OpenText™ Application Security

Application Security

Version 26.4

PDF Generated on November 11, 2026

© Copyright 2026 Open Text

Table of Contents

Application Security 11
1 Change log 11
2 Introduction 16
2.1 Product name changes 17
2.2 Audience 17
2.3 Related documents 18
3 Providing for secure deployment 25
3.1 Securing access to facilities 25
3.2 Securing Tomcat server 25
3.3 Setting Tomcat server attributes to protect sensitive data in cookies 25
3.4 Using HTTPS and SSL communications 26
3.5 About securing passwords and user roles 26
3.6 Managing computer services and accounts 27
4 Deploying Application Security 27
4.1 Deployment overview 27
4.2 High-level deployment tasks 30
4.3 Downloading and unpacking Application Security files 32
4.4 About the Application Security database 33
4.4.1 About JDBC drivers 34
4.4.2 Installing and configuring the database server software 34
4.4.3 Monitoring disk I/O 34
4.4.4 Database user account permissions 34
4.4.5 Database-specific configuration requirements 35
4.4.5.1 Using a SQL server database 35
4.4.5.2 Using a MySQL database 36
4.4.5.3 Using an Oracle database 39
4.4.5.3.1 Preventing the "No more data to read from socket" error 39
4.4.5.3.2 Partitioning an Oracle database for improved performance 40
4.4.6 About the Application Security database tables and schema 40
4.4.7 About seeding the Application Security database 40
4.4.8 Permanently deleting a Application Security database 41
4.5 About deploying Application Security in Kubernetes 42
4.6 About the directory 45
4.6.1 Changing the default location 45
4.6.2 Directory contents 46
4.6.3 Migration of secret.key file 47
5 Configuring Application Security for the first time 48
5.1 Signing in to Application Security for the first time 51
6 Additional Application Security configuration 52
6.1 About integrating components with Application Security 53
6.2 Configuring Issue Stats thresholds 55
6.3 Configuring application security training 56

6.4 Configuring AI Assistant 56
6.4.1 About Fortify Audit Assistant 57
6.4.1.1 Configuring Fortify Audit Assistant 57
6.4.1.2 About Fortify Audit Assistant auto-prediction 59
6.4.2 Configuring Aviator 59
6.5 Configuring security for BIRT reporting 60
6.5.1 Allocating memory for report generation 61
6.5.2 Setting report generation timeout 62
6.6 Configuring core settings 62
6.6.1 About configuring a proxy for Rulepack updates 65
6.7 Managing Fortify Object Storage 66
6.8 Blocking data export to CSV files 68
6.9 Changing the support contact link in the About box 68
6.10 Adding a Fortify Insight link to the Dashboard 69
6.11 Customizing the banner for your organization 69
6.12 Creating a system-wide banner 70
6.13 Configuring global processing rule defaults 71
6.14 Configuring email alert notification settings 71
6.14.1 Configuring whether to receive email alerts 75
6.15 Setting the strategy for resolving issue audit conflicts 75
6.16 Configuring Java Message Service settings 76
6.17 About Application Security user authentication 77
6.18 LDAP user authentication 77
6.18.1 Preparing to configure LDAP authentication 77
6.18.2 Requirements for multiple LDAP servers 78
6.18.3 About the LDAP server referrals feature 79
6.18.4 Disabling LDAP referrals support 79
6.18.5 Configuring LDAP servers 79
6.18.5.1 Editing an LDAP server configuration 85
6.18.5.2 Deleting an LDAP server configuration 86
6.18.5.3 Importing an LDAP server configuration 86
6.18.5.4 Registering LDAP entities 87
6.18.5.5 Refreshing LDAP entities manually 87
6.18.5.6 Handling LDAP entries marked 88
6.18.6 Enabling persistence of the LDAP cache 88
6.19 Implementation of SCIM 2.0 protocol 89
6.19.1 Using SCIM 2.0 and SAML 2.0 to configure a connection to Microsoft Entra ID for user provisioning 90
6.19.2 Enabling SCIM to provision externally managed users and groups 92
6.20 Configuring a proxy for integrations 93
6.21 Enabling the running and management of OpenText ScanCentral DAST scans 94
6.22 Configuring a Kafka Stream to use with OpenText ScanCentral DAST 94
6.23 Enabling integration with Fortify ScanCentral SAST 95
6.24 Configuring job scheduler attributes 96
6.24.1 Setting job execution priority 101

