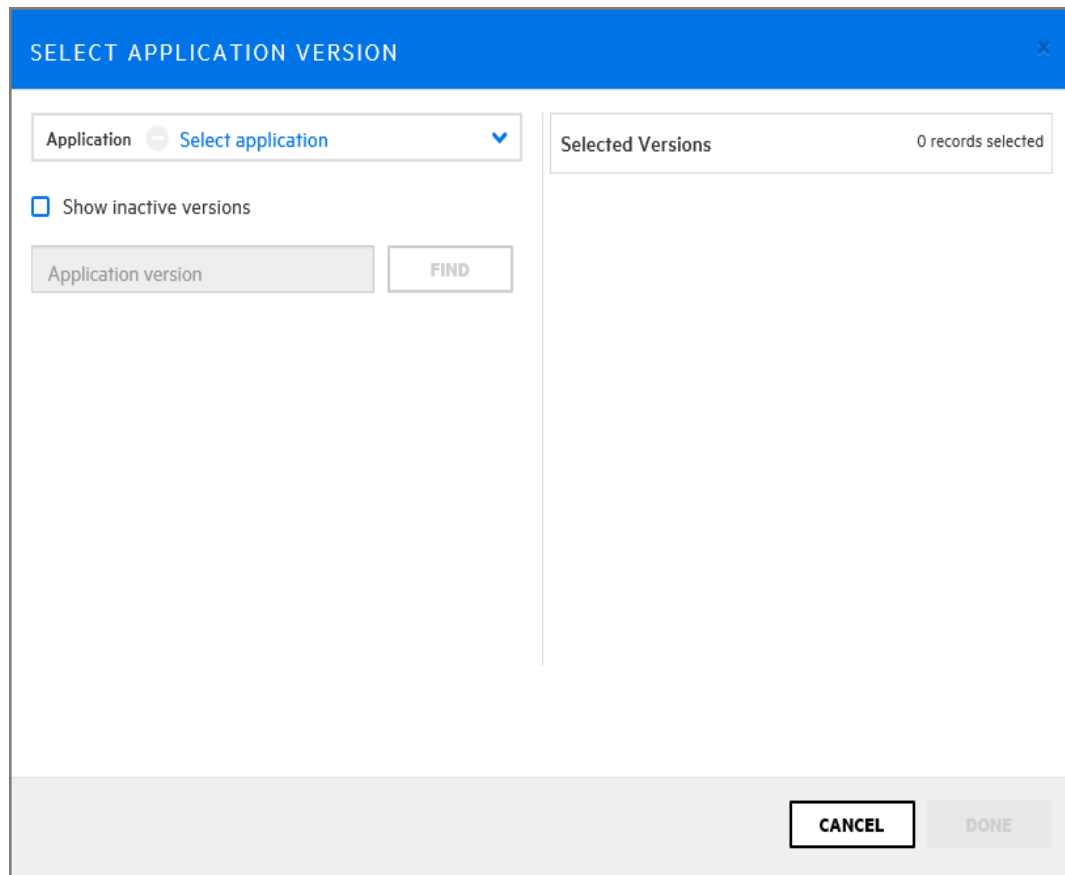
Select the application versions for the user to access.

**CANCEL**    **SAVE AND ADD ANOTHER**    **SAVE**

- In the **Roles** section, select the check boxes that correspond to the roles you want to assign to the selected entity.
- 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**.



The screenshot shows a dialog box titled "SELECT APPLICATION VERSION". At the top left, there is a dropdown menu labeled "Application" with the text "Select application" and a downward arrow. To the right of this is a box labeled "Selected Versions" with "0 records selected" below it. Below the dropdown menu is a checkbox labeled "Show inactive versions". At the bottom left, there is a text input field labeled "Application version" and a "FIND" button. At the bottom right, there are two buttons: "CANCEL" and "DONE".

The SELECT APPLICATION VERSION dialog box opens.

- b. From the **Application** list, select the name of an application that you want the LDAP entry 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.

9. To initiate the LDAP refresh process manually so that your changes are evident sooner than

they would be otherwise:

- a. On the LDAP page, select the check box for the LDAP entity you want to refresh.
- b. On the LDAP toolbar, click **REFRESH**.

For information about how to configure LDAP servers, see ["Configuring LDAP Servers" on page 89](#).

**See Also**

["LDAP User Authentication" on page 53](#)

["About Managing LDAP User Roles" on page 128](#)



# Chapter 12: 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](#) .....179
- [About the Application Creation Process](#) .....179
- [Strategies for Creating Application Versions](#) .....179

About Annotating Application Versions for Reporting .....	180
Viewing a List of Fortify Software Security Center Applications .....	180
About Creating Application Versions .....	181
Application Version Attributes .....	181
About Issue Templates .....	185
Creating the First Version of a New Application .....	187
Adding a New Version to an Application .....	189
Enabling Auto-Apply and Auto-Predict for an Application Version .....	193
Searching Applications and Application Versions from the Applications View .....	195
Updating the Application Overview Page .....	195
Editing Application Version Details .....	195
Using Bug Tracking Systems to Help Manage Security Vulnerabilities .....	196
Bug Tracker Configuration .....	196
Velocity Templates for Bug Filing .....	196
Assigning a Bug Tracking System to an Application Version .....	200
Submitting a Bug for One or More Issues .....	203
Changing the Template Associated with an Application Version .....	205
Setting Analysis Results Processing Rules for Application Versions .....	206
Configuring Audit Assistant Options for an Application Version .....	211
Custom Tags .....	211
Adding Custom Tags to the System .....	212
Modifying Custom Tag Attributes .....	214
Globally Hiding Custom Tags .....	215
Deleting Custom Tags .....	215
Adding Custom Tag Values .....	216
Editing Custom Tags .....	216
Deleting Custom Tag Values .....	217
Associating Custom Tags with Issue Templates .....	217
Removing Custom Tags from Issue Templates .....	218
Assigning Custom Tags to Application Versions .....	219
Disassociating a Custom Tag from an Application Version .....	220
Managing Custom Tags Through Issue Templates .....	221

Managing Custom Tags Through an Issue Template in an FPR File .....	221
About Deleting Application Versions .....	221
Deactivating Application Versions .....	222
Reactivating Application Versions .....	222
Deleting an Application Version .....	223

## 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 .....	179
Strategies for Creating Application Versions .....	179
About Annotating Application Versions for Reporting .....	180
Viewing a List of Fortify Software Security Center Applications .....	180

### 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 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 creation wizard screens.

#### Next

["Application Version Attributes" on page 181](#)

#### See Also

["Template Selection" on page 186](#)

### 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 222](#).

**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 195](#)

## 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 179](#)

["Creating the First Version of a New Application" on page 187](#)

["Adding a New Version to an Application" on page 189](#)

### 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 table lists 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.

**Business Risk Rating** refers to the relative risk the application poses to the organization's business goals (high, medium, or low).

Technical Attribute	Description
*Development Phase	Current phase of development the application version is in.

Technical Attribute	Description
*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	
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 panel, under **Templates**, click **Attributes**.  
The Attributes page lists the attributes on the right.
4. Click **NEW**.

The CREATE NEW ATTRIBUTE dialog box opens.

5. Provide the information described in the following table.

Field	Description
Name	Type a descriptive name for the attribute.
Description	Type a brief description. The description is displayed under the attribute field in the Create New Application 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 wizard.

Field	Description
Category	<p>Select an attribute type. Depending on the category you select, the attribute is displayed on the <b>Business Attributes</b> step, the <b>Technical Attributes</b> step, or the <b>Organization Attributes</b> step of the CREATE NEW APPLICATION wizard.</p> <p><b>Note:</b> If your Fortify Software Security Center instance is integrated with Fortify WebInspect, the list also includes the <b>Dynamic Scan Request</b> category.</p>
Scope	<p>Select the value that indicates whether the attribute applies only to application versions, runtime applications, or to both.</p>
Type	<p>Select one of the following control types:</p> <ul style="list-style-type: none"><li>• To create a check box for the attribute, select <b>Boolean</b>.</li><li>• To create a calendar selection control for the attribute, select <b>Date</b>.</li></ul> <p><b>Note:</b> This type is not available for a Dynamic Scan Request attribute.</p> <ul style="list-style-type: none"><li>• To create a list from which a user can select only a single value for the attribute, select <b>List of Values - Single Selection</b>.</li></ul> <p><b>Note:</b> If you create a single-select type attribute, users can select it from the <b>Group by</b> and <b>Aggregate by</b> lists on the Dashboard to customize the data they view.</p> <ul style="list-style-type: none"><li>• To create a list from which a user can select multiple values for the attribute, select <b>List of Values - Multiple Selection</b>.</li><li>• To create a field that accepts an integer value, select <b>Integer</b>.</li><li>• To create a text field into which a user can type a single line of text, select <b>Text - Single Line</b>.</li><li>• To create a text field into which a user can type multiple lines of text, select <b>Text - Multiple Lines</b>.</li></ul> <p><b>Note:</b> If you select one of the <b>List of Values</b> types, additional fields are displayed in which you add the values and their descriptions, and specify whether or not they are hidden.</p>

6. Click **SAVE**.



The new attribute is available the next time a user uses the CREATE NEW APPLICATION wizard.


For instructions on how to specify custom attributes in existing application versions, see ["Specifying New Custom Attributes in Existing Application Versions" below](#).

**See Also**

["Application Version Attributes" on page 181](#)

### Specifying New Custom Attributes in Existing Application Versions

To apply a new custom attribute to existing application versions:

1. On the Fortify header, select **APPLICATIONS**.
2. On the Applications page, select the application 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.   
The Edit Version wizard opens to **Step 1. GENERAL**.
6. 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 182](#)

["Editing Application Version Details" on page 195](#)

### 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 panel, 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 *Micro Focus Fortify Audit Workbench User Guide*.

### Adding Issue Templates to the System

To add an issue template that was 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 panel 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**.  
The CREATE NEW ISSUE TEMPLATE dialog box opens.
5. In the **Name** 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**.

### 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. In the toolbar, click **+ NEW APPLICATION**.

The Create New Application wizard opens to **STEP 1. GENERAL**.

3. Under **Application Setup**, do the following:
  - a. In the **Application name** box, type a name for the new application.
  - b. (Optional) in the **Application description** box, type a description.
4. In the **Version Setup** section, provide the information described in the following table.

Field	Description
Version name	Type a name for the version. The wizard uses the application name and appends the version name to it automatically.
Version description	(Optional)
Use existing application version	<ol style="list-style-type: none"><li>a. To use the settings of an existing application version, select this check box. Otherwise, proceed to <a href="#">step 5</a>.</li><li>b. To open the Select Application Version dialog box, click <b>Browse</b>.</li><li>c. From the <b>Applications</b> list, select the application.</li><li>d. From the <b>Versions</b> list, select the row that displays the version name you want, and then click <b>DONE</b>.  By default, Fortify Software Security Center includes all settings of the selected application version.</li><li>e. To exclude some of the settings, clear one or more of the following check boxes:<ul style="list-style-type: none"><li>○ <b>Version attributes</b></li><li>○ <b>Custom tags</b></li><li>○ <b>Analysis processing rules</b></li><li>○ <b>User access settings</b></li><li>○ <b>Bug tracker settings</b></li></ul></li></ol>

Field	Description
	f. To copy over all of the issues associated with the selected application version, select the <b>Application state</b> check box.

- To advance to **STEP 2. DEFINE ATRIBUTES AND RISK**, click **NEXT**.
- On the **Technical Attributes** tab, provide the information described in the following table.

Field	Description
Development Phase	Leave <b>New</b> 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.
Authentication System	Select the check boxes for the authentication systems used to access the application.

- 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 version applies.
Region	Select the region for which the application version is being developed.

- Click the **Business Risk Attributes** tab, and then 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.

9. To advance to STEP 3. CHOOSE TEMPLATES, click **NEXT**.
10. Under **Issue Template**, select the check box for a template to set the minimum thresholds for issue detection. To see a description of each template, select its check box.
11. To advance to **STEP 4. ASSIGN RESPONSIBILITIES AND TEAM** section, click **NEXT**.
12. Under **Assign Responsibilities**, click **Project Manager, Security Manager, Development Manager**, or **"TEAM"**.
13. Under **Assign Team**, do one of the following:
  - 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 you want to assign.

**Note:** To find a specific user, type a username into the **Search by user name** box, and then click **FIND**.

14. Click **FINISH**.

Fortify Software Security Center indicates that the application was successfully created and adds the new application version to the application versions list.

## 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. On the Fortify header, click **APPLICATIONS**.
3. On the APPLICATIONS page, select a version of the application for which you want to create a new version.

Fortify Software Security Center displays the AUDIT page for that version.

4. On the application version toolbar, click **+ NEW VERSION**  
The Create New Version wizard opens to **Step 1. GENERAL**.

5. Under **Version Setup**, do the following:

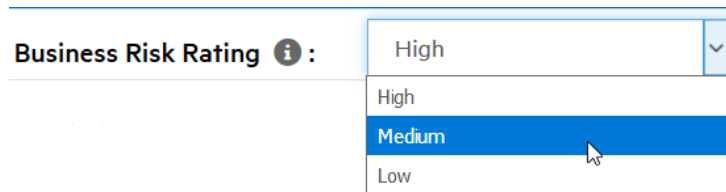
- a. In the **Version name** box, type a name for the new version.  
The wizard uses the application name and appends the version name to it automatically.
- b. In the **Version description** box, type a description of the new version.
- c. If you prefer to specify all of the attributes of the new version manually, proceed to apply the setting of an existing application version to the new version:
  - i. Select the **Use existing application version** check box.
  - ii. Click **BROWSE**, and then navigate to and select the application version with the attribute settings you want to apply to the new version.
  - iii. Clear any of the following check boxes for the settings that you do not want to apply to this version:
    - **Version attributes**
    - **Custom tags**
    - **Analysis processing rules**
    - **User access settings**
    - **Bug tracker integration settings**
- d. To copy over all of the issues associated with the selected application version, select the **Application state** check box.

6. To advance to **Step 2. DEFINE ATTRIBUTES AND RISK**, click **NEXT**.

7. To specify a business risk rating:

**Business Risk Rating** ⓘ : High 

- a. To the right of the **Business Risk Rating** value, click the pencil icon.



<b>Business Risk Rating</b> ⓘ :	High
	High
	Medium
	Low

- b. From the **Business Risk Rating** list, select the level of risk that this application version poses to the organization's business goals.

8. 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 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.

Technical Attributes  Organization Attributes  Business Risk Attributes 

---

9. Click **Organization Attributes**, 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 version applies.
Region	Select the region for which the application version is being developed.

Technical Attributes  Organization Attributes  Business Risk Attributes 

---

10. Click **Business Risk Attributes**, and then 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 **Step 3. CHOOSE TEMPLATES**, 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, select its check box.
13. To advance to **Step 4. ASSIGN RESPONSIBILITIES AND TEAM** section, click **NEXT**.
14. Under **Assign Responsibilities**, select one or more of the following roles:
  - **Project Manager**
  - **Security Manager**
  - **Development Manager**
  - **TEAM**
15. Under **Assign Team**, do one of the following:
  - 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,

- 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 you want to assign.

**Note:** To find FIND a specific user, type a username into the **Search by user name** box, and then click **FIND**.

16. Click **FINISH**.

Fortify Software Security Center indicates that the version was successfully created and adds the new application version to the application versions list.



## 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**.

APPLICATION PROFILE - LOGISTICS | 2.5

**ADVANCED OPTIONS** CUSTOM TAGS PROCESSING RULES BUG TRACKER APPLICATION SETTINGS  
AUDIT ASSISTANT TRAINING AUDIT ASSISTANT OPTIONS

Show suppressed issues

Show removed issues

Show hidden issues

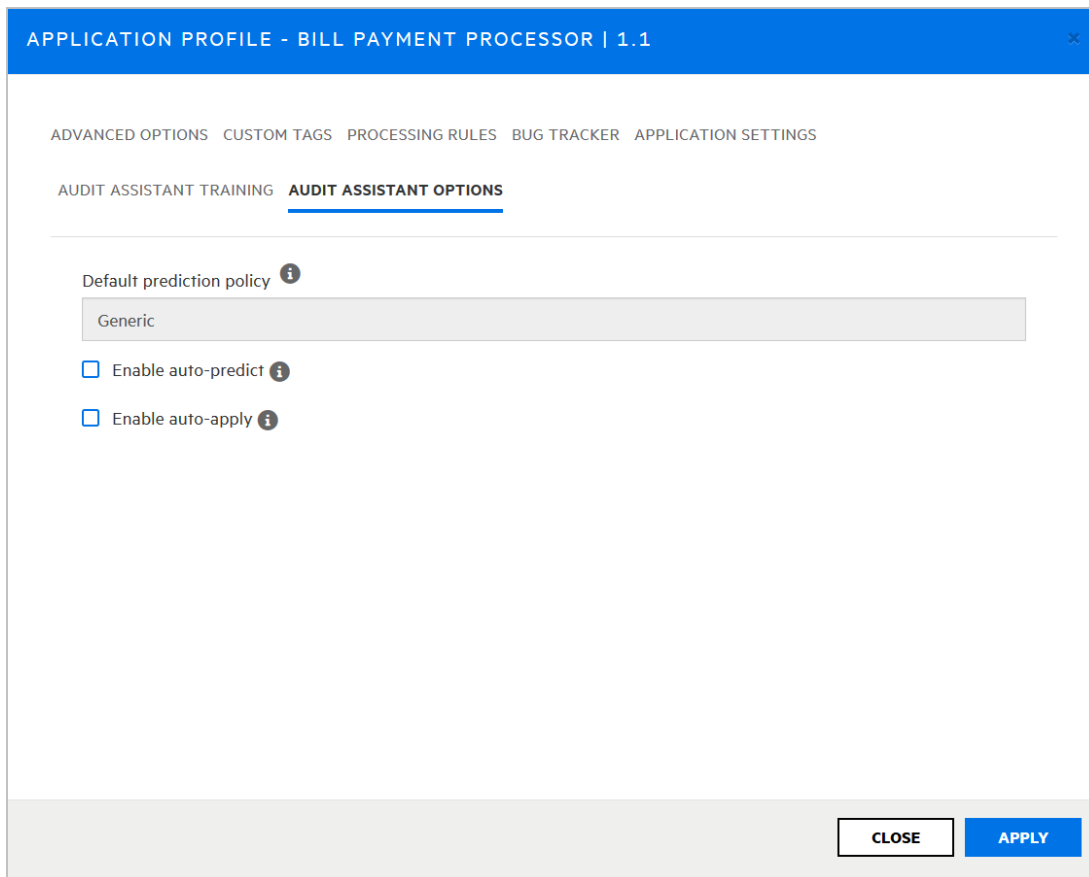
Use short filenames ⓘ

Issue counts by state, based on current selections:  
Hidden issues: 0 Suppressed issues: 0 Removed issues: 0

Issue count totals (A given issue might be counted in more than one of the following states.):  
Hidden issues: 0 Suppressed issues: 50 Removed issues: 0

CLOSE APPLY

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 75.](#))
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 74](#)

## Searching Applications and Application Versions from the Applications View

To search for a specific application or application version from the Applications view:


<input type="text" value="Search Apps and Versions"/>	<input type="button" value="Find"/>
---	-------------------------------------

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 277](#)

## 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 box, 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. At the top of the AUDIT page, click the edit icon .  
The EDIT VERSION: <version> wizard opens.
4. Edit values in any of the fields described in ["Adding a New Version to an Application" on page 189](#).
5. After you make your changes, on Step 4, and then click **FINISH**.