6.24.2 Canceling scheduled jobs 102
6.25 Recurring cleanup jobs 102
6.26 About data retention 104
6.26.1 Enabling data retention 104
6.26.2 Editing the default data retention policy 108
6.27 Configuring secure browser access 109
6.28 About configuring Application Security to work with single sign-on 111
6.28.1 Configuring SAML 2.0-compliant single sign-on 111
6.28.1.1 Troubleshooting SAML SSO integration 115
6.28.2 Configuring single sign-on and single logout solutions that use HTTP headers 116
6.28.3 Configuring X.509 certification-based single sign-on 116
6.28.4 Enabling debug logging for single sign-on authentication 117
6.29 Configuring logging 118
6.30 Running in a Federal Information Processing Standards (FIPS) environment 118
6.31 Setting the required password strength for Application Security sign in 119
6.32 About audit issue history 120
6.32.1 Enabling audit issue history 121
7 Additional installation-related tasks 121
7.1 About bug tracking system integration 121
7.1.1 Adding bug tracker plugins 122
7.1.2 Removing bug tracker plugins 122
7.1.3 Securing logon credentials for bug tracking systems 123
7.1.4 Bug tracker parameters 123
7.1.4.1 ALM Quality Center parameters 123
7.2 Adding and managing parser plugins 124
7.2.1 Preparing to display OpenText Core SCA (Debricked) results 124
7.2.2 Preparing to display Sonatype results 125
7.3 About Application Security user administration 125
7.3.1 Administrator accounts 126
7.3.2 User account types 126
7.3.3 About creating user accounts 126
7.3.4 Preventing destructive library and template uploads to Application Security 127
7.3.5 Viewing permissions for Application Security roles 127
7.3.6 About managing LDAP user roles 127
7.3.6.1 Group membership in Application Security 128
7.3.6.2 Handling failed LDAP user logins 128
7.3.6.3 About mapping Application Security roles to LDAP groups 128
7.4 Global search functionality in Application Security 129
7.4.1 Troubleshooting search index issues 129
7.5 Placing Application Security in maintenance mode 129
7.5.1 If Application Security is stuck in maintenance mode 130
7.6 Pausing and resuming job execution 131
7.7 About OpenText SAST Application Security Content 131
7.7.1 Updating Rulepacks from the Rulepack update server 132
7.7.2 Exporting Rulepacks 132

7.7.3 Importing OpenText SAST Application Security Content 133
7.7.4 Deleting Rulepacks 133
7.7.5 Extending an existing mapping 133
7.7.6 Creating a new mapping 135
7.8 Enabling OpenText SAST and OpenText Application Security Tools upgrades from Fortify Audit Workbench 135
8 Upgrading Application Security 137
8.1 Upgrade prerequisites 137
8.2 Preparing to upgrade the database 137
8.2.1 Setting the Innodb buffer pool size when upgrading a MySQL database 138
8.2.2 Preparing to run the database upgrade script 138
8.3 Upgrade tasks 138
8.4 Upgrade Lucene 139
8.5 Updating and deploying the WAR file 140
8.6 Configuring Application Security after an upgrade 140
8.7 Updating expired licenses 142
8.8 Seeding the database with report seed bundles in quarterly OpenText SAST Application Security Content releases 142
9 Using Application Security 142
9.1 Signing in to Application Security 143
9.1.1 About session logout 143
9.2 Requesting access to Application Security 144
9.3 Changing your password 144
9.4 Setting preferences system-wide and across application versions 144
9.5 Viewing keyboard hotkeys 145
9.6 Accessing the API documentation 145
9.7 About the Application Security Dashboard 146
9.7.1 Overview 146
9.7.2 Issue Stats 148
9.7.3 Viewing high-level summary metrics for your application versions 149
9.7.4 Viewing high-level summary metrics (graphical representation) for an application version 150
9.7.5 Exporting the Dashboard summary table 151
10 Managing user accounts 151
10.1 About tracking teams 151
10.2 About roles 151
10.2.1 Preconfigured roles 151
10.2.2 Creating custom roles 153
10.2.3 Deleting custom roles 154
10.3 Account administration 154
10.3.1 Creating local user accounts 154
10.3.2 Editing local user accounts 156
10.3.3 Unlocking local user accounts 158
10.3.4 Viewing externally managed users and groups 158
11 Applications and application versions 159
11.1 About tracking development teams 159

11.1.1 About the application creation process 160
11.1.2 Strategies for creating application versions 160
11.1.2.1 Strategies for packaged software 160
11.1.2.2 Strategies for continuous deployment 160
11.1.3 About annotating application versions for reporting 160
11.2 About creating application versions 161
11.2.1 Application version attributes 161
11.2.1.1 Creating custom attributes 162
11.2.1.2 Deleting attributes and attribute values 165
11.2.1.3 Applying new custom attributes to application versions 166
11.2.2 About issue templates 167
11.2.2.1 Adding issue templates to the system 167
11.2.2.2 Template selection 168
11.2.3 Creating the first version of a new application 168
11.2.4 Adding a new version to an application 172
11.3 Viewing application versions 175
11.4 Saving application view 177
11.5 Searching applications and application versions from the Applications view 178
11.6 Recalculating application metrics 179
11.7 Editing application version details 180
11.8 Exporting selected data for an application version 180
11.9 Using bug tracking systems to help manage security vulnerabilities 180
11.9.1 Bug tracker configuration 181
11.9.2 Velocity templates for bug filing 181
11.9.2.1 Adding Velocity Templates to Bug Tracker Plugins 181
11.9.2.2 Customizing Velocity templates for bug tracker plugins 182
11.9.2.3 Deleting Velocity templates 183
11.9.3 Assigning a bug tracking system to an application version 184
11.9.4 Submitting a bug for a single issue 184
11.9.5 Submitting a bug for multiple issues 185
11.9.6 Bug state management 186
11.10 Changing the template associated with an application version 186
11.11 Setting analysis result processing rules for application versions 187
11.12 Configuring Fortify Audit Assistant options for an application version 192
11.13 Enabling auto-apply and auto-predict for an application version 192
11.14 About custom tags 193
11.14.1 Adding custom tags to the system 194
11.14.2 Modifying custom tag attributes 195
11.14.3 Globally hiding custom tags 195
11.14.4 Deleting custom tags 196
11.14.5 Adding custom tag values 196
11.14.5.1 Add a custom tag value (Fortify Audit Assistant configured) 196
11.14.5.2 Setting the Issue State 198
11.14.6 Editing custom tags 199
11.14.7 Deleting custom tag values 199

11.14.8 Associating custom tags with issue templates 199
11.14.9 Removing custom tags from issue templates 200
11.14.10 Assigning custom tags to application versions 200
11.14.11 Disassociating a custom tag from an application version 201
11.14.12 Managing custom tags through issue templates 201
11.14.13 Managing custom tags through an issue template in an FPR file 202
11.15 About deleting application versions 202
11.15.1 Deactivating application versions 202
11.15.2 Reactivating application versions 202
11.15.3 Deleting an application version 203
12 About webhooks 203
12.1 Webhooks permissions 204
12.2 Creating webhooks 204
12.3 Editing webhooks 207
12.4 Viewing webhook payloads 208
12.5 Redelivering webhook payloads 209
12.6 Deleting webhooks 209
13 Variables, performance indicators, and alerts 209
13.1 Creating variables 210
13.1.1 Variable syntax 210
13.2 Creating performance indicators 211
13.3 Creating alerts 212
13.3.1 Editing alerts 214
13.3.2 Deleting alerts 214
13.4 Viewing and marking alerts 214
14 Working with scan artifacts 215
14.1 Uploading scan artifacts 215
14.2 Viewing scan artifact details 216
14.3 Downloading analysis results 218
14.4 Approving analysis results for an application version 218
14.5 Viewing issue metadata 219
14.6 Mapping analysis results to external lists 220
14.7 Purging scan artifacts 220
14.8 Deleting artifacts 221
15 Working with Aviator auto-remediation results 222
16 Collaborative auditing 223
16.1 Viewing high-level summary metrics for an application version 223
16.2 About current issues state 224
16.3 Viewing information about issues to audit 224
16.3.1 Viewing issues based on folders 225
16.3.2 Viewing issues assigned to you 226
16.4 Filtering issues for display 227
16.5 Searching issues 228
16.5.1 Search modifiers 229
16.5.2 Search query examples 232