### See Also

["Changing the Template Associated with an Application Version" on page 205](#)

## 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:

<a href="#">Bug Tracker Configuration</a> .....	196
<a href="#">Velocity Templates for Bug Filing</a> .....	196
<a href="#">Assigning a Bug Tracking System to an Application Version</a> .....	200
<a href="#">Submitting a Bug for One or More Issues</a> .....	203

### 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](#)

### 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" below](#)

["Editing Velocity Templates for Bug Tracker Plugins" on the next page](#)

["Deleting Velocity Templates" on page 199](#)

### 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 panel, 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**.  
The ADD TEMPLATE dialog box opens.
6. In the **Mapped field** 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” are 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

["Bug Tracker Configuration" on page 196](#)

["Velocity Templates for Bug Filing" on page 196](#)

["Editing Velocity Templates for Bug Tracker Plugins" below](#)

["Deleting Velocity Templates" on the next page](#)

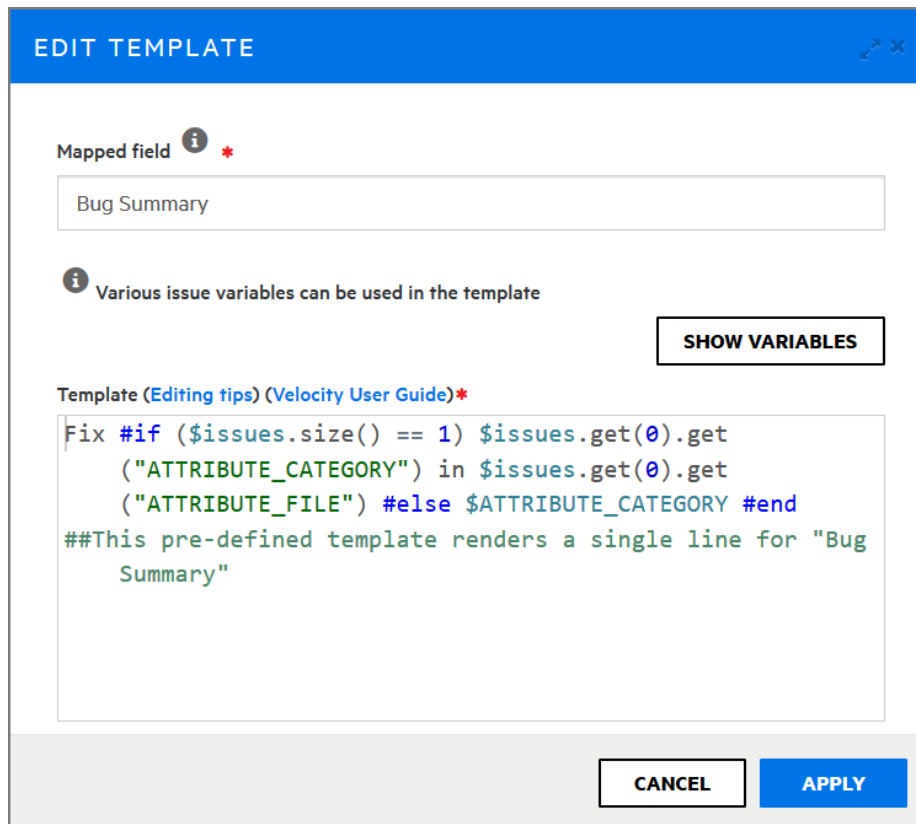
#### Editing Velocity Templates for Bug Tracker Plugins

To edit the Velocity template for a bug tracker plugin:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left panel of the ADMINISTRATION page, select **Templates**, and then select **Bug Filing**.
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.  
The EDIT TEMPLATE dialog box opens.



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

["Velocity Templates for Bug Filing" on page 196](#)

["Adding Velocity Templates to Bug Tracker Plugins" on page 197](#)

["Deleting Velocity Templates" below](#)

### 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 panel 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 196](#)

["Adding Velocity Templates to Bug Tracker Plugins" on page 197](#)

["Editing Velocity Templates for Bug Tracker Plugins" on page 198](#)

## 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 120](#).

To integrate with a bug tracking system:

1. On the Fortify header, click APPLICATIONS.
2. In the **Applications** table, click the application version number to which you want to assign a bug tracker.

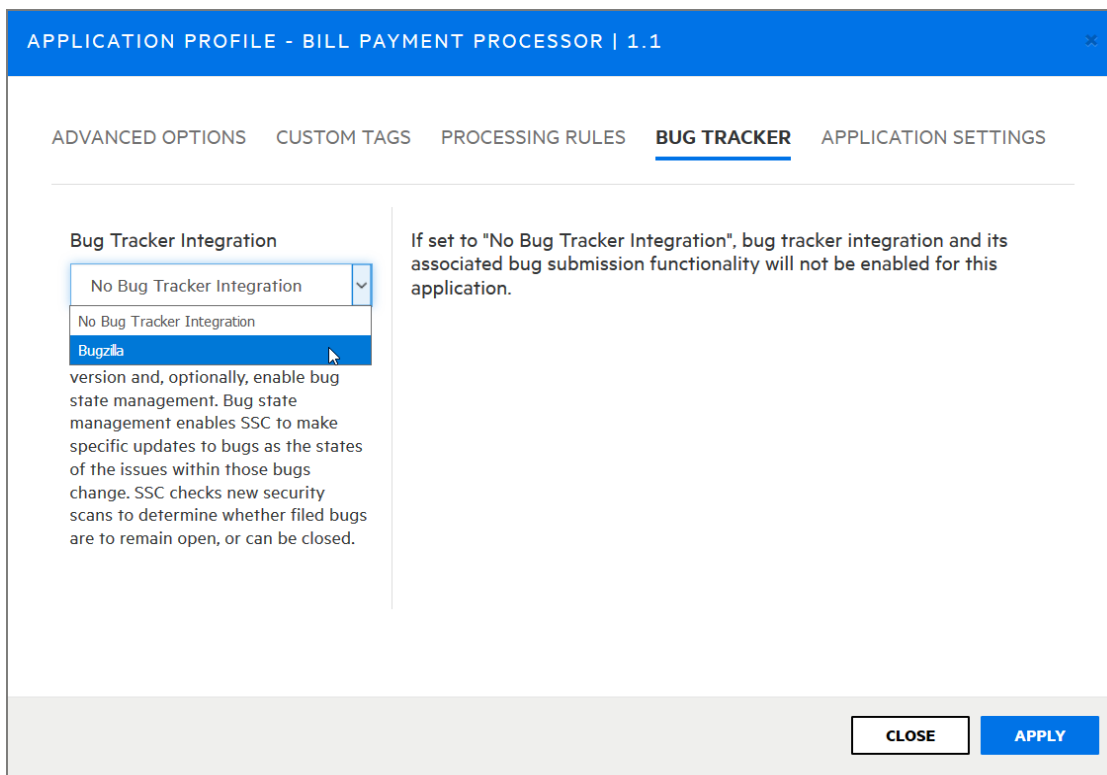
The AUDIT page for the selected application version lists the issues with the version.

3. At the upper right, click **PROFILE**.

The APPLICATION PROFILE - <Application\_Name><Application\_Version> dialog box opens.

4. 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. Click **APPLY**.

APPLICATION PROFILE - BILL PAYMENT PROCESSOR | 1.1

ADVANCED OPTIONS CUSTOM TAGS PROCESSING RULES **BUG TRACKER** APPLICATION SETTINGS

**Bug Tracker Integration**

Bugzilla

You can specify a bug tracker plugin to use to submit bugs against this version and, optionally, enable bug state management. Bug state management enables SSC to make specific updates to bugs as the states of the issues within those bugs change. SSC checks new security scans to determine whether filed bugs are to remain open, or can be closed.

TEST CONNECTION

**Supported Versions**

5.0

Bugzilla URL Prefix\*

Bug state management

**Username :**

**Password :**

CLOSE APPLY

The **Bug Tracker** tab displays additional fields, which vary, depending on the bug tracker application you select.

7. Complete the required fields, and then click **TEST CONNECTION**.

The TEST BUG TRACKER PLUGIN CONFIGURATION dialog box opens.

8. 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.

9. 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.

10. (Optional) To enable bug state management, select the **Enable bug state management** check box.

11. 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. .

12. Click **OK**.

13. Click **CLOSE**.

#### See Also

["About Bug Tracker Integration" on page 119](#)

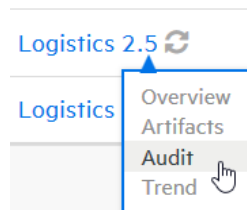
["Managing Bug Tracker Plugins" on page 120](#)

["Authoring Bug Tracker Plugins" on page 320](#)

## Submitting a Bug for One or More 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 200](#)), you can submit bugs that cover one or multiple issues.


To submit a single bug that covers multiple issues:



1. From the Fortify Software Security Center DASHBOARD, move your cursor to the application version for which you want to submit bugs, and then select **Audit** from the shortcut menu.

The AUDIT page opens.

2. To display the issues of interest, use the Fortify Priority risk links, the **Group by** list, and **Filter by** lists. (See ["Viewing Issues Based on Fortify Priority" on page 255](#) and ["Filtering Issues for Display on the OVERVIEW and AUDIT Pages" on page 257](#).)
3. After you review the issues, select the check boxes for one or more issues tagged as exploitable and for which you want to submit in a single bug.
4. Click **file issues** .

**Note:** If, after you select one or more check boxes, **file issues**  is not enabled, 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 200](#).)

The File Issues dialog box opens.

Issue Name	Primary Location
Cross-Site Scripting: Reflected	Challenge.jsp : 59
Privacy Violation: Social Security Number	AccountSummary.java : 28

5. Provide your credentials for your bug tracking system, 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.  
After Fortify Software Security Center connects to the bug tracking server, the File Issues dialog box displays the required bug tracker plugin fields.
6. Provide the required information, and then click **Submit**.

**See Also**

["Viewing Bugs Submitted for Issues" on page 265](#)

**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 or 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 200](#).

## 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.

After you assign an application version a different template, Fortify Software Security Center calculates metrics based on the new issue template. Any in-progress audits are saved and then restarted with the new issue template.

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.

The AUDIT page for the selected version opens.

3. On the application version toolbar, click **PROFILE**.

The APPLICATION PROFILE <application\_version> dialog box opens.

4. Click **APPLICATION SETTINGS**.

The screenshot shows a dialog box titled "APPLICATION PROFILE - BILL PAYMENT PROCESSOR | 1.1". At the top, there are navigation tabs: "ADVANCED OPTIONS", "CUSTOM TAGS", "PROCESSING RULES", "BUG TRACKER", and "APPLICATION SETTINGS" (which is selected and underlined). The main content area is split into two columns. The left column is titled "Application Settings" and contains three sections: "Application name" (Bill Payment Processor), "Application description" (Bill payments processing and support interfaces), and "Owner (Legacy UI)" (admin). The right column is titled "Version Settings" and contains a section for "Version Name: 1.1" with the description "Bill payment processing and support interfaces." and an edit icon. Below this are "DELETE" and "DEACTIVATE" buttons. At the bottom right of the dialog box is a "CLOSE" button.

5. Under **Version Settings**, click the edit icon .

The EDIT VERSION wizard opens.

**Caution!** Changing the template can alter the metrics calculated for the application version. Existing metrics will not be recalculated.

6. Advance to **Step 3. CHOOSE TEMPLATES** (use **NEXT**).

IssueTemplate_0314015152519	<input type="checkbox"/>
PCI v3.1 Basic Issue Template	<input checked="" type="checkbox"/>
Prioritized High Risk Issue Template	<input type="checkbox"/>
Prioritized Low Risk 3rd Party Issue Template	<input type="checkbox"/>
Prioritized Low Risk Issue Template	<input type="checkbox"/>

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 **NEXT**, and then click **FINISH**.

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 configure 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.

The AUDIT page for the application version opens.

2. On the application version toolbar, click **PROFILE**.

The APPLICATION PROFILE - <Application\_Version> dialog box opens.

3. Select the **PROCESSING RULES** tab, and then review the listed processing rules.

4. Select or clear the check boxes for the processing rule you want to apply to the application version. The processing 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 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 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). In reality, both instance IDs identify the same issue. When enabled, this rule migrates old instance IDs to the corresponding new

Rule	Description
	instance IDs even if the Fortify Static Code Analyzer version (or Rulepack) versions are the same. (Also see <a href="#">"Automatically perform Instance ID migration on upload" below.</a> )
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 a Rulepack can change an instance ID from an instance ID created in a previous scan by an older version of Fortify Static Code Analyzer or a Rulepack. In reality, 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 as a troubleshooting measure for customer support. (Also see <a href="#">"Perform Force Instance ID migration on upload" on the previous page</a> )
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



Rule	Description
	<p>than the one already used in the application. If it detects newer versions, it flags the upload for management approval.</p>
<p>Ignore SCA scans performed in Quick Scan mode</p>	<p>Blocks the processing of Fortify Static Code Analyzer scans done in Quick Scan Mode, which searches for high-confidence, high-severity issues.</p>
<p>Require approval if the Rulepacks used in the scan do not match the Rulepacks used in the previous scan</p>	<p>Fortify Software Security Center checks to determine whether you have added or removed a 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.</p>
<p>Require approval if Fortify SCA or Fortify WebInspect Agent scan does not have valid certification</p>	<p>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.</p>
<p>Require approval if result has analysis warnings</p>	<p>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.</p> <p><b>Note:</b> This rule applies only to the first upload of a given results file, and does not apply to subsequent uploads of the</p>

Rule	Description
	<p>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.</p>
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	<p>If an earlier scan artifact requires approval, and was not approved, this rule blocks the user from approving the current scan artifact.</p> <p>If this processing rule is <i>not</i> selected, then when a user approves the current FPR, all previous FPRs are automatically approved.</p>

Fortify Software Security Center prompts you to confirm that you want to save the settings for analysis result processing rules.

5. Click **APPLY**.

**See Also**

["Uploading Scan Artifacts" on page 234](#)

## 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 74.](#))
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 74.](#)) 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 74.](#))

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 74](#)

## Custom Tags

To audit code in Fortify Software Security Center, the security team examines analysis results (FPR) 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 a Fortify Software Security Center application version. For example, you could create a custom tag used track the sign-off process for an issue. After a developer audits his own issues, a security expert can review those same 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:

<a href="#">Adding Custom Tags to the System</a>	212
<a href="#">Modifying Custom Tag Attributes</a>	214
<a href="#">Globally Hiding Custom Tags</a>	215
<a href="#">Deleting Custom Tags</a>	215
<a href="#">Adding Custom Tag Values</a>	216
<a href="#">Editing Custom Tags</a>	216
<a href="#">Deleting Custom Tag Values</a>	217
<a href="#">Associating Custom Tags with Issue Templates</a>	217
<a href="#">Removing Custom Tags from Issue Templates</a>	218
<a href="#">Assigning Custom Tags to Application Versions</a>	219
<a href="#">Disassociating a Custom Tag from an Application Version</a>	220
<a href="#">Managing Custom Tags Through Issue Templates</a>	221
<a href="#">Managing Custom Tags Through an Issue Template in an FPR File</a>	221

## 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 257](#).

To add a custom tag:

1. On the Fortify header, click **ADMINISTRATION**.
2. In the left panel of the ADMINISTRATION view, select **Templates**, and then select **Custom Tags**.
3. On the Custom Tags page header, click **NEW**.  
The Create New Custom Tag dialog box opens.
4. In the **Name** box, type a name for the new tag.

**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 following tag types:
  - Date—Accepts a calendar date in the format yyyy-mm-dd
  - Decimal—Accepts a number with a precision of up to 18 (up to 9 decimal places)
  - List—Accepts a selection from the list of values that you specify for the tag
  - Text—Accepts a string with up to 500 characters (HTML/XML tags and newlines are not allowed)
7. Select one or both 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.
  - To prevent the display of the tag in the ASSIGN dialog box or in Audit Workbench, select the **Hidden** check 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.  
A list-type custom tag can be *extensible*, which means that auditors can add values to it as they audit issues.
9. If you are adding a list-type tag, and you want to enable users to add new values to the tag during audits, select the **Extensible** check box.
10. To specify a value for the new tag:
  - a. Click **+ ADD VALUE**.  
The ADD VALUE dialog box opens.
  - b. In the **Name** box, type a value.  
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 or in Audit Workbench, select the **Hidden** check box.
  - e. Click **APPLY**.

- f. Repeat the previous step until you have defined all of the values you need for the new custom 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 becomes "Not Set."

11. From the **Default Value** list, select the default value for this tag.

If your new custom tag is a list-type tag, then you can designate it as the *primary tag* for auditing an application version. If your Fortify Software Security Center instance is integrated with Fortify Scan Analytics and Audit Assistant is enabled, it is important that you provide Audit Assistant with information that it can use to distinguish between tag values that signify true issues and those that signify non issues (true positives versus "noisy" or a false positives). You do this in the **Audit Assistant Guidance** section, where the **True Issue** list initially contains all tag values.

**Tip:** Although you can provide the information for Audit Assistant later by editing the custom tag, you might want to provide it now, before the tag is assigned to an application version and selected as the primary tag.

Under **Audit Assistant Guidance**, the **Non-Issue** list contains all of the values you added for the tag.

12. In the **Non-Issue** list, select the tag values that, if selected, indicate a true vulnerability (use the **Ctrl** and **Shift** keys to select multiple values) and use the right-pointing arrow to move them to the **True Issue** list.
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 219](#).

### See Also

["Custom Tags" on page 211](#)

["Editing Custom Tags" on page 216](#)

["Globally Hiding Custom Tags " on the next page](#)

["Associating Custom Tags with Issue Templates" on page 217](#)

["Managing Custom Tags Through Issue Templates" on page 221](#)

["Managing Custom Tags Through an Issue Template in an FPR File" on page 221](#)

["Deleting Custom Tags" on the next page](#)

### Modifying Custom Tag Attributes

To modify the attributes of a custom tag:

1. From the left panel 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 Tags to the System" on page 212](#)

["Adding Custom Tag Values" on the next page](#)

## Globally Hiding Custom Tags

To globally hide a custom tag:

1. From the left panel 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. Under the **Description** box, select the **Hidden** check box.
5. Click **SAVE**.

The custom tag no longer appears on the AUDIT page or in 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:

- The tag is currently set as the primary tag.
- The tag is currently associated with an application version or issue template.
- If an issue has been audited using the custom tag.

You can never delete the Analysis tag.

To delete custom tags:

1. From the left panel 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 211](#)

## 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 panel, 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 VALUE**.
6. In the ADD VALUE dialog box, type a name and, optionally, a description for the new value.
7. To make the value unavailable in the AUDIT page and in Fortify Audit Workbench, select the **Hidden** check box.
8. Click **APPLY**.
9. On the Custom Tags page, click **SAVE**.

**See Also**

["Adding Custom Tags to the System" on page 212](#)

["Assigning Custom Tags to Application Versions" on page 219](#)

["Editing Custom Tags" below](#)

["Deleting Custom Tag Values" on the next page](#)

## 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 panel 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 212](#).

#### See Also

["Deleting Custom Tag Values" below](#)


["Assigning Custom Tags to Application Versions" on page 219](#)

## 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 panel 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

["Adding Custom Tags to the System" on page 212](#)

["Adding Custom Tag Values" on the previous page](#)

["Editing Custom Tags" on the previous page](#)

## 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**.  
The table on the right lists all of the issue templates in the system.
2. In the left panel, select **Templates**, and then select **Issue**.
3. Click the row that displays the issue template 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**.  
The Add Custom Tag dialog box opens.
6. Select the check box for the custom tag to associate with the issue template, and then click **+ADD**.
7. Click **CLOSE**.
8. Click **SAVE**.

#### **See Also**

["Disassociating a Custom Tag from an Application Version" on page 220](#)

## **Removing Custom Tags from Issue Templates**

To remove a custom tag from an issue template:

1. From the left panel 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 associated with the template.

PCI v3.1 Basic Issue Template

The PCI DSS v3.1 standard gives specific guidance on what types of software defects should be removed from software before deployment. To better aid with remediation, this view displays those issues that are immediately related to the PCI standard. To enhance the auditing of the application, one should group the issues by "PCI 3.1" for better clarity.

Name: PCI v3.1 Basic Issue Template

Template: ProjectTemplate.xml

Description: The PCI DSS v3.1 standard gives specific guidance on what types of software defects should be removed from software before deployment. To better aid with remediation, this view displays those issues that are immediately related to the PCI standard. To enhance the auditing of the application, one should group the issues by "PCI 3.1" for better clarity.

Select Primary Tag: Analysis

Name	Description	Hidden	Extensible	Restricted
Analysis	The analysis tag must be set for an issue to be counted as 'Audited.' This is encouraged to be the final action performed by an auditor.			
Recurrence	Indicates that an issue was uncovered before in the current, or previous application version.			

Buttons: SET AS DEFAULT, DELETE, DOWNLOAD TEMPLATE, EDIT


3. At the bottom of the expanded row, click **EDIT**.

CUSTOM TAGS

+ ADD CUSTOM TAG

Name	Description	Hidden	Extensible	Restricted
Analysis	The analysis tag must be set for an issue to be counted as 'Audited.' This is encouraged to be the final action performed by an auditor.			
Recurrence	Indicates that an issue was uncovered before in the current, or previous application version.			

Buttons: CANCEL, SAVE

4. In the last column, click the remove icon  for the custom tag that you want to remove from the template.
5. Click **SAVE**.

### See Also

["Custom Tags" on page 211](#)

## 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, select the version name for the application version you plan to audit.  
Fortify Software Security Center opens the AUDIT page for the selected version.
2. In the application version toolbar, click **PROFILE**.
3. In the Application Profile dialog box, click **CUSTOM TAGS**.
4. Click **ASSIGN/ REMOVE**.

The ASSIGN CUSTOM TAGS dialog box opens and lists the tags available for auditing issues for this application version.