16.6 Searching globally 233
16.7 Auditing analysis results 234
16.7.1 Auditing correlated issues 238
16.7.2 About suppressed, removed, and hidden issues 239
16.7.2.1 Setting issue viewing preferences 240
16.7.3 Changing displayed issues using filter sets 241
16.7.4 Overriding assigned issue priority 241
16.7.5 Viewing bugs submitted for issues 244
16.7.6 Auditing a batch of issues 244
16.8 Using Fortify Audit Assistant with Application Security 245
16.8.1 Consistent use of tags 246
16.8.2 Mapping Fortify Audit Assistant analysis tag values to Application Security custom tag values 246
16.8.3 About setting prediction policies 248
16.8.4 Fortify Audit Assistant workflow 248
16.8.5 Reviewing Fortify Audit Assistant results 249
16.8.6 About Fortify Audit Assistant training 250
16.8.6.1 Train your model using decisions your auditors make 251
16.8.6.2 Selecting a Fortify Audit Assistant training tag 251
16.8.6.3 Submitting training data to Fortify Audit Assistant 251
16.9 Exporting open source data 252
16.10 Integrating Application Security with Fortify WebInspect Enterprise 252
16.10.1 Viewing OpenText DAST analysis results in Application Security 252
16.10.2 OpenText DAST audit data 254
16.10.3 False positives 254
16.10.4 Submitting dynamic scan requests to Fortify WebInspect Enterprise 254
16.10.5 Processing dynamic scan requests from Fortify WebInspect Enterprise 255
16.10.6 Editing and canceling dynamic scan requests 256
16.11 Viewing open source data 257
16.12 Downloading an OpenText Core SCA (Debricked) software bill of materials 258
17 Working with OpenText ScanCentral DAST 259
17.1 OpenText ScanCentral DAST permissions 259
17.2 Submitting requests for dynamic scans to OpenText ScanCentral DAST 261
17.3 Synchronizing audit history changes in OpenText ScanCentral DAST using Kafka 261
18 Working with Fortify ScanCentral SAST 261
18.1 Fortify ScanCentral SAST permissions 262
18.2 Viewing Fortify ScanCentral SAST scan request details 263
18.3 Prioritizing a Fortify ScanCentral SAST scan request 263
18.4 Canceling Fortify ScanCentral SAST scan requests 264
18.5 Viewing Fortify ScanCentral SAST sensor information 264
18.6 Viewing Fortify ScanCentral SAST Controller information 264
18.6.1 Stopping the Controller 265
18.6.2 Placing the Controller in maintenance mode 265
18.6.3 Safely shutting down Fortify ScanCentral SAST sensors 265
18.6.4 Removing the Controller from maintenance mode 266
18.7 About Fortify ScanCentral SAST sensor pools 266