5. Select the check box for the custom tag you want to assign to the application version, and then click **DONE**.

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 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**.

The SELECT PRIMARY TAG dialog box opens.

- b. From the **Select Primary Tag** list, 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 212](#). For information about how to edit a custom tag, see ["Editing Custom Tags" on page 216](#).

- 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

["Adding Custom Tags to the System" on page 212](#)

["Adding Custom Tag Values" on page 216](#)

["Auditing Issues" on page 249](#)

["Editing Custom Tags" on page 216](#)

## 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.

- The OVERVIEW page opens.
3. On the application version toolbar, click **PROFILE**.  
The APPLICATION PROFILE window opens.
  4. Click the **CUSTOM TAGS** tab.
  5. Click **ASSIGN/REMOVE**.  
The ASSIGN CUSTOM TAGS dialog box opens.
  6. Clear the check box for the custom tag that you want to remove, and then click **DONE**.

#### See Also

["Adding Custom Tags to the System" on page 212](#)

["Assigning Custom Tags to Application Versions" on page 219](#)

### 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 panel 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 the next page](#)

## Deactivating Application Versions

Deactivating an application version hides that version on 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, select the application version you want to deactivate.  
The AUDIT page for the selected version opens.
2. Click **PROFILE**.
3. In the APPLICATION PROFILE dialog box, click **APPLICATION SETTINGS**.
4. In the **Version Settings** panel, 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

["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:

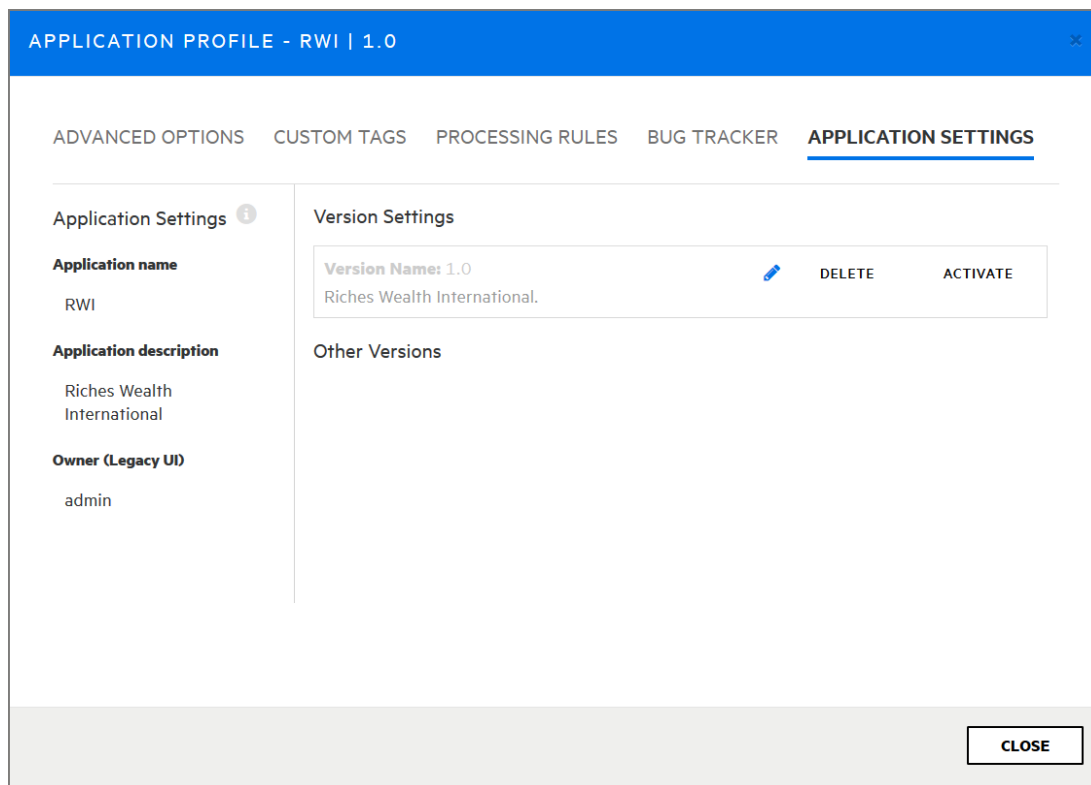
- Create a new version of the deactivated application, and then follow the procedure described below.

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.  
The AUDIT page for the selected application version opens.
4. On the application version toolbar, click **PROFILE**.

The APPLICATION PROFILE dialog box opens.

5. Click **APPLICATION SETTINGS**.



6. In the **Other Versions** section, next to the inactive version you want to reactivate, 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 the previous page](#)

**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** panel, 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 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 .....	225
Creating Variables .....	226
Variable Syntax .....	226
Performance Indicators .....	227
Creating Performance Indicators .....	227
Alert Definitions .....	228
Creating Alerts .....	229
Editing Alerts .....	231
Deleting Alerts .....	231
Viewing and Marking Alerts .....	232

## 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 panel on the left, under **Metrics & Tracking**, select **Variables**.
3. In the **Variables** toolbar, click **NEW**.

The CREATE NEW VARIABLE dialog box opens.

4. 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, see <a href="#">"Variable Syntax" below.</a> )
Folder	From this list, select a folder from the default filter set to associate with the variable.  The <b>Folder</b> 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. Click **VALIDATE**.

Fortify Software Security Center displays the variable validation result.

6. 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	<p>A comma-separated pair of numbers used to specify the beginning and end of a range of numbers.</p> <p>Use a left or right bracket (“[ ]”) to specify that the range includes the adjoining number.</p> <p>Use a begin or end parenthesis (“( )”) to specify that the range excludes (is greater than or less than) the adjoining number.</p>	<p>(2,4]</p> <p>Indicates a range of greater than two, and less than or equal to four</p>
! (not equal)	<p>Negate a modifier with an exclamation character (!).</p>	<p>!file:Main.java</p> <p>Returns all issues that are not in Main.java.</p>

## 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" below](#).

### 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 panel on the left, under **Metrics & Tracking**, select **Performance Indicators**.  
The table to the right lists existing performance indicators.
3. Click **NEW**.  
The CREATE NEW PERFORMANCE INDICATOR dialog box opens.
4. 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** on 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" on the next page](#)

### See Also

["Enabling and Disabling Receipt of Email Alerts" on page 156](#)

["Configuring Email Alert Notification Settings" on page 85](#)

["Deleting Alerts" on page 231](#)

## 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 panel 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**.  
The CREATE NEW ALERT dialog box opens.
4. In the **Name** box, type a name for the alert.
5. To create the alert without enabling it, clear the **Enabled Alert** check box. To enable this alert, leave the check box selected.
6. (Optional) In the **Description** box, type text that describes what the alert is for.
7. Next to **Type**, select the type of alert you want to create.

**Note:** Only administrators can create *scheduled* alerts.

8. Provide the information for the alert type you selected, as shown in one of the following tables.

<b>Performance indicator</b>
<ol style="list-style-type: none"><li>a. From the <b>Alert when</b> list, select a performance indicator.</li><li>b. From the list of operators, select an operator.</li><li>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 <b>Alert when</b>. For example, an alert with the trigger criterion set to Critical Exposure Issues &lt; 50 is triggered only once, even if many new critical issues are uncovered in subsequent scans.</li><li>d. To have Fortify Software Security Center reset your alert after each new artifact upload, select the <b>Reset after triggering</b> check box.</li></ol>
<b>Variable</b>
<ol style="list-style-type: none"><li>a. From the <b>Alert when</b> list, select a variable.</li><li>b. From the list of operators, select the appropriate operator.</li><li>c. Type a numeric value. The type of variable you selected determines whether the value represents an integer or a percentage.</li></ol>

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.

9. 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. In the **Apply to** section, click **+ ADD**.  
The SELECT APPLICATION VERSION dialog box opens.
  - b. In the **Application** list, select an application for which you want to use the alert.
  - c. To include inactive versions of the application in the **Versions** list, select the **Show inactive versions** check box.
  - d. To use the alert for all application versions, select the **Versions** check box. Otherwise, in the **Versions** list, select the check boxes for the versions for which you want to use the alert.
  - e. Click **DONE**.
10. In the **Recipients** section, select one of the following recipient preferences:

**Note:** Regardless of the option you select, you will receive the notification.

- To have the notification sent only to you, select **Me Only**.
- To have the notification sent to all Fortify Software Security Center users who have access to the application versions you specified (in the Select Application Version dialog box), select **Version assignees**.
- If you are creating a scheduled alert, and you want to have the notification sent to all Fortify Software Security Center users, select **All system users**.

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 a recipient.

Fortify Software Security Center displays the details for your new alert.

## 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 panel 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 panel 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

["Alert Definitions" on page 228](#)

["Creating Alerts" on page 229](#)

## 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 panel 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 panel, 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 panel, click **Show all alert notifications**.

# Chapter 14: About Working with Scan Artifacts

## Uploading Scan Artifacts

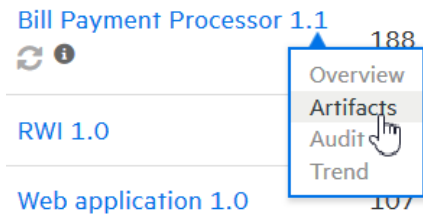
The following procedure describes how to upload your scan artifacts to the Fortify Software Security Center database. For information about how to submit training metadata to Fortify Audit Assistant, see ["Submitting Training Data to Audit Assistant" on page 274](#).

**Important!** The files you upload to Fortify Software Security Center must not exceed 2GB.

**Note:** If a scan artifact requires approval based on analysis result processing rules, it must be approved before it can be processed. For information, see ["Approving Scan Artifacts" on page 238](#).

To upload a scan artifact to the Fortify Software Security Center database:

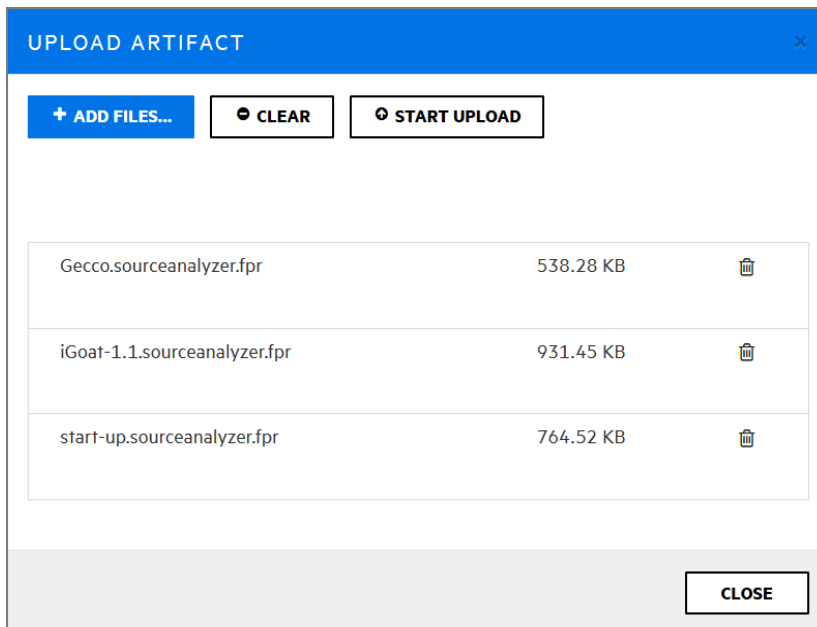
1. On the Dashboard or Applications view, move your cursor to the application version for which you want to upload an artifact, and then select **Artifacts** from the shortcut menu.




2. The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the application version.



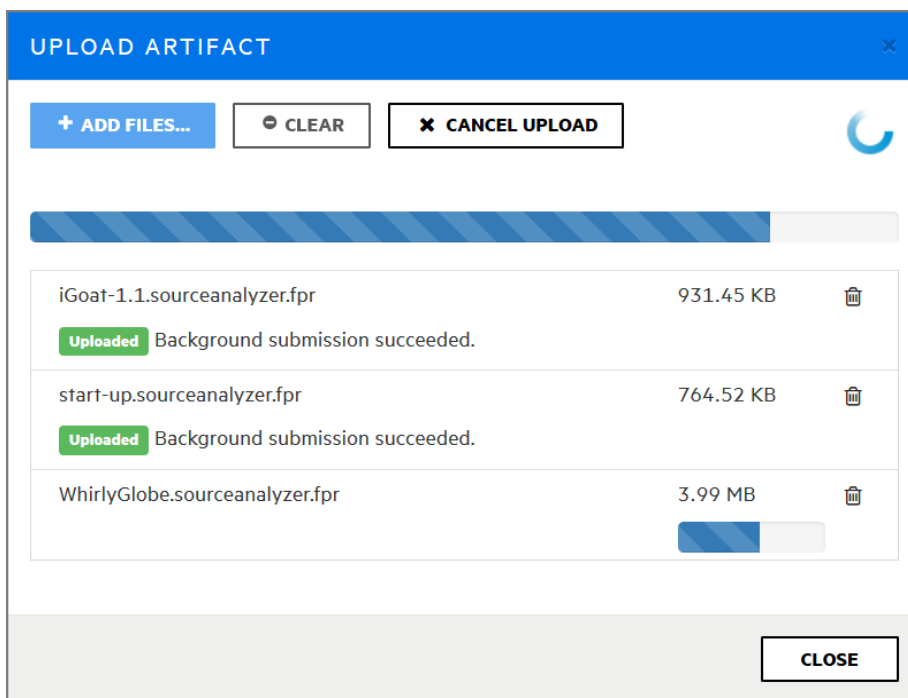
3. Click **ARTIFACT**.  
The UPLOAD ARTIFACT dialog box opens.
4. Click **+ ADD FILES**.
5. Navigate to and select one or more (up to five) artifact files to upload.



The UPLOAD ARTIFACT dialog box lists the selected files.

6. To remove a file from the list, click the trash icon  for that file.
7. To remove all of the listed files, click **CLEAR**.
8. After the list shows all of the files that you want to upload, click **START UPLOAD**.

The dialog box displays a green progress bar as each file is uploaded.



9. After your files are successfully uploaded, click **CLOSE**.

## 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

["Using an Application Identifier to Upload FPR Files" on page 314](#)

["Using an Application Name and Version to Upload FPR Files" on page 315](#)

["Downloading Scan Artifacts" on the next page](#)

["Deleting Artifacts" on page 244](#)

["Setting Analysis Results Processing Rules for Application Versions" on page 206](#)

["About Auditing" on page 247](#)

## Viewing Scan Errors and Warnings

If errors occurred during a code scan, this information is included in the uploaded scan artifact and made available for viewing through the SCAN ERRORS or SCAN WARNINGS window.

To view scan errors:

1. From the Dashboard, hover your cursor over the application version of interest, and then select **Artifacts** from the shortcut menu.

The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the application version. If errors occurred during a scan, Fortify Software Security Center displays a circled number next to the scan artifact name to indicate the number of errors encountered when the scan artifact was first uploaded. (Subsequent uploads of a given scan artifact do not affect the number displayed.)

ARTIFACT HISTORY						
[UPLOAD ARTIFACT] [DOWNLOAD APPLICATION FILE] [DOWNLOAD APPLICATION FILE WITH SOURCES] [REFRESH TABLE]						
Upload Date	Status	Uploaded By	Type	Audits	Scan Artifact	
03/07/2018 1:51:55 AM	Processing Complete	susan	SCA	[icon]	webgoat_5.fpr	
03/07/2018 1:51:34 AM	Processing Complete	susan	SCA	[icon]	webgoat_4.fpr	
03/07/2018 1:51:18 AM	Processing Complete	susan	SCA	[icon]	webgoat_3.fpr	
03/07/2018 1:51:05 AM	Processing Complete	lisa	SCA	[icon]	webgoat_2.fpr	1
03/07/2018 1:50:52 AM	Processing Complete	susan	SCA	[icon]	webgoat_1.fpr	1

2. To open the SCAN WARNINGS or SCAN ERRORS window and view detailed information about the errors encountered, click the number in the red circle.

### See Also

["Purging Scan Artifacts" on page 243](#)

## 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. On the **APPLICATIONS** page, click the link for the application 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.

4. Do one of the following:
  - To download the current merged application scan results in FPR format, click **DOWNLOAD APPLICATION FILE**.
  - To download the current merged application scan results in FPR format with sources, click **DOWNLOAD APPLICATION FILE WITH SOURCES**.
5. In the Opening *<file\_name.fpr>* dialog box, do one of the following:
  - Note the file name, leave **Save file** selected, and then click **OK**.
  - Select **Open with**, browse to the program with which to open the file, and then click **OK**. (If you do not select a program, Fortify Software Security Center tries to open the file in Audit Workbench, which is the default program).

### Downloading Individual Scan Results

To download to results for a given processed scan:

1. On the Fortify header, click **APPLICATIONS**.
2. On the **APPLICATIONS** page, click the link for the application version you are interested in.
3. On the application version toolbar, click **ARTIFACTS**.

The **ARTIFACT HISTORY** table lists all artifacts uploaded for the application version.

4. Click the row that displays the artifact you want to download.  
The row expands to reveal detailed information about the scan.
5. Do one of the following:
  - To download the scan results for the artifact in FPR format, click **DOWNLOAD**.
  - To download the scan results with sources in FPR format, click **DOWNLOAD WITH SOURCES**.
6. Save the file, and then open the saved file from Audit Workbench or other application.

### See Also

["Uploading Scan Artifacts" on page 234](#)

["Deleting Artifacts" on page 244](#)

["Viewing Scan Errors and Warnings" on page 236](#)

## Approving Scan Artifacts

If a scan artifact requires approval based on analysis result processing rules, it must be approved before you can upload it.

To approve a scan artifact from the Fortify Software Security Center database:

1. From the `<application_version>` OVERVIEW page, click **ARTIFACTS**.  
The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the application version.
2. Click the row that displays the artifact that requires approval based on analysis result processing rules.  
The table expands to show the details for the selected artifact.
3. Below the artifact details, click **APPROVE**.  
Fortify Software Security Center prompts you to confirm that you want to approve the artifact.
4. Click **OK**.

### See Also

["Setting Analysis Results Processing Rules for Application Versions" on page 206](#)

## 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.

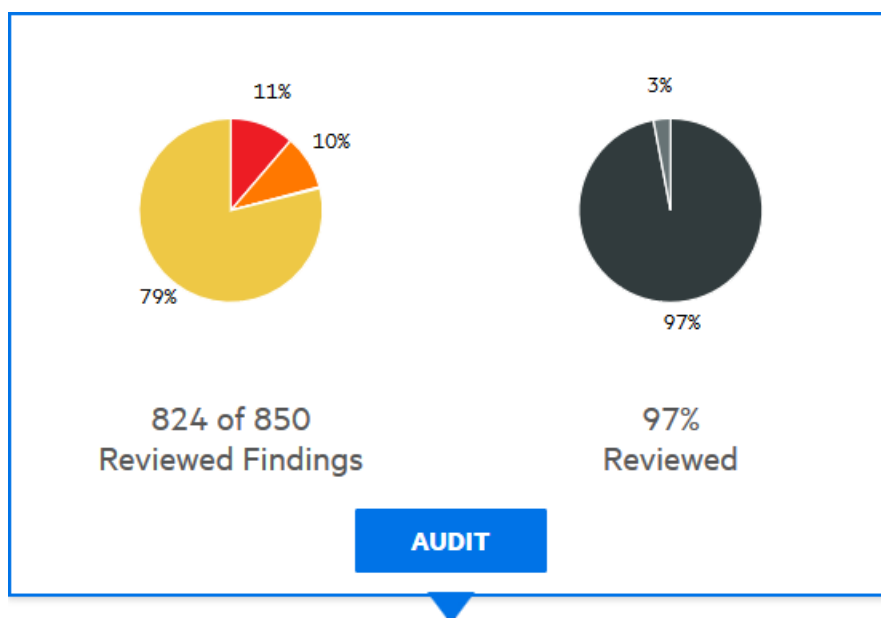
Together, the portlets and table enable you to see how quickly issues are being reviewed and remediated.

### 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.

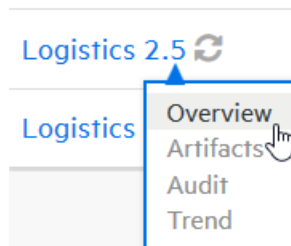


Fortify Software Security Center shows the summary findings for the version. In the example shown here, the pie chart of the left shows the security ratings for the 97% of findings (824 of 850) that have been audited to date for this application version. The chart on the right shows the percentage of findings audited (97) and the percentage of the total that has yet to be audited (3).