18.7.1 Creating Fortify ScanCentral SAST sensor pools 267
18.7.2 Moving sensors between pools 268
18.7.3 Deleting Fortify ScanCentral SAST sensor pools 268
19 BIRT reports 269
19.1 BIRT libraries 269
19.2 Importing report libraries 269
19.3 Generating and downloading reports 270
19.4 Generating and downloading customized BIRT reports in XLSX 271
19.5 Customizing BIRT reports 271
19.6 Acquiring the BIRT Report Designer 272
19.7 Downloading report templates 272
19.8 Importing report definitions 272
20 Authentication tokens 273
20.1 Authentication token types 274
20.2 Generating authentication tokens 276
20.3 Editing authentication tokens 277
20.4 Deleting authentication tokens 277
21 Fortify CLI (fcli) documentation 277
22 Using the fortifyclient utility 278
22.1 Preparing to use fortifyclient 278
22.1.1 fortifyclient HTTP timeouts 278
22.2 Listing fortifyclient commands and options 279
22.3 Generating an authentication token from the command line 279
22.3.1 Specifying the number of days before a token expires 279
22.4 Listing authentication tokens 280
22.5 Invalidating tokens 280
22.6 Listing application versions 280
22.7 Uploading FPR files 281
22.8 Downloading FPR files 281
22.9 Purging application version artifacts 282
22.10 Importing content bundles 282
22.11 Downloading audit attachment files 282
23 Authoring bug tracker plugins 282
23.1 Use case 283
23.2 Component setup 283
23.3 Implementation 284
23.4 Plugin methods and method calls 284
23.5 Plugin helper 289
23.6 Error handling 289
23.7 Almost stateless 289
23.8 Debugging a bug tracker plugin 290
23.9 Deploying a customized bug tracker plugin 290
24 Advanced configuration 291
24.1 Automating Application Security configuration 291
24.1.1 Automating configuration in a root context 293

24.2 Application configuration options 294
24.2.1 Configuring background job execution strategy 296
25 Webhook payloads 297
25.1 Event payloads 298
25.2 Artifact upload payload 298
25.3 Project version payload 299
25.4 Report generation payload 301
25.5 User payload 301

Application Security

Software Version: 26.4.0

Document Release Date: November 2026

Software Release Date: November 2026

1. Change log

The following table lists changes made to this document. Revisions to this document are published between software releases only if the changes made affect product functionality.

Software release / Document revision	Changes
26.4.0	Added: • Added guidance for enabling console log mirroring by setting `COM_FORTIFY_SSC_LOG_CONSOLE=true` (see Configuring logging) • Managing Fortify Object Storage • Added support for SMTP server using OAuth 2.0 authentication mechanism (see Configuring email alert notification settings) • Added instructions for configuring the initial `admin` email address and password on the new `ADMIN ACCOUNT` page in the Setup wizard (See Configuring Application Security for the first time) Updated: • For a new installation, the default `admin` user account is no longer seeded with a hardcoded password. You must provide the initial password and email address for the `admin` account using the `init.admin.password` and `init.admin.email` autoconfig properties, or through the Setup wizard (see Automating Application Security configuration, Automating configuration in a root context, Application configuration options, and About seeding the Application Security database). Upgrades with an existing admin account are unaffected. • Information about password strength requirements and the **zxcvbn4j** library used to evaluate password strength (see Setting the required password strength for Application Security sign in) • Instructions for signing in for the first time now reference the initial `admin` password that you configure, instead of the default `admin` / `admin` credentials (see Signing in to Application Security for the first time) • Ability to see the status message tooltip and the information when you expand the scan request details (see Viewing OpenText ScanCentral SAST scan request details) • Described configurable global file-count and line-count percentages (see Setting analysis result processing rules for application versions)

26.2.0	Added: • Overview page in Dashboard view • Configuring AI Assistant • Configuring Aviator • Working with Aviator auto-remediation results • Default values of `sql-mode` (see Using a MySQL database) • Upgrade Lucene • Updated: • Using a MySQL database • `fortifyclient` has been deprecated (see Using the fortifyclient utility) Removed: • CE mark from the Login screen, masthead, and the About Screen of Application Security has been removed.
25.4.0	Added: • Support to verify the IdP metadata signature using the IdP's public key (X.509 certificate) (see Configuring SAML 2.0-compliant single sign-on) • Saving application view • Fortify CLI (fcli) documentation • A ScanCentral DAST Controller role in Preconfigured roles Updated: • Instructions of Partitioning an Oracle database for improved performance • Improved **Applications** view (see Viewing application versions) • Introduction of a new **Filters** option for **Your Versions** (see Searching applications and application versions from the Applications view)