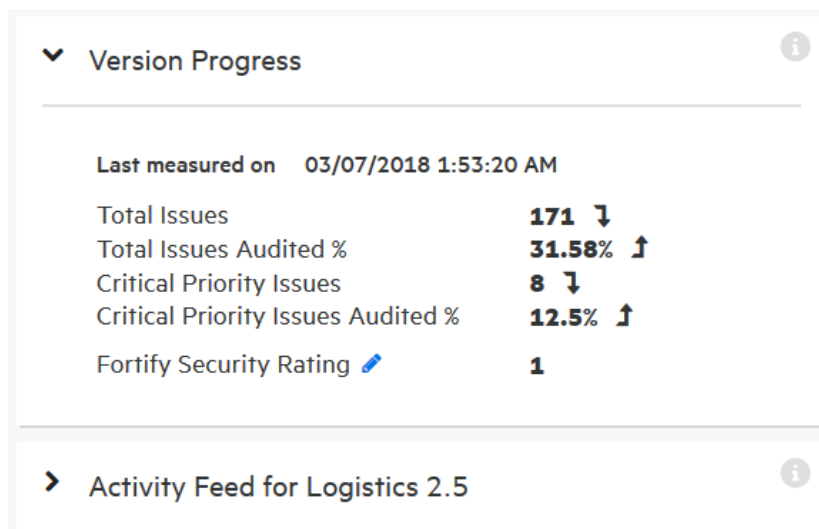
**Note:** To go from here to the AUDIT page for the application version, click **AUDIT**.

## Viewing Summary Metrics on the Overview Page


To view high-level summary results for an application version from the Overview page:



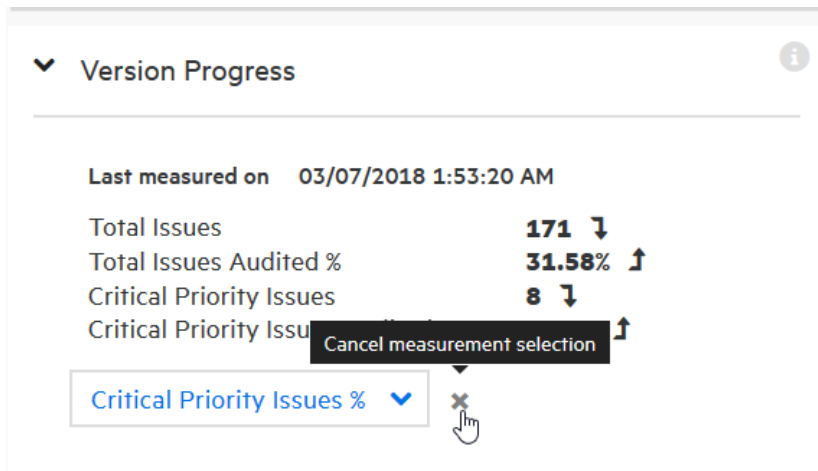
1. On the Fortify Dashboard, hover your cursor over the link for the version you are interested in, and then select **Overview** from the shortcut menu.
2. On the **Overview** page, if the panel on the right is collapsed, expand it.



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.





4. To cancel your selection and leave edit mode, click the X next to the list.

**See Also**

["Auditing Issues" on page 249](#)

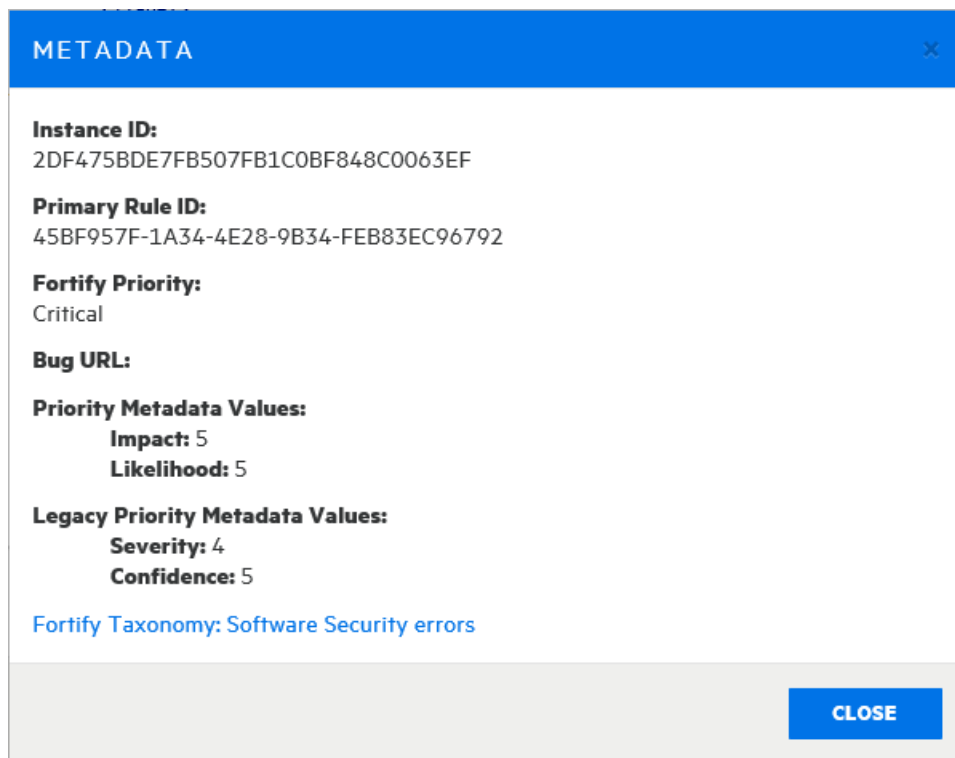
## Viewing Issue Metadata

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.

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 DSS 3.2, 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 panel, under **Metrics & Tracking**, select **Rulepacks**.
3. In the upper right corner of the Rulepacks page, click **IMPORT**.

The IMPORT RULEPACK dialog box opens.

4. 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.

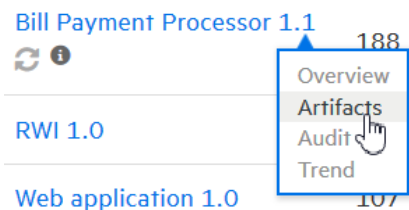
## Purging Scan Artifacts

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://softwaresupport.softwaregrp.com>) first to determine whether an artifact purge will affect them.

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.

Upload Date	Status	Uploaded By	Type	Audits	Scan Artifact
08/01/2018 4:27:24 PM	Processing Complete	susan	SCA		webgoat_5.fpr

<b>Upload IP</b> Not Available	<b>File Name</b> webgoat_5.fpr	
<b>Uploaded By</b> susan	<b>File Size</b> 2.0 MB	
<b>Analysis Type</b> SCA	<b>Analysis Date</b> 06/23/2009 9:12:12 AM	<b>Certification</b> VALID
<b>Engine Version</b> 5.7.0.0025	<b>Scan Elapsed Time</b> 02:25	<b>Hostname</b> mobile004.mycingular.net
<b>Number Of Files</b> 188	<b>Total Lines of Code</b> 32613	<b>Executable Lines</b> 9892

Buttons: DOWNLOAD, DOWNLOAD WITH SOURCES, APPROVE, **PURGE**, DELETE

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**.

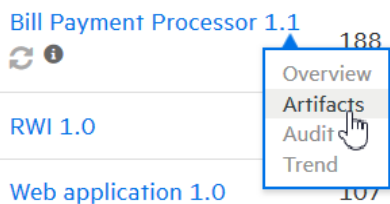
**See Also**

["Deleting Artifacts" below](#)

## Deleting Artifacts

Deleting an artifact removes all traces of the artifact. Use this option if you upload an artifact by mistake.

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 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 scan artifact you want to delete.  
The table expands to show the details for the selected artifact.

ARTIFACT HISTORY

ARTIFACT APPLICATION FILE APPLICATION & SOURCES REFRESH

Upload Date	Status	Uploaded By	Type	Audits	Scan Artifact
08/01/2018 4:27:24 PM	Processing Complete	susan	SCA		webgoat_5.fpr
08/01/2018 4:27:13 PM	Processing Complete	susan	SCA		webgoat_4.fpr

**Upload IP** Not Available **File Name** webgoat\_4.fpr  
**Uploaded By** susan **File Size** 2.0 MB  
**Analysis Type** SCA **Analysis Date** 05/14/2009 6:42:12 PM **Certification** VALID  
**Engine Version** 5.7.0.0025 **Scan Elapsed Time** 02:25 **Hostname** mobile004.mycingular.net  
**Number Of Files** 188 **Total Lines of Code** 32613 **Executable Lines** 9892

DOWNLOAD DOWNLOAD WITH SOURCES APPROVE PURGE **DELETE**

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 243](#)

## Chapter 15: Collaborative Auditing

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 177.)

Topics covered in this section:

About Auditing .....	247
About Current Issues State .....	247
Setting the Strategy for Resolving Issue Audit Conflicts .....	248
Auditing Issues .....	249
Accessing the AUDIT Page from the Issue Stats Page of the Dashboard .....	255
Accessing the AUDIT Page from the Applications View .....	255
Viewing Issues Based on Fortify Priority .....	255
Filtering Issues for Display on the OVERVIEW and AUDIT Pages .....	257
Viewing Issues Assigned to You .....	259
Searching Issues .....	259
About Suppressed, Removed, and Hidden Issues .....	264
Changing Displayed Issues Using Filter Sets .....	265
Viewing Bugs Submitted for Issues .....	265
About Audit Assistant .....	265
Audit Assistant Workflow .....	266
About Classifiers and Prediction Policies .....	267
Defining Classifiers .....	268
Defining Prediction Policies .....	271
Enabling Metadata Sharing .....	273
Submitting Training Data to Audit Assistant .....	274
Reviewing Audit Assistant Results .....	274
Setting Issue Viewing Preferences .....	276

Viewing Suppressed Issues .....	276
Viewing Removed Issues .....	276
Viewing Hidden Issues .....	277
Searching Globally in Fortify Software Security Center .....	277
Fortify Software Security Center and WebInspect Integration .....	279
Viewing Fortify WebInspect Scan Results in Fortify Software Security Center .....	279
WebInspect Audit Data .....	282
False Positives .....	282
Submitting Dynamic Scan Requests to Fortify WebInspect Enterprise .....	283
Processing Dynamic Scan Requests from Fortify WebInspect Enterprise .....	285
Editing and Cancelling Dynamic Scan Requests .....	286

## About Auditing

When 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.

## 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.

## 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 panel, 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**
- **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

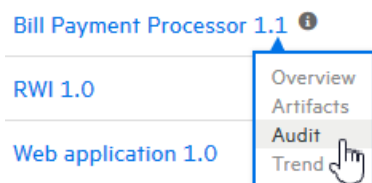
["About Current Issues State" on page 247](#)

## Auditing Issues

To display the issues you want to audit:

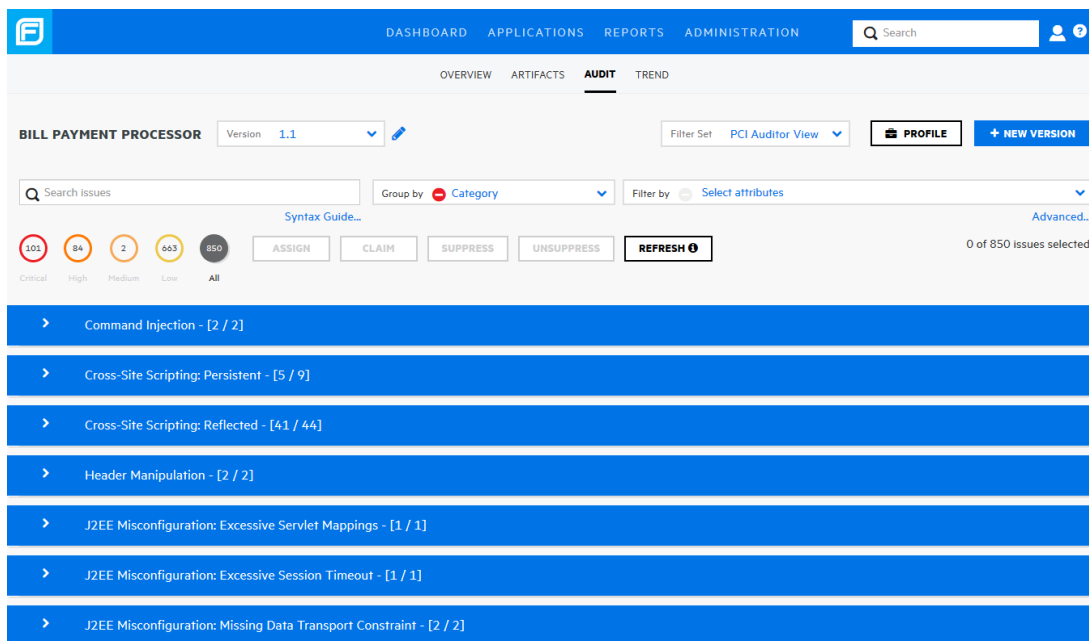
1. Upload scan results for the application version you want to audit. For instructions, see ["Uploading Scan Artifacts" on page 234](#).

Application Version ⇅



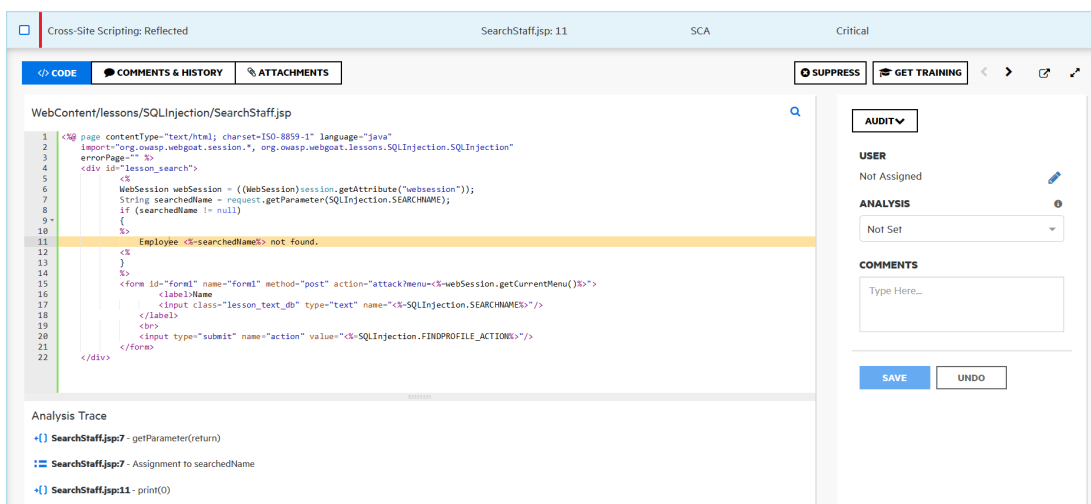
2. Open the AUDIT page for the application version.
3. To selectively display the issues you want to audit, apply filters to the issues list. (See ["Filtering Issues for Display on the OVERVIEW and AUDIT Pages" on page 257](#) and ["Viewing Issues Based on Fortify Priority" on page 255](#).)
4. In the issues table, if you have selected a grouping, expand a group to view the issues it

contains.



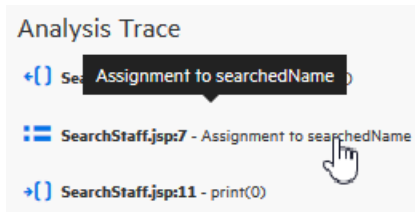
To audit an issue:

1. To expand the issue and view its details, click its row in the table.

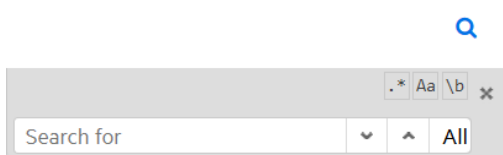


**Note:** This screen capture shows the details for an issue uncovered during a Fortify Static Code Analyzer scan. For information about viewing Fortify WebInspect results, see ["Viewing Fortify WebInspect Scan Results in Fortify Software Security Center" on page 279.](#)

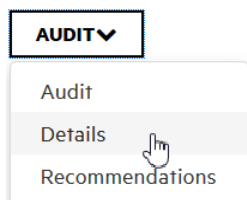
The **CODE** tab displays the area of source associated with the issue.



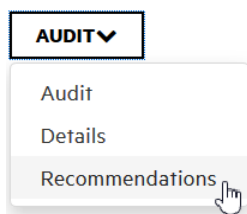
2. To view summary details about a step along the course that tainted data has taken, under **Analysis Trace**, move your cursor to that step.
3. To view code associated with a step, click the step under **Analysis Trace**.  
The corresponding line of code is highlighted on the **CODE** tab.



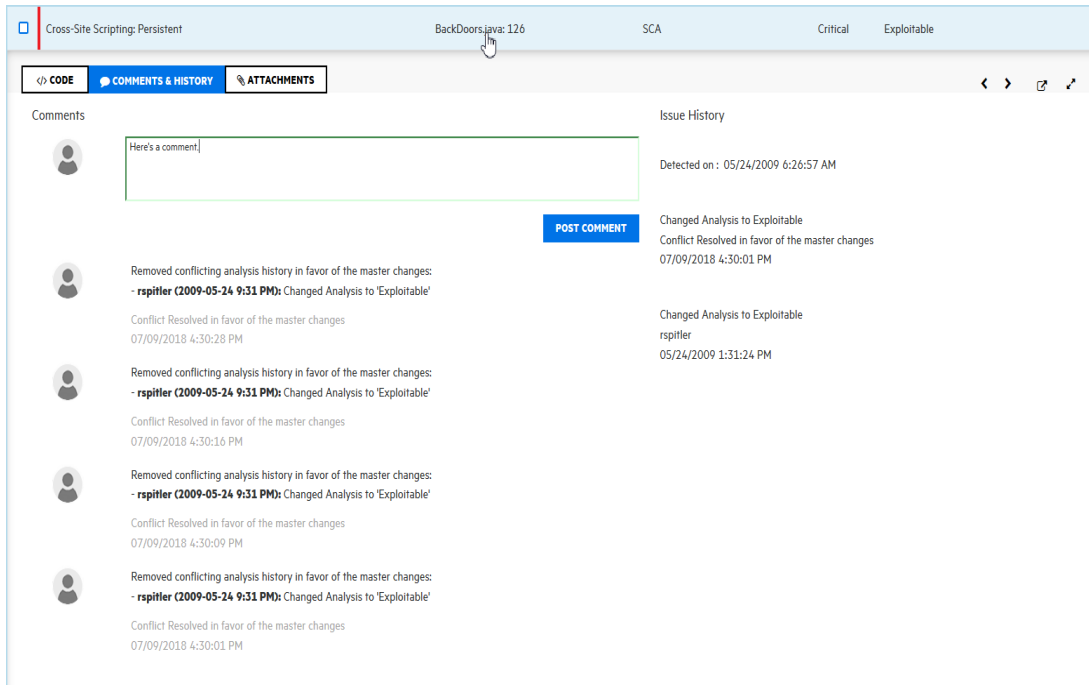
4. To search for a specific string in the code associated with the issue, click the search icon, and then, in the text box displayed, type the character string. Use the next  and previous  icons to move through the search results.



5. To view detailed information about the issue, in the right panel, select the **Details** tab.



6. To view recommended actions you might use to remediate the issue, in the right panel, select the **Recommendations** tab.
7. To view the issue history and any comments related to the issue, near the top of the details section, select the **COMMENTS & HISTORY** tab.



- To add a comment, type it into the **Comments** box, and then click **POST COMMENT**.

**Note:** You can also add a comment from the **CODE** tab. Just type it in the **COMMENTS** box in the right panel.

- (Optional) To exclude an issue from display because you know it is fixed or it is not of immediate concern, click **SUPPRESS**.
- (Optional) If your administrator has configured application security training in Fortify Software Security Center (see "[Configuring Application Security Training](#)" on page 71), 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.

You can attach an image file to the selected issue. The image file must be smaller than 3MB, and in JPG, JPEG, BMP, PNG, or GIF format.

**Note:** After a file is attached to an issue, you can modify only its description.

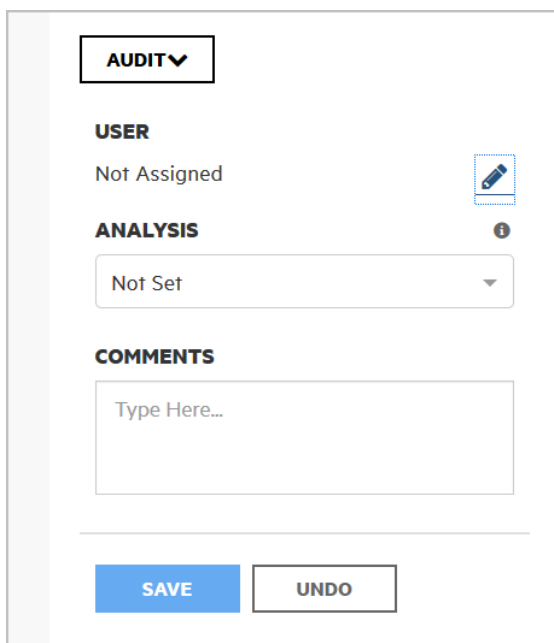
- To attach an image file to the issue:
  - Click **ATTACHMENTS**.
  - Click **CLICK HERE TO ADD**.
  - In the UPLOAD ATTACHMENT dialog box, click **BROWSE**, and then navigate to and select the image file (JPG, JPEG, BMP, PNG, or GIF) to upload.