25.2.0	Added: • System requirements • Automating configuration in a root context Updated: • Incorporated product name changes (see Product name changes) • The location for plugin log files has changed (see Directory contents) • Introduction of an improved modern **Applications** view (see Viewing application versions) • Application version processing rules for if the file count or line count increases or decreases by 10% (see Setting analysis results processing rules for application versions) • The **Analysis Type** column in the **AUDIT** page issues table and the **ARTIFACT HISTORY** table displays the analysis type of SAST or DAST for product rebranding (see Viewing information about issues to audit and Viewing scan artifact details) • Improved display and filtering of OpenText Fortify ScanCentral SAST analysis results (see Viewing OpenText Fortify ScanCentral SAST scan request details) Removed: • The topic about enabling Java Security manager was removed because it is no longer supported • Content for Kerberos/SPNEGO and CAS single sign-on solutions because they are no longer supported • Job execution strategies from the job scheduler configuration • All references to the Dashboard technology preview implemented with Magellan BI and Reporting have been removed. This feature is deprecated and is not planned for a future release.
24.4.0 / Revision 1: November 2024	Updated: • Added information about the service account required to integrate with OpenText Fortify ScanCentral DAST (see Enabling the running and management of OpenText Fortify ScanCentral DAST scans)

24.4.0	Added: • Administrators can implement Magellan BI and Reporting dashboards for a comprehensive application security program overview, and insight into important vulnerability metrics. Because this feature is released as a technology preview, report any omissions, issues, or gaps in functionality so that we can address them prior to the next release. • Ability to review the issue history for an audit (see About audit issue history) • A OpenText Fortify ScanCentral SAST Controller role in Preconfigured roles and User account types. • Configuring logging • Migration of keystore file Updated: • Running in a Federal Information Processing Standards (FIPS) environment • The description for the `secret.key` parameter (see <fortify.home> directory contents) Removed: • Topics Changing Log Levels for Fortify Software Security Center and Customizing Fortify Software Security Center Logging are removed and replaced with Configuring logging • The topic About Susceptibility Analysis of Web Applications was removed as Fortify SourceAndLibScanner is deprecated

24.2.0	Added: • Ability for Administrators to enable a data retention policy that defines the time period for retaining application version artifacts (see About data retention) • Instructions for changing the UI theme (see Setting preferences system-wide and across application versions) • Instructions on how to download customized BIRT reports in XLSX format (see Generating and downloading customized BIRT reports in XLSX) • Ability to set up Kafka to synchronize audit history changes for suppressed issues, priority override, and analysis tag with OpenText Fortify ScanCentral DAST (see Synchronizing audit history changes in OpenText Fortify ScanCentral DAST using Kafka, and Configuring a Kafka Stream to use with OpenText Fortify ScanCentral DAST) • Ability to set up timeouts for connect, read, and write for `fortifyclient` (see fortifyclient HTTP timeouts) Updated: • Added an informational note to Monitoring disk I/O • The default schedule for LDAP Refresh (see Recurring Cleanup Jobs) • Modified the IdP metadata location and keystore location (see Configuring Application Security to Work with SAML 2.0-Compliant Single Sign-On) • Updated the list of supported operators (see Creating performance indicators) • Added a description for the Issue State (see Setting the Issue State) • Changed the default job execution strategy to Flexible (see Configuring Job Scheduler Settings) Removed: • The `activity`, `requirement`, and `requirementtemplate` table names from Configuring Security for BIRT Reporting • The authentication token of type AuditToken • All mentions of the Bug Tracker Plugin for Bugzilla

2. Introduction

OpenText™ Application Security is a browser-based application 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 available from the following products:

- OpenText™ Static Application Security Testing (OpenText Fortify SAST)

- OpenText™ Fortify ScanCentral SAST
- OpenText™ Fortify ScanCentral DAST
- Fortify WebInspect Enterprise
- OpenText™ Fortify Software Composition Analysis (OpenText Fortify SCA)
- Sonatype