**Note:** The image file size cannot exceed 3 MB.

- d. (Optional) In the **Description** box, type a description of the image.
- e. Click **SAVE**.

Fortify Software Security Center displays a preview of the image on the right, under **Image Preview**.

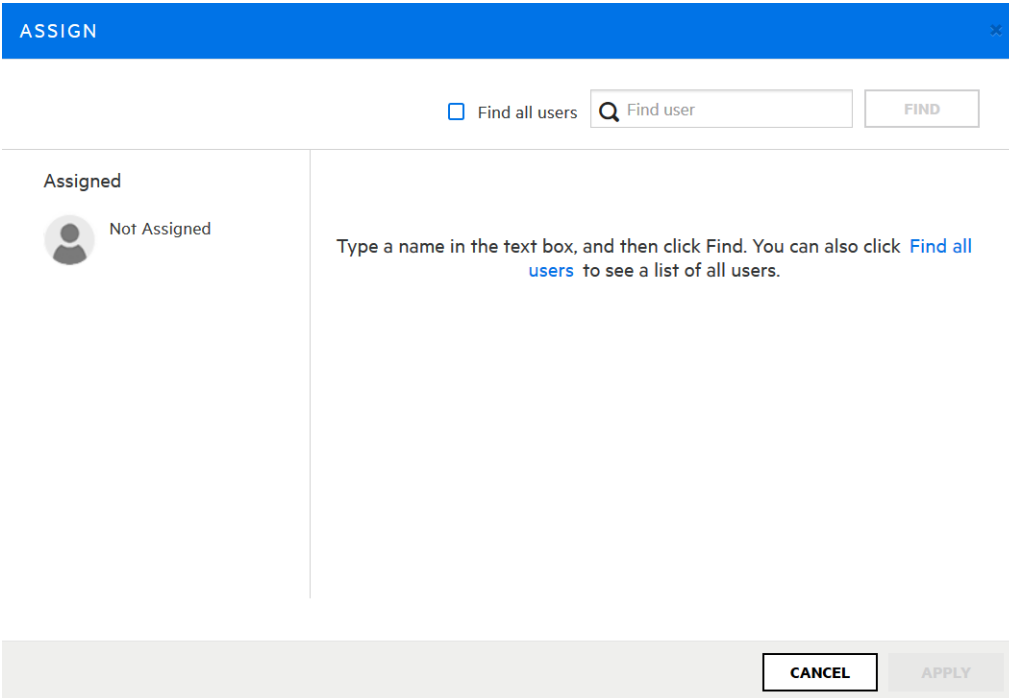
- 12. Click **CODE**, and then, in the right panel, select the **AUDIT** tab.



The screenshot shows a user interface for the 'AUDIT' tab. At the top, there is a dropdown menu labeled 'AUDIT' with a downward arrow. Below this, the 'USER' section displays 'Not Assigned' with a pencil icon to its right. The 'ANALYSIS' section features a dropdown menu currently set to 'Not Set' with a downward arrow and a small information icon to its right. The 'COMMENTS' section contains a text input field with the placeholder text 'Type Here...'. At the bottom of the panel, there are two buttons: a blue 'SAVE' button and a white 'UNDO' button with a black border.

- 13. To assign a user to the issue:

- a. Under **USER**, click the pencil icon .



The ASSIGN dialog box opens.

- b. To locate a user to assign to the issue, in the **Find user** box, type part or all of a user's name, and then click **FIND**. Alternatively, to list all users in the system, click the **Find all users** link.
- c. In the list of returned names, click the name of the user to assign to the issue.
- d. Click **APPLY**.

The **AUDIT** tab now displays the selected user name and avatar (if available).

14. From the **ANALYSIS** list in the right panel, select a value that reflects your assessment of this issue.
15. If additional custom tags are associated with the application version, specify the values for these tags.

**Note:** Make sure that you provide a value for the custom tag that is designated as the primary tag for the application version. Otherwise, Fortify Software Security Center treats the issue as unaudited.

**Note:** If Audit Assistant assessed the issues, the right panel 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 274.

16. (Optional) In the **COMMENTS** box, type a comment about this issue audit.
17. At the bottom of the **AUDIT** tab, click **SAVE**.

**See Also**

["About Auditing" on page 247](#)

## Accessing the AUDIT Page from the Issue Stats Page of the Dashboard

To access the AUDIT page from the Issue Stats page of the Fortify Software Security Center Dashboard:

1. On the Fortify header, click **DASHBOARD**.
2. In the application version summary table, select the link to the application version of interest.

Fortify Software Security Center displays the AUDIT page for the selected application version.

### Next

["Auditing Issues" on page 249](#)

### See Also

["Accessing the AUDIT Page from the Applications View" below](#)

## Accessing the AUDIT Page from the Applications View

To access the AUDIT page from the Applications view:

1. From the Fortify Software Security Center DASHBOARD, click **APPLICATIONS**.
2. In the **Version** column of the **Applications** table, click the application version of interest.

Fortify Software Security Center displays the AUDIT page for the selected application version.

### Next

["Auditing Issues" on page 249](#)

### See Also

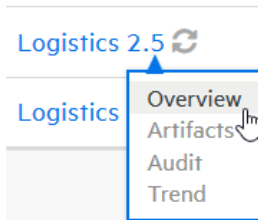
["Accessing the AUDIT Page from the Issue Stats Page of the Dashboard" above](#)

## Viewing Issues Based on Fortify Priority

The OVERVIEW and AUDIT pages include **Critical**, **High**, **Medium**, **Low**, and **All** links, which you can use to view issues based on Fortify priority order (and the potential risk they pose to the enterprise).

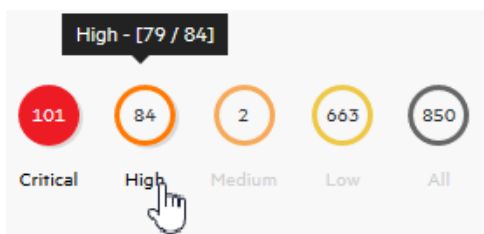
To view issues from the OVERVIEW page based on Fortify Priority:

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 **Critical, High, Medium, Low**, and **All** links display the total number of issues in their respective Fortify priority categories. By default, all issues are shown.

2. To see the number of issues in a priority category that have been reviewed, move your cursor to the risk category.

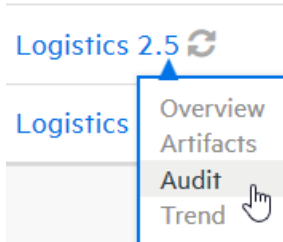


The number of reviewed issues is on the left, and the total number of issues is on the right. In the example shown here, you can see that 79 of 84 total high priority issues were reviewed.

3. To view issue charts on the OVERVIEW page based on a given Fortify priority, select the link.

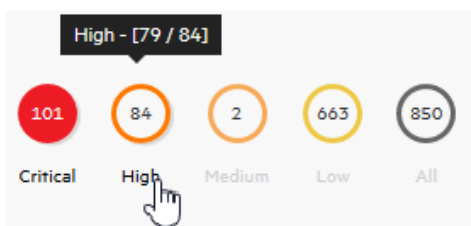
To view issues from the AUDIT page based on Fortify Priority:

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. Under the search field, the **Critical, High, Medium, Low**, and **All** links display the total number of issues in their respective Fortify priority categories. By default, all issues are shown.

2. To see the number of issues in a priority category that have been reviewed, move your cursor to the risk category.





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 a given Fortify priority, select the priority link.

### See Also

["Filtering Issues for Display on the OVERVIEW and AUDIT Pages" below](#)

## 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.

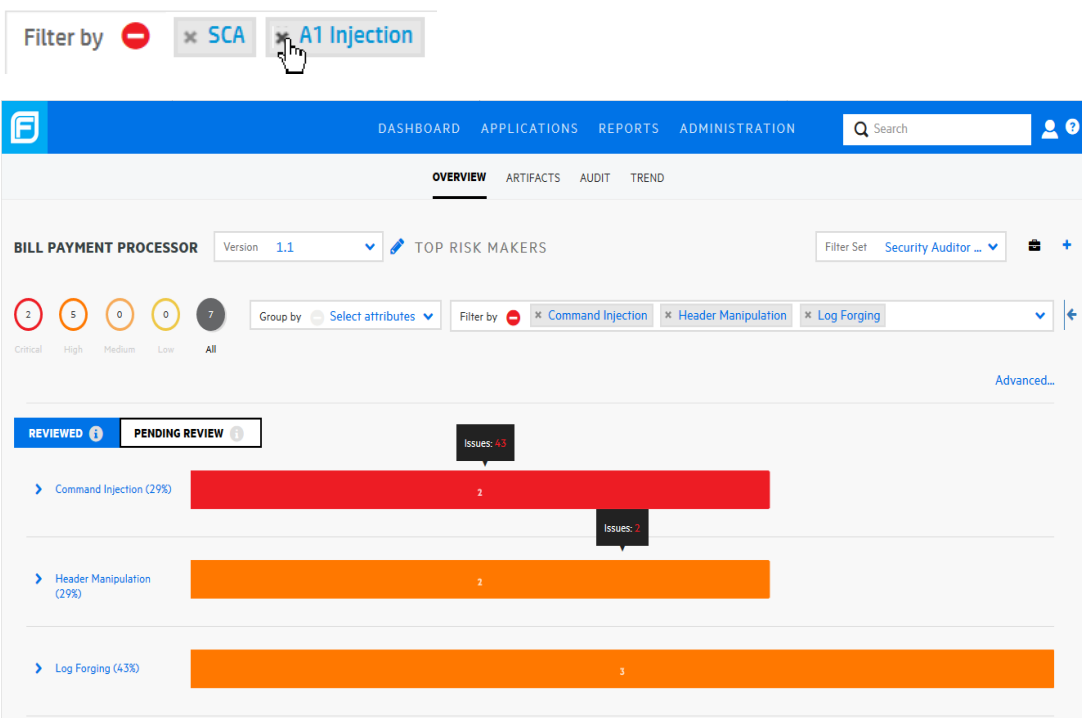
**Note:** You can also select a filter set to change the issues displayed on the OVERVIEW and AUDIT pages. For information and instructions, see ["Changing Displayed Issues Using Filter Sets" on page 265](#).

The screenshot displays the Fortify software interface. At the top, there is a navigation bar with tabs for DASHBOARD, APPLICATIONS, REPORTS, and ADMINISTRATION. Below this, the 'OVERVIEW' tab is selected. The main content area shows the application name 'BILL PAYMENT PROCESSOR' and its version '1.1'. There are buttons for 'TOP RISK MAKERS', 'Filter Set' (set to 'Security Auditor ...'), 'PROFILE', and '+ NEW VERSION'. A summary section shows issue counts by priority: 101 Critical, 84 High, 2 Medium, 663 Low, and 850 All. Below this, there are 'Group by' and 'Filter by' dropdown menus. The main table lists issues with expandable arrows and colored bars indicating counts: Command Injection (13) with 2, Cross-Site Scripting: Persistent (13) with 5, Cross-Site Scripting: Reflected (53) with 41, Header Manipulation (13) with 2, and J2EE Misconfigurati...ve Servlet Mappings (13) with 1. A legend at the bottom indicates 'REVIEWED' (blue) and 'PENDING REVIEW' (grey) counts.

To filter issues for display on the OVERVIEW (shown) or AUDIT page:

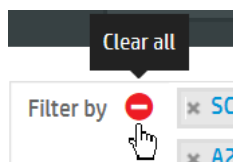
1. From the **Group by** list, select the attribute to use to group the issues in the issues table.
2. From the **Filter by** list, select the attributes to use to filter the issues for display in the issues table. You can select multiple attributes from this list. However, you must select them one at a time.
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.  
The ADVANCED ISSUE FILTERS window opens.
- b. From the **Select filter category** list, select a category.  
The **Select filters** list is populated with the filters available for the selected category.
- c. To refine the list further, type a text string in the **Select filter** box.  
The **Select filters** list displays the filters that contain the text that matches the text you typed.
- 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 selected filters, click the **Clear all** icon.

### See Also

["Viewing Issues Based on Fortify Priority" on page 255](#)

["Searching Issues" on the next page](#)

["Searching Globally in Fortify Software Security Center" on page 277](#)

## 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

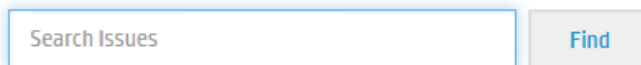
["Viewing Removed Issues" on page 276](#)

## 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. Access the AUDIT page for the application version. (See ["Accessing the AUDIT Page from the Issue Stats Page of the Dashboard" on page 255](#) or ["Accessing the AUDIT Page from the Issue Stats Page of the Dashboard" on page 255](#).)



The image shows a user interface for searching issues. It consists of a text input field with the placeholder text "Search Issues" and a button labeled "Find" to its right.

[Syntax Guide](#)

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" below](#).)

**Note:** If an application version is assigned a date-type custom tag, and you want to search for issues based on the date assigned to the issue, you must specify the date in the format `<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 257](#)

["Search Query Examples" on page 263](#)

["Searching Globally in Fortify Software Security Center" on page 277](#)

**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 <code>exploitable</code> , <code>not an issue</code> , and so on).
analyzer	Searches the issues for the specified analyzer
audience	Searches for issues by intended audience. Valid values are <code>targeted</code> , <code>medium</code> , and <code>broad</code> .
audited	Searches the issues to find <code>true</code> if the primary custom tag is set and <code>false</code> 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.
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.
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 determined by Fortify Static Code Analyzer. Valid values are <code>critical</code> , <code>high</code> , <code>medium</code> , and

Modifier	Description
	<p>Low, based on the expected <i>impact</i> and <i>likelihood</i> of exploitation.</p> <p>The impact value indicates the potential damage that might result if an issue is successfully exploited. The likelihood value is a combination of confidence, accuracy of the rule, and probability that the issue can be exploited.</p>
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 3.2], 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. 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 <a href="#">sink</a> and <a href="#">[source context]</a> .
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 <a href="#">[primary context]</a> .
source	Searches for dataflow issues that have the specified source function name. Also see <a href="#">[source context]</a> .
[source context]	Searches for dataflow issues that have the source function call contained in the specified code context

Modifier	Description
	Also see <a href="#">source</a> and <a href="#">[primary context]</a> .
sourcefile	Searches for dataflow issues with the source function call that the specified file contains.  Also see <a href="#">file</a> .
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 259](#)

### 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 paths that contain traces with `mydbcode.sqlcleanse` as part of the name, type:  
`trace:mydbcode.sqlcleanse`
- To search for all paths that contain traces with `cleanse` as part of the name, type:  
`trace:cleanse`
- 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 259](#)

["Search Modifiers" on page 260](#)

## About Suppressed, Removed, and Hidden Issues

You can control whether the issues panel lists the following types of 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 panel on the AUDIT page. Suppressed issues are also not included in the calculation of application version metrics. For information about how to suppress an issue, see ["Auditing Issues" on page 249](#).

### Removed issues

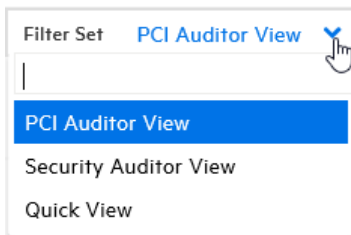
As multiple scans are run on an application over time, issues are often remediated or become obsolete. As Fortify Software Security Center merges scan results, it marks issues that were uncovered in a previous scan, but are no longer evident in the most recent analysis results as *Removed*. Removed issues are not included in the Total Issues value shown in the **Version Progress** section of the expandable panel on the AUDIT page.

### 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.



## 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 and AUDIT pages:

- Quick View  
The Quick View filter set provides a view only 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). The Quick View 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.

## 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.

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

## 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 Community Intelligence data (pooled, anonymized data from Fortify users), audit data that your security team has completed, or data from both sources. This data provision is referred to as *training*. 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. This gives you access to the Fortify Community Intelligence data set. If you choose *not* to share your training data, and so do not have access to the Fortify Community Intelligence data set (default configuration), then you must submit your own training data before you can get valid assessments from Audit Assistant.

Audit Assistant can also learn through corrections that are included in the training 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.

## 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>.

**Fortify**  
SCAN ANALYTICS

Email

Password

**LOGIN**

[Forgot Your Password?](#) | [Need an Account?](#)

- 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 classifiers.
3. From Fortify Scan Analytics, create one or more policies.
4. (Optional) Choose to share anonymous metadata.

5. Obtain a Fortify Scan Analytics token.
6. 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 74).
  - 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.
7. 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*.
8. From Fortify Software Security Center, open an application version and submit its Fortify Static Code Analyzer scan results to Audit Assistant.
9. After Audit Assistant completes its assessment, view those results and, if necessary, adjust them.
10. 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**

["Configuring Audit Assistant" on page 74](#)

["About Classifiers and Prediction Policies" below](#)

["Defining Classifiers" on the next page](#)

["Defining a Catch-All Classifier" on page 271](#)

["Defining Prediction Policies" on page 271](#)

["Enabling Metadata Sharing" on page 273](#)

["Enabling Auto-Apply and Auto-Predict for an Application Version" on page 193](#)

["Submitting Training Data to Audit Assistant" on page 274](#)

["Reviewing Audit Assistant Results" on page 274](#)

#### **About Classifiers and Prediction Policies**

To use Audit Assistant to process your scan results, you must first define classifiers and prediction policies in Fortify Scan Analytics.

Audit Assistant uses classifiers to classify issues and predict whether the issues represent true vulnerabilities. To define a classifier, you specify the criteria (issue attributes) that are to

determine which Fortify Software Security Center issue training metadata to pull into Fortify Scan Analytics.

You must also define at least one prediction policy to map issue attributes to different classifiers. For example, you can establish a prediction policy that directs all .NET issues to Classifier\_A, and all Java issues to Classifier\_B, all cross-site scripting Issues to Classifier\_C, and so on.

Prediction policies determine the confidence thresholds that Audit Assistant (and Scan Analytics) uses to determine which issues to treat as indeterminate - that is, neither a true issue nor a non-issue. To use Audit Assistant to process your scan results, you must first define one or more *prediction policies* in Fortify Scan Analytics.

When you submit a new scan to Audit Assistant for prediction, each issue can go to a different classifier, based on the prediction policy you specify in Fortify Software Security Center.

**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 Next

["Defining Classifiers" below](#)

#### See Also

["Defining Prediction Policies" on page 271](#)

["About Audit Assistant Auto-Prediction" on page 75](#)

["Configuring Audit Assistant Options for an Application Version" on page 211](#)["Configuring Audit Assistant" on page 74](#)

["Configuring Audit Assistant" on page 74](#)

## Defining Classifiers

Audit Assistant uses *classifiers* to classify issues and predict whether or not they represent true vulnerabilities. To define classifiers, you specify the criteria (issue attributes) that determine which Fortify Software Security Center issue training metadata to pull into Fortify Scan Analytics.

Fortify recommends that you define at least two classifiers: one that filters for certain criteria, and a *catch-all classifier* that specifies no filters. Using a catch-all classifier with a prediction policy ensures that issues that do not match any training criteria of other classifiers are still assessed. For information about how to use a catch-all classifier, see ["Defining Prediction Policies" on page 271](#).

**Note:** If you submit no training data *and* you do not enable metadata sharing, then the underlying classifier is not created and all issues end up "Not Predicted."

To define a classifier:

1. Log in to Fortify Scan Analytics (<https://analytics.fortify.com>).  
Fortify Scan Analytics opens to the Classifiers page.
2. Click **+ADD**.  
The Classifiers > Add page opens.
3. Under **Details**, type the classifier name and (optionally) description.  
Next, you specify the training criteria for the classifier to use by building a set of one or more AND / OR statements.
4. Under **Training Filter Criteria**, use the lists and combo boxes to build your training filter criteria (groupings of ANDs and ORs) for the classifier.

The following screen capture shows example training filter criteria for a classifier.