Application Security provides:

- Security team leads with a high-level overview of the history and current status of an application. Your security team can then ensure that both developers and auditors work effectively together to provide the best response to application issues.
- Auditors with a centralized facility for managing issues. If the manager needs to work offline or with the advanced tools that OpenText™ Fortify Audit Workbench offers, current application state, and up-to-date auditing information are made available for download.
- Managers with the ability to prioritize issues to reflect the needs of the enterprise. That prioritization can then be used to prioritize the activities of the application development team.
- Developers with a focal point for managing and transmitting information about specific issues received from analysis agents to supported Integrated Development Environments (IDEs), or to standalone clients such as Fortify Audit Workbench. Developers can then use the application snapshots to measure their progress through the secure development life cycle.

This section contains the following topics:

- Product name changes
- Audience
- Related documents

2.1. Product name changes

OpenText is in the process of changing the following product names:

Previous name	New name
Fortify Static Code Analyzer	OpenText™ Static Application Security Testing (OpenText Fortify SAST)
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	OpenText™ Dynamic Application Security Testing (OpenText Fortify DAST)
Fortify on Demand	OpenText™ Fortify on Demand
Debricked	OpenText™ Fortify Software Composition Analysis (OpenText Fortify SCA)
Fortify Applications and Tools	OpenText™ Application Security Tools

The product names have changed on product splash pages, mastheads, login pages, and other places where the product is identified. The name changes are intended to clarify product functionality and to better align the Fortify Software products with OpenText. In some cases, such as on the documentation title page, the old name might temporarily be included in parenthesis. You can expect to see more changes in future product releases.

2.2. Audience

The information presented in this guide is for administrators (who are responsible for deploying and maintaining Application Security), enterprise security leads, auditors, development team managers, and developers.

The content for Application Security deployment, configuration, and maintenance is for administrators who are moderately knowledgeable about enterprise application development and skilled in enterprise system and database administration. For information about how to access the Application Security API documentation, see Accessing the API documentation.

Document structure

This document is presented in two main parts. The first part includes topics that describe how to deploy and configure Application Security starting with Providing for secure deployment. The second part describes how to use Application Security starting with Using Application Security.

2.3. Related documents

ADD this topic to the end of your Chapter 1 in the TOC. This topic uses the Product_Conditions tag set to include the "All Products" section and the section of content for your specific product. You do not need to customize this topic unless you need to add a Technical Note or Technology Preview for your product. For example, to produce the WebInspect User Guide, the WebInspect writer does not currently need to make any changes. However, if the writer needed to add a Technology Preview, he would add it to the table and tag it with the WebInspect Product_Conditions tag. For more information about how to use this topic, see the article on OneNote at MadCap Flare > Templates and SFFS > Related Documents Topic.

This topic describes documents that provide information about OpenText Application Security Software products.

Note

You can find the Application Security Product Documentation at https://www.microfocus.com/support/documentation. Most guides are available in both PDF and HTML formats. Product help is available within the Fortify License and Infrastructure Manager (LIM) and the OpenText Fortify DAST products.

All products

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

Document / file name	Description
About OpenText Application Security Software Documentation appsec-docs-n-<*version*>.pdf	This paper provides information about how to access OpenText Application Security Software product documentation. **Note** This document is included only with the product download.
OpenText™ Application Security Software System Requirements appsec-sr-<*version*>.pdf	This document provides the details about the environments and products supported for this version of OpenText Application Security Software.
What's New in OpenText Application Security Software <version> appsec-wn-<*version*>.pdf	This document describes the new features in OpenText Application Security Software products.
OpenText Application Security Software Release Notes appsec-rn-<version>.pdf	This document provides an overview of the changes made to OpenText Application Security Software for this release and important information not included elsewhere in the product documentation.

OpenText Fortify ScanCentral DAST

The following document provides information about OpenText Fortify ScanCentral DAST. These documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-ScanCentral-DAST.