Training Filter Criteria [preview]

ALL of the following (AND) ▾

ANY of the following (OR) ▾ -

ALL of the following (AND) ▾ -

Fortify Priority Order ▾ = ▾ 4 ▾ -

Confidence ▾ = ▾ 3.7 ▾ -

+ Group + Value

ALL of the following (AND) ▾ -

Fortify Priority Order ▾ < ▾ 4 ▾ -

Confidence ▾ > ▾ 4.6 ▾ -

+ Group + Value

+ Group + Value

ANY of the following (OR) ▾ -

Has Source ▾ = ▾ True ▾ -

Has Snippets ▾ = ▾ True ▾ -

+ Group + Value

+ Group + Value

Limit to tenant training data

If you specify the value by selecting from a list of known values, as is true for attributes such as file type and language, then an **Override** check box is available under the list.



ALL of the following (AND) -

Category = [value]

Override

5. To specify a value that is not listed, select **Override**, and then type a value in the box.
6. To see the code for the filter you created, click **[PREVIEW]**.



```
(
  (
    (
      Fortify Priority Order = 4
      AND Confidence = 3.7
    )
    OR (
      Fortify Priority Order < 4
      AND Confidence > 4.6
    )
  )
  AND (
    Has Source = true
    OR Has Snippets = true
  )
)
```

Close

7. Close the Training Filter Criteria box.
8. To delete an element (either a group, or a child of a group), click the red minus character (-) to the right of the element.

in addition to the training data you submit to Audit Assistant, you can use the *Fortify Community Intelligence data set*. This is a large pool of anonymous data that Fortify customers have contributed for their training purposes.

9. To globally enable the use of (and contribute your metadata to) the Fortify Community Intelligence data set, follow the instructions provided in ["Enabling Metadata Sharing" on page 273](#)
10. To use this classifier with only the training data that you submit from Fortify Software Security Center, leave the **Limit to tenant training data** check box selected. To use this classifier with your training data *and* the Fortify Community Intelligence data set, clear this check box.

**Note:** The **Limit to tenant training data** check box is disabled if you have not enabled data sharing.

11. Click **SAVE**.

For information about how to associate your classifiers to prediction policies, see "[Defining Prediction Policies](#)" below.

#### See Also

["Configuring Audit Assistant" on page 74](#)

["About Classifiers and Prediction Policies" on page 267](#)

### Defining a Catch-All Classifier

In addition to the classifiers you define to filter issues based on training criteria, Fortify strongly recommends that you create a *catch-all classifier*, for which you specify *no* training criteria. Using a catch-all classifier with a prediction policy ensures that issues that do not match any training criteria of other classifiers are still assessed.

To define a catch-all classifier:

1. Log in to Fortify Scan Analytics (<https://analytics.fortify.com>).  
The Classifiers page opens.
2. Click **+ADD**.  
The Classifiers > Add page opens.
3. Under **Details**, type the classifier name and (optionally) description.
4. Click **SAVE**.

For information about how to associate your classifiers to prediction policies, see "[Defining Prediction Policies](#)" below.

#### See Also

["Defining Classifiers" on page 268](#)

### Defining Prediction Policies

Audit Assistant uses prediction policies to map issues to your classifiers.

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).

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**.  
The Prediction Policies > Add page opens.

4. In the **Policy Name** box, 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 shows how each issue was assessed. Possible values are **Exploitable**, **Not an issue**, and **Not Predicted**.
- 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. To associate a classifier with the new prediction policy:
  - a. Under **Classifiers**, from the **CLASSIFIER NAME** list, select a classifier, and then click **+ADD**.


The Prediction Policies | Add page imports the training criteria specified for the selected classifier as the mapping.



In the following screen capture, the added classifier Java\_JS specifies that, for this prediction policy, issues in either the Java or JavaScript language are to be sent to classifier Java\_JS.



You can either use the classifier as is, or you can override the classifier *for this prediction policy*. The training criteria that determine what the classifier "learns" from does not change.



- b. To override the classifier training criteria for this prediction policy:
  - i. To the right of the training criteria, click the override icon .
  - ii. In the Override Classifier Prediction Filter dialog box, modify the training criteria (just as you would if you were creating a classifier), and then click **OK**.
8. To associate another classifier with the prediction policy, repeat "[To associate a classifier with the new prediction policy:](#)" on the previous page.

Audit Assistant filters issues based on the order in which you list the classifiers for the prediction policy, starting from the top.
9. To change the order of a classifier in the List, use the up and down arrows   to the left of the classifier name.

Audit Assistant does not assess issues that do not match the filter criteria that the added classifiers specify. However, you can add a catch-all classifier to make sure that issues that do not meet the listed training criteria still get assessed.
10. To ensure that Audit Assistant assesses all issues, add your catch-all classifier as the last classifier. For information about how to create a catch-all classifier, see
11. To remove a classifier, click the red minus character (-) to the right of its name.
12. Click **SAVE**.

#### See Also

["About Classifiers and Prediction Policies" on page 267](#)

["Configuring Audit Assistant" on page 74](#)

["Configuring Audit Assistant Options for an Application Version" on page 211](#)

## 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 panel, select **Settings**.
3. Select the **Share anonymous issue metrics** check box.
4. Click **Save**.

#### See Also

["About Classifiers and Prediction Policies" on page 267](#)

["Configuring Audit Assistant" on page 74](#)

## 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.

To submit training data to Audit Assistant:

1. From the Dashboard, open a page (OVERVIEW, ARTIFACTS, AUDIT or TREND) 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 74](#).

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 265](#)

["Enabling Auto-Apply and Auto-Predict for an Application Version" on page 193](#)

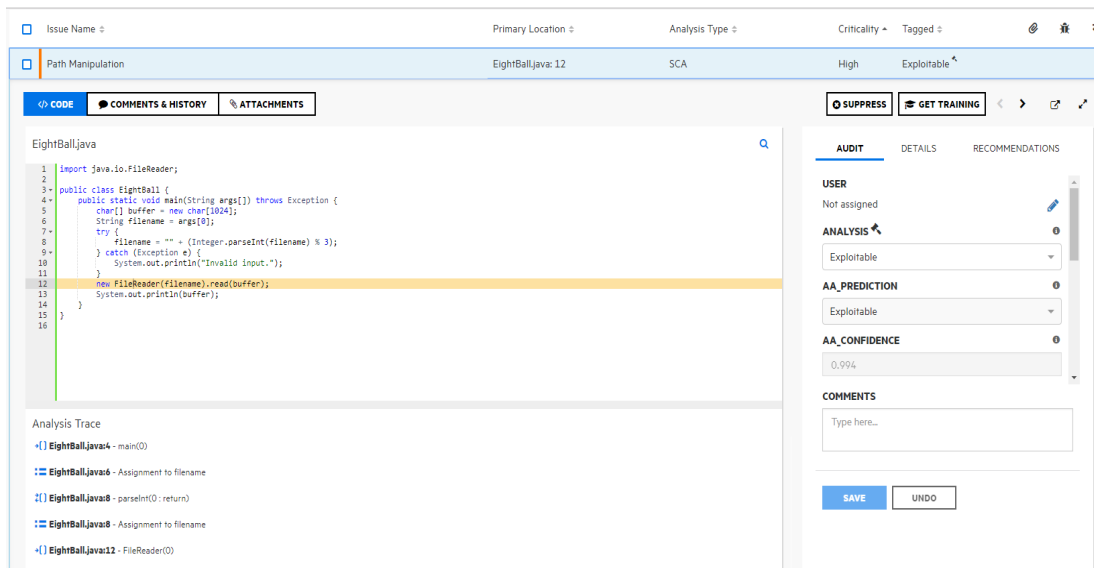
## Reviewing Audit Assistant Results

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 Fortify Priority" on page 255](#) and ["Filtering Issues for Display on the OVERVIEW and AUDIT Pages" on page 257](#).)
3. To selectively display the issues you want to view, apply filters to the issues list. (See ["Filtering Issues for Display on the OVERVIEW and AUDIT Pages" on page 257](#).)

- In the issues table, if you have selected a grouping, expand a group to view the issues it contains.
- To expand an issue and view its details, click its row in the table.



- In addition to the Analysis tag and any other custom tags associated with the application version, the right panel 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.
- 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.
- To specify whether to include the issue in or exclude it from Audit Assistant training, from the **AA\_Training** list, select either **Include** (the default) or **Exclude**.  
If the value you select from the **Analysis** list differs from the **AA\_Prediction** value, and you select **Include** from the **AA\_Training** list, then the next time you submit data for this application version to Audit Assistant, Audit Assistant updates the classifier based on your clarification.
- Click **SAVE**.

**See Also**

["About Audit Assistant" on page 265](#)

["Auditing Issues" on page 249](#)

## Setting Issue Viewing Preferences

You can set certain viewing preferences for individual application versions from the Application Profile dialog box. After you change your issue viewing options, that configuration will be persisted and Fortify Software Security Center will apply the same options when you switch to different application versions.

### Viewing Suppressed Issues

To view the suppressed issues associated with an application version:

1. From the Applications view, select the version name for the application version you are interested in.

Fortify Software Security Center opens the Overview page for the selected version.

2. On the application version toolbar, click **Profile**.

The Application Profile dialog box opens to the **Advanced Options** tab.

The number in parentheses (*N*) next to **Show suppressed issues** represents the total number of suppressed issues in the database associated with the selected application version.

**Note:** The filter set you have selected 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 (N)** check box.
4. Click **Apply**.

#### See Also

["Viewing Removed Issues" below](#)

### 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 Applications view, select the version name for the application version you are interested in.

Fortify Software Security Center opens the Overview page for the selected version.

2. On the application version toolbar, click **Profile**.

The Application Profile dialog box opens to the **Advanced Options** tab.

The number in parentheses (*N*) next to **Show removed issues** represents the total number of 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 (N)** check box.
4. Click **Apply**.

#### See Also

["Viewing Hidden Issues" below](#)

["Viewing Suppressed Issues" on the previous page](#)

## 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 Applications view, select the version name for the application version you are interested in.

Fortify Software Security Center opens the Overview page for the selected version.

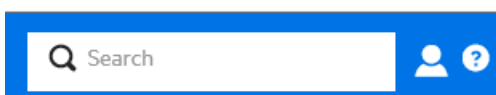
2. On the application version toolbar, click **Profile**.

The Application Profile dialog box opens to the **Advanced Options** tab.

The number in parentheses (*N*) next to **Show hidden issues** represents the total number of hidden issues in the database associated with the selected application version.

3. Select the **Show hidden issues (N)** check box.
4. Click **Apply**.

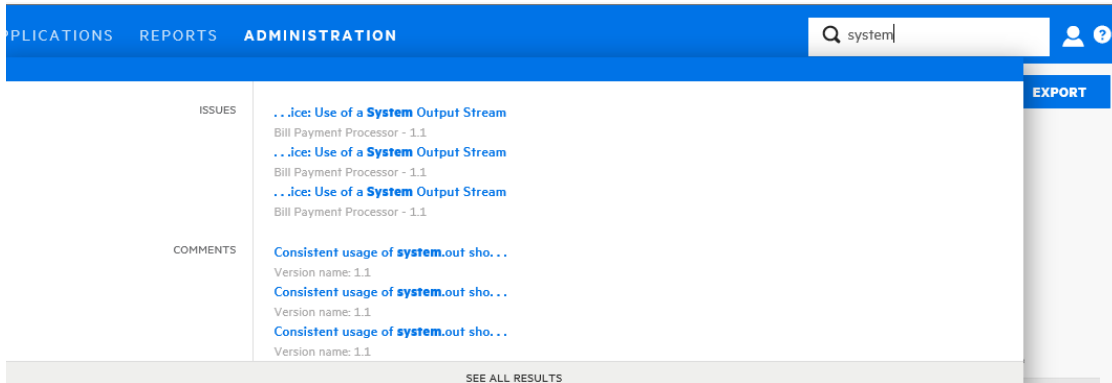
## Searching Globally in Fortify Software Security Center



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.

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.



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 off all search results, click **SEE ALL RESULTS**.

### Example: Finding issues

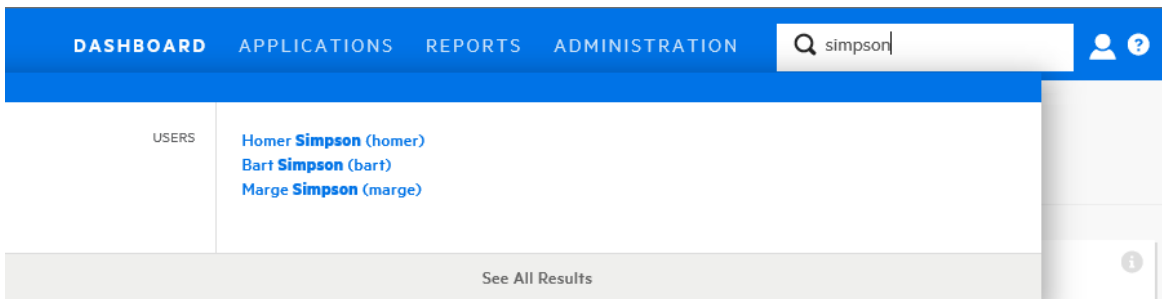


After you select a single issue from the listed results, Fortify Software Security Center takes you to the corresponding version page with the issue expanded to full view.

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.

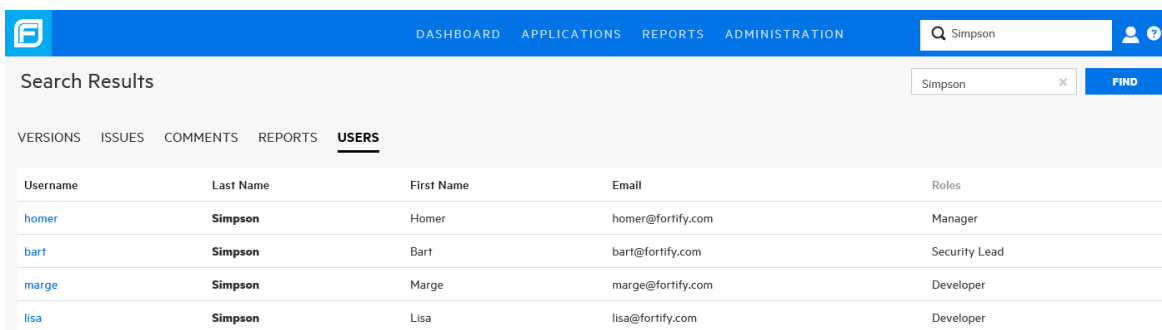
From there, you can use the next and previous buttons   to page through all of the findings.

## 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 195](#)

## Fortify Software Security Center and WebInspect Integration

Fortify Software Security Center and Fortify WebInspect are closely integrated and can share scan results. Administrators can also submit requests for WebInspect dynamic scans from the Fortify Software Security Center user interface. This section describes how to view 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 234.](#)) 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 panel 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 panel 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**.



Cross-Site Scripting hidden\_AdminControl.jsp WEBINSPECT Critical

CODE COMMENTS & HISTORY ATTACHMENTS SUPPRESS GET TRAINING

Overview

Cross-Site Scripting vulnerabilities were verified as executing code on the web application. Cross-Site Scripting occurs when dynamically generated web pages display user input, such as login information, that is not properly validated, allowing an attacker to...

Implication

XSS can generally be subdivided into two categories: stored and reflected attacks. The main difference between the two is in how the payload arrives at the server. Stored attacks are just that...in some form stored on the target server, such as in a database, or via a submission to a bulletin board or visitor log. The victim will retrieve and execute the attack code in his browser when a request is made for the stored information. Reflected attacks, on the other hand, come from somewhere else. This happens when user input from a web client is immediately included via server-side scripts in a dynamically generated web page. Via some script...

Additional References

HP Cross-Site Scripting Whitepaper  
[http://download.hp.smartupdate.com/asclabs/cross-site\\_scripting.pdf](http://download.hp.smartupdate.com/asclabs/cross-site_scripting.pdf)

OWASP Cross-Site Scripting Information  
<http://www.owasp.org/documentation/topten/a4.html>

Microsoft  
<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q252985>

Microsoft Anti-Cross Site Scripting Library V1.0  
<http://www.microsoft.com/downloads/details.aspx?familyid=9a2b9c92-7ad...>

URL: http://tomcatss.spidynamics.com:80/riches/pages/common/hidden\_AdminControl.jsp

Method: GET

Vulnerable Parameter: users

Attack Payload: users: 12345%3csCriP%3T%3ealer%3C%2FsCriP%3E

Request

```
GET /riches/pages/common/hidden_AdminControl.jsp?actions=12345&message=1974&users=12345&
Referer: http://tomcatss.spidynamics.com:80/riches/pages/common/hidden_AdminControl.jsp
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Accept: */*
Pragma: no-cache
Host: tomcatss.spidynamics.com
X-Scan-Memo: Category="Audit"; Function="createStateRequestFromAttackDefinition"; SID="D
Connection: Keep-Alive
Cookie: CustomCookie=WebInspect745672X283F9C295F541D790520A8090293A15VA029;JSESSID=ID=C
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 15 Sep 2011 16:46:10 GMT
X-WIPP-Version: java / 1.0 / tomcatss_5575
X-WIPP-RequestID: fcd7ba7f-5c93-484b-807f-67f11698778b
Content-Type: text/html; charset=ISO-8859-1
Content-Length: 901
Vary: Accept-Encoding
Keep-Alive: timeout=15, max=1
Connection: Keep-Alive

<form method=get action="hidden_AdminControl.jsp">
Shell Command<br />
<input name="actions" type=text size="80"><br />
<input type=submit value="Execute"><br /><br />
Automated shutdown message (sent to everyone by default)<br />
<input name="message" type=text size="80"><br />
<p><i>Send to Specific Users (semicolon separated list)</i></p><br />
<input name="users" type=text size="80"><br />

<input type=submit value="Broadcast Alert">

<h1>Emergency Broadcast sent to users:</h1><pre>12345csCriP%3T%3ealer%3C%2FsCriP%3E
</pre>

<h1>Transactions reported from database for account <i>12345</i></h1>

<br /><br /><tbody>Debug Code</tbody><br />
<i>Note: This code should be removed once debugging is complete for bug 192203 (insper
Account Number <input name="acctno" type=text size="15"/><br />
<input type=submit value="Retrieve">
</form>
```

AUDIT

USER  
Not Assigned

ANALYSIS  
Not Set

COMMENTS  
Type Here...

SAVE UNDO

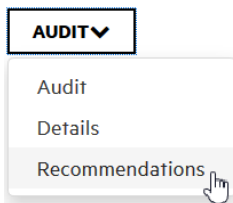
The **Steps** tab is available only if the steps are included in the WebInspect results file.

## 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 panel on the right to audit the issue, see ["Auditing Issues" on page 249](#).

## 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**.

<input type="checkbox"/> Issue Name ⇅	Primary Location ⇅
<input type="checkbox"/> Poor Error Handling: Overly Broad Catch	 AbstractLesson.java : 420

**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

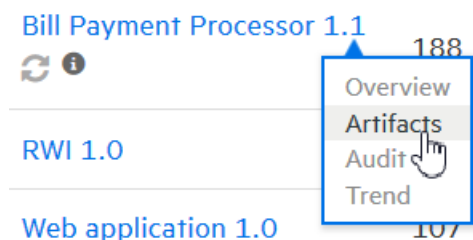
["Viewing Suppressed Issues" on page 276](#)

## 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**.  
The DYNAMIC SCAN - <APPLICATION VERSION> dialog box opens.
3. 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.

<b>Dynamic Scan Attribute</b> <b>* (Required field)</b>	<b>Description</b>
*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

<b>Dynamic Scan Attribute</b> <b>* (Required field)</b>	<b>Description</b>
	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	<p>Dates and times during which the tester can perform the scan</p> <p><b>Example:</b> From 17:00 h to 06:00 h, Monday through Friday, from 09/03/18 to 11/30/18</p> <p>You can run the scan immediately instead of scheduling it to run later. For instructions, see <a href="#">"Processing Dynamic Scan Requests from Fortify WebInspect Enterprise" on the next page.</a></p>
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 ["Submitting Dynamic Scan Requests to Fortify WebInspect Enterprise" on the previous page.](#) 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" on the next page.](#)

**See Also**

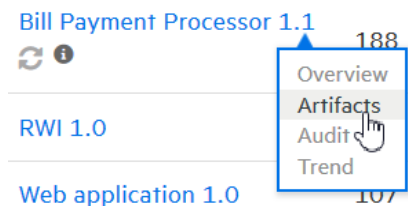
["Viewing Fortify WebInspect Scan Results in Fortify Software Security Center" on page 279](#)

## Processing Dynamic Scan Requests from Fortify WebInspect Enterprise

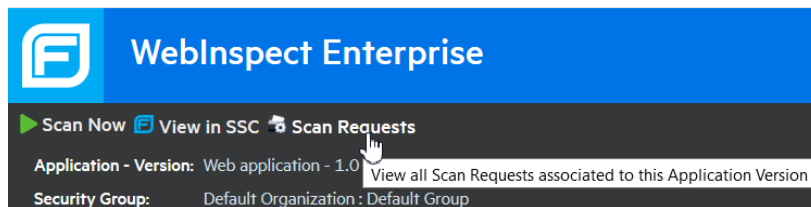
If you are in the role of Administrator or Application security tester, you can start Fortify WebInspect Enterprise, where you can view and process dynamic scan requests submitted by Fortify Software Security Center users.

To process dynamic scan requests in WebInspect Enterprise:

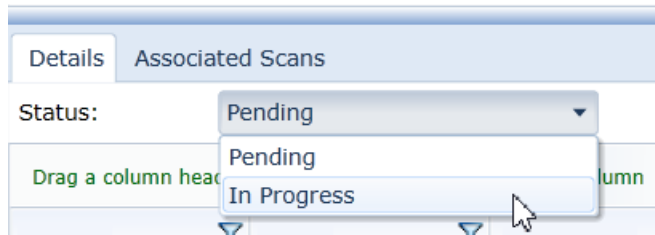
1. From Fortify WebInspect Enterprise, initialize Fortify Software Security Center, and then use the WebInspect Enterprise Console to synchronize Fortify Software Security Center application versions with WebInspect projects. (For instructions, see the *Micro Focus Fortify WebInspect Enterprise User 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 panel, 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 283](#)

## 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, 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 only edit 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 **Edit**.  
The Dynamic Scan Request dialog box opens.
3. 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 only cancel 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: Integrating with Fortify CloudScan



If Fortify Software Security Center is configured to communicate with Fortify CloudScan, then the Fortify Software Security Center user interface includes the Scans view, which contains the CloudScan 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 CloudScan, see "[Configuring CloudScan Monitoring in Fortify Software Security Center](#)" on page 81.

Topics covered in this section:

<a href="#">CloudScan Permissions</a>	288
<a href="#">Viewing CloudScan Scan Request Details</a>	289
<a href="#">Canceling CloudScan Scan Requests</a>	290
<a href="#">Viewing CloudScan Sensor Information</a>	290
<a href="#">Viewing CloudScan Controller Information</a>	291
<a href="#">About Fortify CloudScan Sensor Pools</a>	292
<a href="#">Pre-defined Sensor Pools</a>	292
<a href="#">Creating CloudScan Sensor Pools</a>	292
<a href="#">Deleting CloudScan Pools</a>	295

## CloudScan Permissions

The following table shows which Fortify Software Security Center roles have permission to perform which CloudScan-related tasks.

Roles	Permissions
Developer	View information on the Scan Requests, Sensors, and Sensor Pools pages
View Only	<b>Restrictions:</b> <ul style="list-style-type: none"><li>• Users see only the scan requests for application versions to which they are assigned</li><li>• Users see only sensor pool assignment for the application versions to which they are assigned</li></ul>
Administrator	View information on the Scan Requests, Sensors, and Sensor Pools pages



Security Lead  Manager	<p>Performing all tasks that involve changes to sensor pool</p> <p>Cancel scan requests</p> <p>Assign sensors and application versions to sensor pools.</p> <p><b>Restrictions:</b></p> <ul style="list-style-type: none"> <li>• Users can cancel only those scan requests for application versions to which they are assigned.</li> <li>• Users can assign only application versions to which they are assigned to sensor pools.</li> </ul>
------------------------------	--

To see what actions each Fortify Software Security Center role can perform:

1. On the Fortify header, select **ADMINISTRATION**.
2. In the left panel, 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 CloudScan Scan Request Details

To view details on CloudScan scan requests:

1. On the Fortify header, click **SCANS**.  
The Scans view opens to the Scan Requests page, which lists all scan requests and details for each, including the job token for the request, the build ID, status, application version, and more.
2. 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 the row.

Job Token	Build ID	Status	Application Version	Submitter	Queued Time	Completion Time	Queued Duration	Scan Duration
0b6be26-4ded-49fa-b3de-d2350a7431a2	dotnet	Upload Failed		root	07/29/2016 6:02:57 AM	07/29/2016 6:04:28 AM	59s	31s
a0c0f061-b0b5-40ef-9129-6536a29db3a6	dotnet	Upload Failed		root	07/29/2016 6:02:28 AM	07/29/2016 6:02:57 AM	14s	14s

**Submitter IP address**  
15.194.210.162

**Scan arguments**  
-scan

**Sensor Detail**

<b>UUID</b> caef1e5a-f6fd-45da-9aae-f5e1f5te911c	<b>SCA version</b> 16.10.0095	<b>Sensor IP address</b> 15.194.210.168	<b>Sensors JVM</b> 2780@qa-cs-rh6-wrka07	<b>Pool</b> AUTO_Pool_1_16200075_16100095
---	----------------------------------	--	---	--

4. To update the data displayed, click **Refresh Table**.

### See Also

["Canceling CloudScan Scan Requests" on the next page](#)

["Viewing CloudScan Sensor Information" below](#)

["Viewing CloudScan Controller Information" on the next page](#)

## Canceling CloudScan Scan Requests

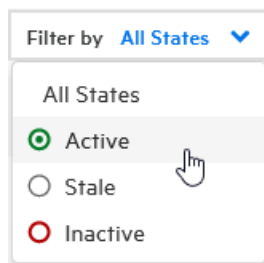
To cancel a pending CloudScan scan request:

1. On the Fortify header, click **SCANS**.  
The SCANS view opens to the Scan Requests page, 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 page, click **REFRESH TABLE**.

## Viewing CloudScan Sensor Information

To view current information about CloudScan sensor states and activities:

1. On the Fortify header, click **SCANS**.  
The Scans view opens to the Scan Requests page, which lists all sensors and the details for each.
2. In the left panel, select **Sensors**.  
A sensor can be in the active, inactive, or stale state.
3. To filter the displayed sensors based on current state (**Active**, **Inactive**, or **Stale**) from the **Filter by** list, select a state. (**All States** is the default.)



- To expand a row and see more detail about a sensor, click the row.

UUID	State	IP Address	VM Name	Last Seen	Start Time
f2ae5fa5-eadd-4411-beb2-6709de73b333	Active	15.194.210.27	2824@qa-cs-win-wrk01	02/24/2016 9:57:13 AM	02/22/2016 4:23:30 AM
<b>Sensor Start Time</b> 02/22/2016 4:23:30 AM		<b>Sensor Expiry Time</b> 03/02/2016 9:57:13 AM		<b>Sensor Last Seen</b> 02/24/2016 9:57:13 AM	
<b>SCA Version</b> 6.31.0012		<b>OS Name</b> Windows Server 2012		<b>OS Version</b> 6.2	
<b>Total Physical Memory</b> 8.0 GB		<b>Available Processors</b> 4		<b>OS Architecture</b> amd64	
<b>State</b> Active		<b>Last Activity</b> workrequest			
There are no CloudScan Jobs to display					

**See Also**

- ["Viewing CloudScan Scan Request Details" on page 289](#)
- ["Canceling CloudScan Scan Requests" on the previous page](#)

## Viewing CloudScan Controller Information

To view CloudScan Controller information:

- On the Fortify header, click **SCANS**.  
The Scans view opens to the Scan Requests page, where a table lists all scan requests and the details for each.
- In the left panel, select **Controller**.

CloudScan	Last poll status	Last Controller poll	Last poll time	Controller start time
Scan Requests	Available	04/09/2018 9:05:47 AM	04/09/2018 9:05:47 AM	04/06/2018 14:6:30 AM
Sensors	CloudScan controller URL	Max file size for upload	Controller disk free	Controller disk used
Controller	http://qa-cs-r-ctrl8080/cloud-ctrl	4.3 GB	37.3 GB	6.1 MB
Sensor Pools	Sensor shelf life	Sensor inactive delay	Job expiration	Job clean up period
	1m	1h	7d	1h
	SMTP host	SMTP port	Outgoing email address	
	localhost	25	cloud.control@hpe.com	
	SSC URL	SSC lockdown mode	Pool mapping mode	
	http://qa-sv-sles-was6.prgqa.hpecorp.net:8080/ssc23	False	Disabled	

- For descriptions of the information displayed, click the information icons

**See Also**

- ["Viewing CloudScan Scan Request Details" on page 289](#)
- ["Canceling CloudScan Scan Requests" on the previous page](#)
- ["Viewing CloudScan Sensor Information" on the previous page](#)

## About Fortify CloudScan Sensor Pools

If your Fortify Software Security Center server is integrated with Fortify CloudScan, 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 no team can consume all sensors and block scan requests submitted by others teams.

If a scan request is associated with an application version, the CloudScan Controller queries Fortify Software Security Center for available sensor pools. If the scan request is not associated with an application version, Fortify CloudScan clients can request a specific sensor pool for a scan request.

### 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. 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

["CloudScan Permissions" on page 288](#)

["Creating CloudScan Sensor Pools" below](#)

["Deleting CloudScan Pools" on page 295](#)

### Creating CloudScan Sensor Pools

If your Fortify Software Security Center server is integrated with CloudScan, you can create CloudScan sensor pools, which you can then target for scan requests.

To create a new sensor pool:

1. On the Fortify header, select **SCANS**.  
The Scan view opens to the Scan Requests page for CloudScan.
2. In the left panel, select **Sensor Pools**.  
The Sensor Pools page opens to **Sensor Pools** tab, which lists the default pool and any other sensor pools created on the system.

**Note:** The Default Pool is a pool of all application versions that have not been assigned

to a sensor pool.


3. On the Sensor Pools page header, click **+ NEW POOL**.

The CREATE NEW POOL wizard opens.

4. On **STEP 1. GENERAL**, do the following:

- a. 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).
- b. (Optional) In the **Description** box, type a description of the new pool (its properties or purpose).

The screenshot shows the 'Add Version' wizard interface. At the top, it says 'Add Version' with an information icon. Below that is a dropdown menu for 'Application' with 'Logistics' selected. There is a red minus icon to the left of the dropdown and a blue checkmark icon to the right. Below the dropdown is a checkbox labeled 'Show inactive versions'. Underneath is a search input field labeled 'Application version' and a 'FIND' button. Below the search field is another checkbox labeled 'Versions'. At the bottom, there are two version entries, each with a checkbox and a number: '1' and '2'.

- c. Under **Add Version**, from the list, select an application with versions that you want to assign to this pool.  
The wizard lists all active versions of the selected application.
- d. To have the wizard to list any inactive versions of the selected application, select the **Show inactive versions** check box.
- e. To assign all of the listed versions to the new pool, select the **Versions** check box. Otherwise, to assign only a subset of the application versions, select the check boxes next to the version names.  
On the right, the wizard lists your selections under **Selected Versions**.
- f. To assign versions of another application to this pool, repeat steps c through e.
- g. To remove an application version from the **Selected Versions** list, click the trash icon next to its name. 

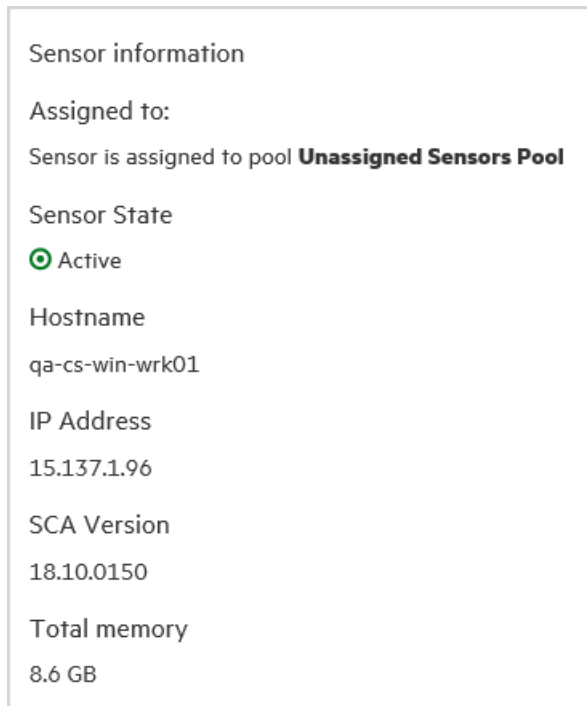
5. Click **NEXT**.

6. On **STEP 2. ASSIGN SENSORS**, do the following:

- a. To locate a specific sensor, type part or all of its host's name in the search box, and then click **FIND**.

The wizard lists all sensor hosts that include the specified text. The lock icon (🔒) next to the hostname indicates that the sensor is already assigned to a pool.

To see which pool the sensor is in, in the **Sensor Hostname** list, select the hostname, and then, in the **Sensor information** section, check the **Assigned to** value.



- b. To see which pool the sensor is in, in the **Sensor Hostname** list, select the hostname, and then, in the **Sensor information** section, check the **Assigned to** value.

The **Sensor information** section also displays the sensor state, the host IP address, available memory, and the Fortify Static Code Analyzer version installed.

- c. Select the check boxes for the sensors that you want to include in the pool. To add sensors that are not currently assigned to other pools, select the **Use unassigned sensors** check box.

The wizard lists your selections in the **Selected Sensors** list.

- d. To add another sensor, repeat steps a through c.
- e. To remove a sensor from the **Selected Sensors** list, either click the trash icon (🗑️) next to its name, or clear the check box for the sensor in the **Sensors** list.

#### 7. Click **FINISH**.

The **Sensor Pools** table now lists your new pool. The **Pool** column in the table on the Sensors page also lists the new pool name for the sensors included.

You can edit or delete the pool at any time.




#### **See Also**

["Viewing CloudScan Sensor Information" on page 290](#)

["Deleting CloudScan Pools" below](#)

## Deleting CloudScan Pools

To delete a CloudScan pool:

1. On the Fortify header, select **SCANS**.  
The Scan Requests view opens to the Scan Requests page for CloudScan.
2. In the left panel, 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 CloudScan Sensor Information" on page 290](#)

["Creating CloudScan Sensor Pools" on page 292](#)

## Chapter 17: 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:

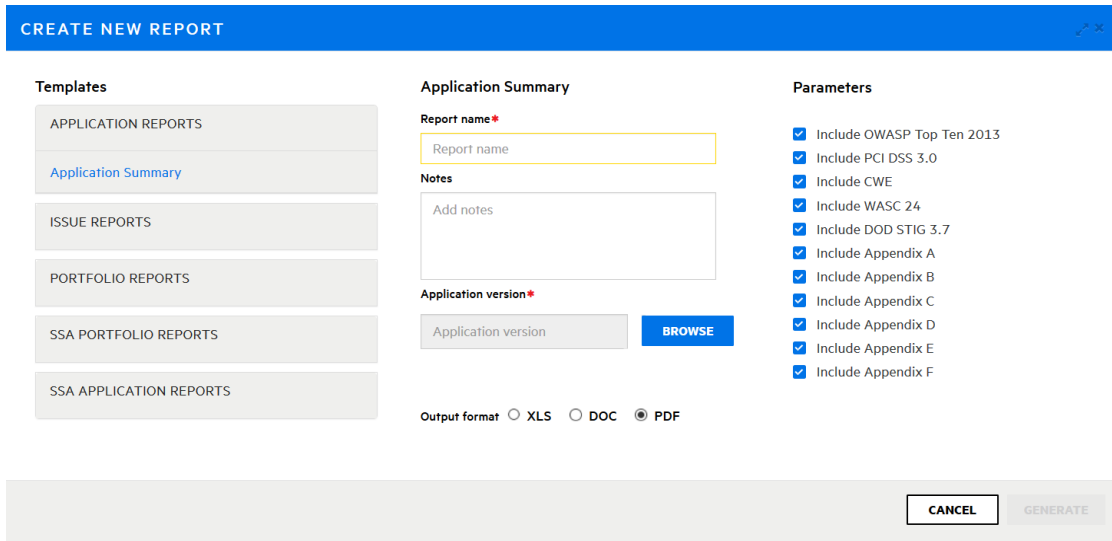
- **Application Summary Report:**  
Use the Application Summary report to summarize a single version of an application. This report includes a high-level look at the outstanding issues associated with the application version and detailed information related to its risk profile. It also includes a summary 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.
- **SSA Progress Report**  
The SSA Progress report details the completion of the security requirements for several applications. By monitoring the progress of various applications throughout the secure software development lifecycle (SDL), project managers and corporate security officers can identify potential security roadblocks to the SDL process roll-out. The data presented can also be used to determine if applications are completing their security obligations in a timely and consistent manner. Data is organized and presented for maximum usefulness to security officers and project manager.

### Generating and Viewing Reports

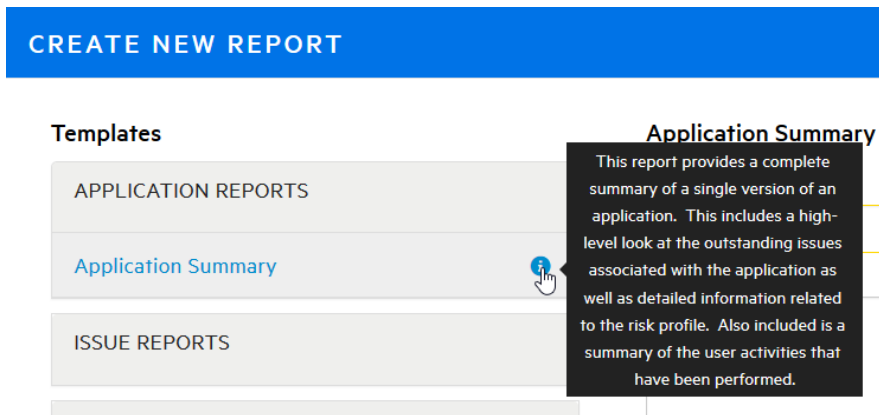
To generate and view a Fortify Software Security Center report:

1. On the Fortify header, click **REPORTS**.  
The **Reports** page opens.
2. On the **Reports** page toolbar, click **+ NEW REPORT**.

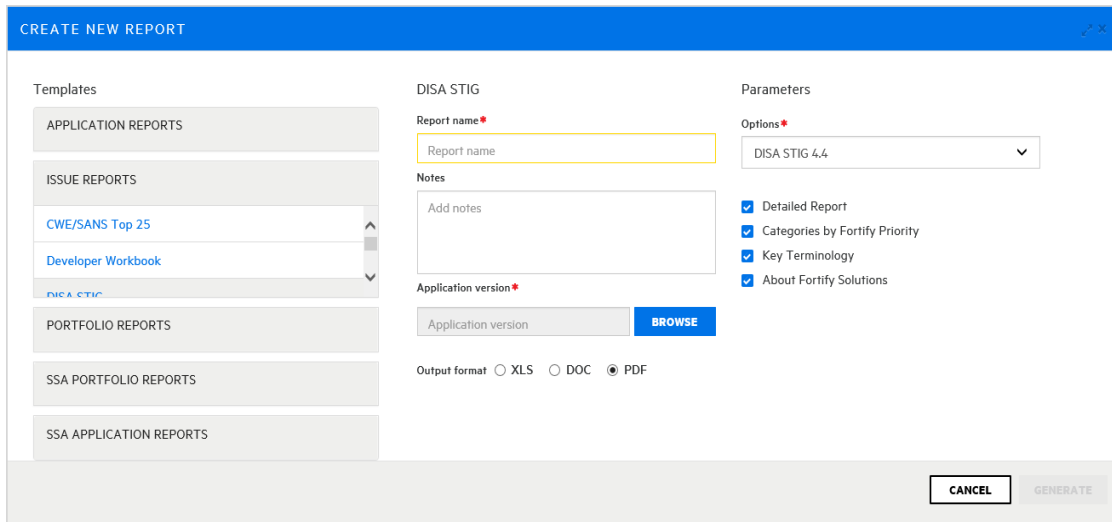




The CREATE NEW REPORT dialog box opens.



3. To see a description of the report that results from a listed template, move your cursor to the report listing, and then move it to the information icon **i**.
4. Navigate to and select the report template you want to use.



The panels on the right display the configuration fields for the template you select.

5. Specify the required report settings, including the report name, output format, and application versions to include in the report.

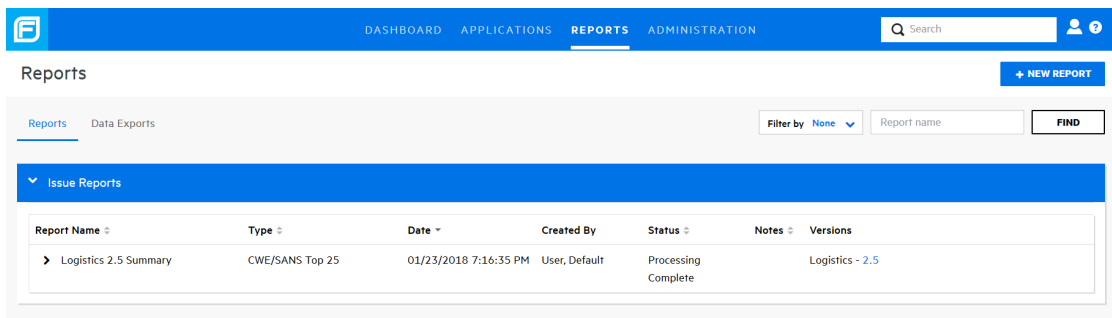
Depending on the report type, additional settings might be required or available.

#### Parameters

##### Options\*

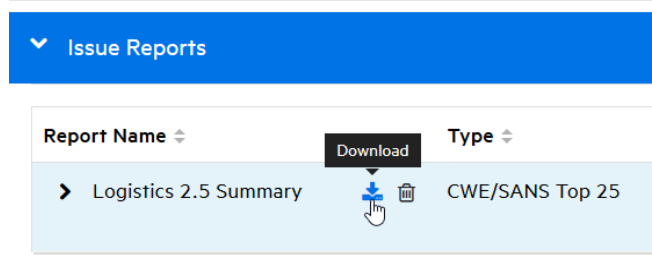



6. If multiple editions of a report template are available (for example, for CWE/SANS Top 25 issue reports), from the **Options** list, select the edition you want to generate.
7. Click **GENERATE**.



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 **Processing Complete**.

If you typed content in the **Notes** box when you configured the report, the **Notes** column displays a note icon for the report.



8. To view the report, move your cursor to the report name, and then click the **Download** icon .
9. Save or open the report.

## Preventing Destructive Libraries and Templates from Being Uploaded

**Caution!** A malicious user might modify a report library or template so that it contains arbitrary and potentially destructive SQL queries and commands. Only upload libraries and templates that have been written by a trusted user and that have been reviewed for malicious queries and commands.

Only users with 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 SQL queries and commands from being uploaded to Fortify Software Security Center:

- Make sure to assign these permissions only to trusted users.
- Make sure to check all custom templates for arbitrary SQL queries and commands before uploading them to Fortify Software Security Center.

## 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 the next page.](#)

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 panel 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. Click **IMPORT**.  
The IMPORT NEW LIBRARY TEMPLATE dialog box opens.
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 Libraries and Templates from Being Uploaded" on the previous page](#)

["Preventing Destructive Library and Template Uploads to Fortify Software Security Center" on page 126](#)

["Generating and Viewing Reports" on page 296](#)

## 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 *Micro Focus Fortify Software System Requirement* 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 Definitions](#)" below.
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 the next page.

## 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 *Micro Focus 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:  
[http://download.eclipse.org/birt/downloads/build\\_list.php](http://download.eclipse.org/birt/downloads/build_list.php)
2. Download the Report Designer Full Eclipse Install for your operating system.

## Downloading Report Definitions

To download a Fortify Software Security Center report definition:

1. On the Fortify header, click **REPORTS**.
2. In the **REPORTS** table, select the report.  
The row expands to display the report file name, report definition, category, and document type.
3. At the lower right, click **DOWNLOAD**.  
The Opening <Report\_File\_Name>. dialog box opens.
4. Open or save the file to your **Downloads** folder.

## 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 add 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 panel, select **Templates**, and then select **Reports**.

The **Reports** table lists existing report templates, along with the report template types and descriptions.

3. Click **IMPORT**.

The IMPORT NEW REPORT TEMPLATE dialog box opens.

4. 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 <b>BIRT</b> selected.
Template	Browse to and select a Fortify Software Security Center BIRT definition (with the <code>rptdesign</code> filename extension).

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. To add the new report definition to the list of definitions, click **SAVE**.

**See Also**

["Generating and Viewing Reports" on page 296](#)

# Chapter 18: 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

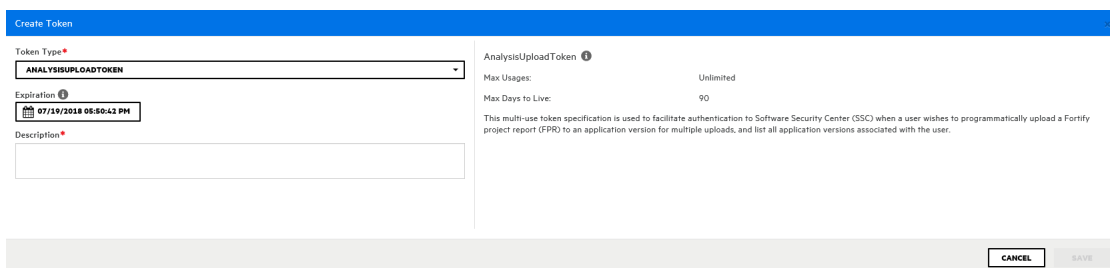
You can generate authentication tokens from either the ADMINISTRATION view in Fortify Software Security Center, or from the command-line interface. Only you can see the details of your tokens. The Fortify Software Security Center administrator can extend the life of the tokens you create, but cannot see detailed information about your tokens.

**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 panel of the ADMINISTRATION view, expand the **Users** section, and then select **Token Management**.
3. On the **Token Management** toolbar, click **NEW**.  
The Create Token dialog box opens.
4. From the **Token Type** list, select the type of token you want to create.



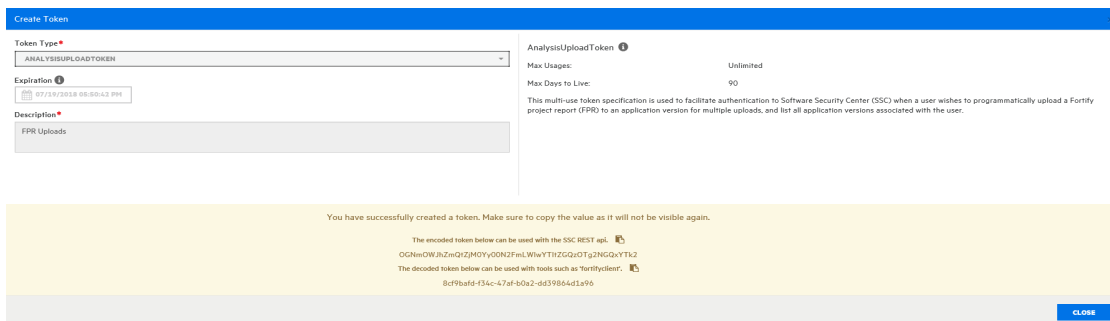
The Create Token dialog box displays a description of the selected token type in the right panel.



- 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.)

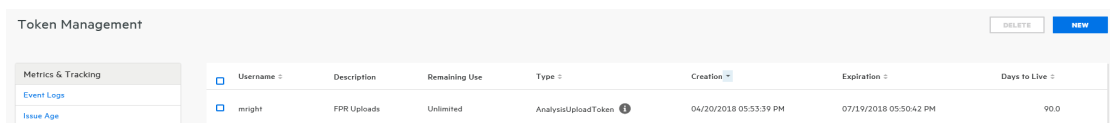
**Note:** By default, the expiration date value is set to the maximum number of days to live for the selected token type. You can set this to an earlier date to give the token a shorter life. You can also extend the life of the token later.

- In the **Description** box, type a description of the intended use of the new token.
- Click **SAVE**.



The Create Token dialog box displays a message to let you know the token was successfully created.

- 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.)
- Click **CLOSE**



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
```

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

Option	Description
	tags
CIToken	Enables integration of Software Security Center with continuous integration plugins
CloudCtrlToken	For CloudScan communications using the Fortify CloudScan CLI tools
CloudOneTimeJobToken	Single-use token specification typically created programmatically by the CloudScan client
DownloadFileTransferToken	Typically created programmatically by automation scripts using the /fileTokens endpoint to support a file download within an authenticated session
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  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
UnifiedLoginToken	Enables access to most of the REST API. It is intended for short-run automations that last less than a day
UploadFileTransferToken	Typically created programmatically by automation scripts using the /fileTokens endpoint to support a file upload within an authenticated session
VSTSExtensionToken	Used by the Fortify VSTS extension to upload FPR files to

Option	Description
	Fortify Software Security Center and, optionally, to submit a scan to Fortify CloudScan

Authentication tokens are defined at runtime in `WEB-INF/internal/serviceContext.xml`.

**See Also**

["Specifying DaysToLive for fortifyclient Authentication Tokens" on page 311.](#)

## 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 panel 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.
6. Click **SAVE**.

**See Also**

["Generating Authentication Tokens" on page 304](#)

## 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 panel 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 304](#)

# 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 that 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](#) ..... 309
- [Listing fortifyclient Options and Parameters](#) ..... 310
- [About Uploading Authentication Tokens](#) ..... 310
- [Listing fortifyclient Authentication Tokens](#) ..... 312
- [Invalidating Tokens](#) ..... 312
- [Listing Application Versions](#) ..... 313
- [Purging Application Versions](#) ..... 314
- [About Uploading FPRs](#) ..... 314
- [About Downloading FPRs](#) ..... 316
- [Importing Content Bundles](#) ..... 317
- [Downloading Audit Attachment Files](#) ..... 318

## 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](#) ..... 310
- [fortifyclient Authentication Tokens](#) ..... 310

## 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 Uploading 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](#) ..... 311

## 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 `fortify client` to acquire an upload authentication token. For information about how to generate one from the ADMINISTRATION view, see ["Generating Authentication Tokens" on page 304](#).

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. You are prompted for a password.

2. 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 Uploading 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 310](#)).

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 310](#)) 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.  
A list showing the ID, owner, creation date, expiration date, and creation IP address for all `fortifyclient` authentication tokens is returned.

## 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 panel 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

<code>&lt;ssc_url&gt;</code>	represents the URL of the Fortify Software Security Center instance (see <a href="#">"About Specifying the Fortify Software Security Center URL" on page 310</a> )
<code>&lt;token_ID&gt;</code>	represents the ID of the token to invalidate
<code>&lt;owner&gt;</code>	represents the user for whom the token is to be invalid
<code>&lt;token&gt;</code>	represents the name of the token to invalidate

### See Also

["Generating Authentication Tokens" on page 304](#)

## 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 Uploading Authentication Tokens" on page 310](#).)

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 310](#)) 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 310](#)) and `<app_identifier>` represents the `-application <app_name>`, `-version <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 page 316](#).

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 Uploading Authentication Tokens" on page 310](#).)

You can upload FPR files using one of the methods described in the following topics:

<a href="#">Using an Application Identifier to Upload FPR Files</a> .....	314
<a href="#">Using an Application Name and Version to Upload FPR Files</a> .....	315

### 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 <a href="#">"About Specifying the Fortify Software Security Center URL" on page 310</a> )
<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 313](#).

## 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>  
-project <app_name> -version <app_version>
```

where

<ssc_url>	represents the URL of the Fortify Software Security Center instance (see <a href="#">"About Specifying the Fortify Software Security Center URL" on page 310</a> )
<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
<app_version>	represents the Fortify Software Security Center application version that corresponds to the specified application name

## 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 314](#).

Topics covered in this section:

<a href="#">Downloading an FPR Using an Application Identifier .....</a>	<a href="#">316</a>
<a href="#">Downloading an FPR Using an Application Name and Version .....</a>	<a href="#">317</a>

### 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

<code>&lt;ssc_url&gt;</code>	represents the URL of the Fortify Software Security Center instance (see <a href="#">"About Specifying the Fortify Software Security Center URL" on page 310</a> )
<code>&lt;Username&gt;</code>	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
<code>&lt;password&gt;</code>	represents the password for the Developer-level (or higher) Software Security Center account with access to the application version that contains the FPR file
<code>&lt;FPRname&gt;</code>	represents the full path and name of the FPR file with its extension
<code>&lt;id&gt;</code>	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 313](#).

## 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

<code>&lt;ssc_url&gt;</code>	represents the URL of the Fortify Software Security Center instance (see <a href="#">"About Specifying the Fortify Software Security Center URL" on page 310</a> )
<code>&lt;username&gt;</code>	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
<code>&lt;password&gt;</code>	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
<code>&lt;fpr_name&gt;</code>	represents the full path and name of the FPR file with its extension
<code>&lt;app_name&gt;</code>	represents the Fortify Software Security Center application name
<code>&lt;app_version&gt;</code>	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

<code>&lt;ssc_url&gt;</code>	represents the URL of the Fortify Software Security Center instance (see <a href="#">"About Specifying the Fortify Software Security Center URL" on page 310</a> )
<code>&lt;username&gt;</code>	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.
<code>&lt;password&gt;</code>	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.
<code>&lt;bundle_name&gt;</code>	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_<br>file>  
-attachmentId <Attachment_Id>
```

where

<code>&lt;ssc_url&gt;</code>	represents the URL of the Fortify Software Security Center instance (see <a href="#">"About Specifying the Fortify Software Security Center URL" on page 310</a> )
<code>&lt;destination_file&gt;</code>	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 TFS/VSTS. (For specific versions supported, see the Micro Focus 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 ..... 320
- Application Setup ..... 321
- Implementation ..... 321
- Plugin Methods and Method Calls ..... 322
- Plugin Helper ..... 325
- Error Handling ..... 325
- Almost Stateless ..... 326
- Debugging a Bug Tracker Plugin ..... 326
- Deploying a Customized Bug Tracker Plugin ..... 326

## 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 119](#). 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.

## Application Setup

The bug tracker plugin can be an independent application that you can write using your preferred IDE.

Configure a bug tracker plugin with the following dependencies:

- `fortify-public-<version>.jar` (required)
- Apache Commons Logging (optional)
- Apache Commons Lang (optional)

You can use your preferred build system to build your application 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 removed from current versions of Java post-Java8. Such packages include JAXB API and implementation, javax.activation, javax.annotation, javax.transaction, javax.xml.ws, and CORBA-related packages.

## Implementation

All plugins must implement the `com.fortify.pub.bugtracker.plugin.BugTrackerPlugin` interface. Fortify strongly recommends that your implementation class extend `com.fortify.pub.bugtracker.plugin.AbstractBugTrackerPlugin` so that you can take advantage of any backward-compatibility support that becomes available in future releases. Also, you must annotate the implementation class with `@BugTrackerPluginImplementation`.

The `BugTracker` plugin interface 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, UserAuthenticationStore credentials);  
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 <code>true</code> if it requires the framework to request credentials from the user for any bug-tracking operation. This almost always returns <code>true</code> , 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 <code>false</code> , the system passes null for all the <code>UserAuthenticationStore</code> parameters of the plugin methods.
getConfiguration	The plugin framework uses the <code>getConfiguration</code> method to get metadata about the questions to be presented to the user during plugin configuration. The return value is a list of <code>BugTrackerConfig</code> objects that provide required information about the configuration item. Each item corresponds to a text box in the user interface. The <code>value</code> 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

Method or Call	Description
	<p>plugin are preceded by the <code>setConfiguration</code> call, which sets the configuration for the plugin using which operations are to be carried out.</p>
<p><code>testConfiguration</code> (call)</p>	<p>The plugin framework uses the <code>testConfiguration</code> call to test the configuration previously set using the <code>setConfiguration</code> 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.</p>
<p><code>getShortDisplayName</code></p>	<p>The <code>getShortDisplayName</code> 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.</p> <div data-bbox="516 814 1403 1083" style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p><b>Important!</b> 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 <i>do</i> change the name of the main implementation class, then you must also change the display name(s) for the plugin.</p> </div>
<p><code>getLongDisplayName</code></p>	<p>The <code>getLongDisplayName</code> 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.</p> <div data-bbox="516 1304 1403 1572" style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p><b>Caution!</b> 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 <i>do</i> change the name of the main implementation class, then you must also change the display name(s) for the plugin.</p> </div>
<p><code>getBugParameters</code></p>	<p>The <code>getBugParameters</code> method returns metadata about the bug parameters to present to users. Fortify Software Security Center supports the following three bug parameter types:</p> <ul style="list-style-type: none"> <li>• <code>BugParamText</code> translates to a text box.</li> <li>• <code>BugParamTextArea</code> translates to a multiple-line text box and is typically used for bug descriptions.</li> </ul>

Method or Call	Description
	<ul style="list-style-type: none"> <li>• BugParamChoice translates to a list.</li> <li>• The <code>issueDetail</code> object encompasses the details of the issue for which the user is 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 <code>pluginHelper</code> protected member has a helper method to build a suggested default bug description. (See <a href="#">"Plugin Helper" on the next page.</a>)</li> </ul>
<p><code>onParameterChange</code></p>	<p>The plugin framework calls the <code>onParameterChange</code> method whenever the value for a bug parameter marked as <code>hasDependentParams</code> (see <code>BugParamChoice</code> class javadoc) changes. This method can take action and return a new list of bug parameters to display.</p> <p>Keep the following guidelines in mind:</p> <ul style="list-style-type: none"> <li>• Act on each bug parameter that has dependent parameters</li> <li>• Do not forget handling case when parameter value changes to null (no selection made)</li> <li>• Do not forget to set the parameter value in a return list to null when its selections change</li> <li>• Before you add a new parameter, check the return list to make sure that it does not already include the parameter</li> <li>• Return null if there is no change</li> <li>• Use one of the following strategies: <ul style="list-style-type: none"> <li>• Modify the <code>currentValues</code> parameter and return it</li> <li>• Construct the return value from raw parameters maintained. Set values and choice lists before returning.</li> </ul> </li> </ul>
<p><code>fileBug</code></p>	<p>This method files a bug on the external bug-tracking system. The <code>BugSubmission</code> object passed encompasses all bug details.</p> <p>Make sure that you correctly differentiate between the <code>bug.getIssueDetail()</code> object and the <code>bug.getParams()</code> object. The <code>bug.getIssueDetail()</code> object returns details of the issue, whereas the <code>bug.getParams()</code> object returns the bug parameter values that the user provides.</p> <p>If you added Bug Description as a user-editable bug parameter, then fetch the bug description from the <code>bug.getParams()</code> object instead of from</p>

Method or Call	Description
	<p>the <code>bug.getIssueDetail()</code> object. The return value of the <code>fileBug</code> object must be a <code>bugId</code>, which can be used to fetch the bug with the <code>fetchBug</code> method and formulate the deep link with the <code>getBugDeepLink</code> method.</p> <p>Use fields in <code>BugSubmission.getIssueDetail()</code>, namely <code>getLastBuildWithoutIssue()</code>, <code>getDetectedInBuild()</code>, and <code>getFileName()</code> to perform changeset discovery if you have access to your repository.</p>
<code>fetchBug</code>	This method is used to fetch the current bug status.
<code>getBugDeepLink</code>	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 **AbstractBugTrackerPlugin** 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 = '1.7'
targetCompatibility = '1.7'

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 320](#)

## Appendix C: Automating Fortify Software Security Center Configuration

You can automate Fortify Software Security Center configuration before deployment using the `<appcontext>.autoconfig` autoconfig file. This YAML file includes sections for each configurable aspect of Fortify Software Security Center. The auto configuration file enables automated Fortify Software Security Center deployment by providing settings and seed bundles for silently Fortify Software Security Center update and installation. You can use the `<appcontext>.autoconfig` file to automate all Setup wizard tasks except for the database migration. The Setup wizard picks this file up at the server startup and automates the entire installation.

To automate Fortify Software Security Center configuration:

1. Open a text editor and create a file named `ssc.autoconfig`, where `ssc` is the context of the application server where SSC is deployed.

**Important!** The file name must match the application context name (for SSC, `ssc.autoconfig`) with exception of ROOT context (`_default_.autoconfig`).

2. Add the contents to the file in the following format:

```
ssc.autoconfig // located in <fortify.home>
appProperties: {
  /* any property found in <fortifyhome>/ssc/conf/app.properties
  such as host.validation: false,
  /*
  }
datasourceProperties: {
  /* any property found in
  <fortifyhome>/ssc/conf/datasource.properties such as
  db.driver.class: 'com.mysql.jdbc.Driver',
  /*
  }
  /*Array of bundles to seed into the database automatically*/
seeds: [
  'somepath/Fortify_Process_Seed_Bundle.zip',
  'somepath/Fortify_Report_Seed_Bundle.zip',
  'somepath/Fortify_PCI_Basic_Seed_Bundle.zip',
  ]
}
```

3. Add your database details.
4. Specify the paths to seed bundle zip files.
5. Specify the search index location.



6. Specify values for any other properties in `<fortify.home>/ssc/conf/app.properties`.
7. Save the file in `/root/.fortify/`.
8. Place a copy of your `fortify.license` file to your `<fortify.home>` folder.
9. Start Tomcat Server.
10. Remove the `*.autoconfig` file from `/root/.fortify/` after you deploy Fortify Software Security Center.

**Important!** You must remove or rename the `*.autoconfig` file after deployment. Otherwise, Fortify Software Security Center will be reconfigured and re-seeded at every time you start the server.

# Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

**Feedback on User Guide (Fortify Software Security Center 18.20)**

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](mailto:FortifyDocTeam@microfocus.com).

We appreciate your feedback!