Document / file name	Description
OpenText™ Fortify ScanCentral DAST Configuration and Usage Guide sc-dast-ugd-<*version*>.pdf	This document provides information about how to configure and use OpenText Fortify ScanCentral DAST to conduct dynamic scans of Web applications.
OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide lim-ugd-<*version*>.pdf	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.
OpenText™ Dynamic Application Security Testing and OAST on Docker User Guide dast-docker-ugd-<*version*>.pdf	This document describes how to download, configure, and use OpenText Fortify DAST and Fortify OAST that are available as container images on the Docker platform. The OpenText Fortify DAST image is intended to be used in automated processes as a headless sensor configured by way of the command line interface (CLI) or the application programming interface (API). It can also be run as an OpenText Fortify ScanCentral DAST sensor and used in conjunction with Application Security. Fortify OAST is an out-of-band application security testing (OAST) server that provides DNS, SMTP, and HTTP/HTTPS services for the detection of OAST vulnerabilities.

OpenText Fortify ScanCentral SAST

The following document provides information about OpenText Fortify ScanCentral SAST. This document is available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center.

Document / file name	Description
OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide sc-sast-ugd-<*version*>.pdf	This document provides information about how to install, configure, and use OpenText Fortify ScanCentral SAST to streamline the static code analysis process. It is written for anyone who intends to install, configure, or use OpenText Fortify ScanCentral SAST to offload the resource-intensive translation and scanning phases of their OpenText Fortify SAST process.

Application Security

The following document provides information about Application Security. This document is available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center.

Document / file name	Description
OpenText™ Application Security User Guide ssc-ugd-<*version*>.pdf	This document provides Application Security users with detailed information about how to deploy and use Application Security. It provides all the information you need to deploy, configure, and use Application Security. It is intended for use by system and instance administrators, database administrators (DBAs), enterprise security leads, development team managers, and developers. Application Security provides security team leads with a high-level overview of the history and status of a project.

OpenText Fortify SAST

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

Document / file name	Description
OpenText™ Static Application Security Testing User Guide sast-ugd-<*version*>.pdf	This document describes how to install and use OpenText Fortify SAST to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding.
OpenText™ Static Application Security Testing Custom Rules Guide sast-cr-ugd-<*version*>.zip	This document provides the information that you need to create custom rules for OpenText Fortify SAST. This guide includes examples that apply rule-writing concepts to real-world security issues. **Note** This document is included only with the product download.
OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide lim-ugd-<*version*>.pdf	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.

OpenText Application Security Tools

The following documents provide information about OpenText Application Security Tools. These documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools.

Document / file name	Description
OpenText™ Application Security Tools Guide sast-tgd-<*version*>.pdf	This document describes how to install application security tools. It provides an overview of the applications and command-line tools that enable you to scan your code with OpenText Fortify SAST, review analysis results, work with analysis results files, and more.
OpenText™ Fortify Audit Workbench User Guide awb-ugd-<*version*>.pdf	This document describes how to use Fortify Audit Workbench to scan software projects and audit analysis results. This guide also includes how to integrate with bug trackers, produce reports, and perform collaborative auditing.
OpenText™ Fortify Plugin for Eclipse User Guide ep-udg-<*version*>.pdf	This document provides information about how to install and use the Fortify Plugin for Eclipse to analyze and audit your code.
OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio User Guide iap-udg-<*version*>.pdf	This document describes how to install and use the Fortify Analysis Plugin for IntelliJ IDEA and Android Studio to analyze your code and optionally upload the results to Application Security.
OpenText™ Fortify Extension for Visual Studio User Guide vse-ugd-<*version*>.pdf	This document provides information about how to install and use the Fortify Extension for Visual Studio to analyze, audit, and remediate your code to resolve security-related issues in solutions and projects.

OpenText Fortify DAST

The following documents provide information about OpenText Fortify DAST (Fortify WebInspect). These documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-webinspect.

Document / file name	Description
OpenText™ Dynamic Application Security Testing Installation Guide dast-igd-<*version*>.pdf	This document provides an overview of OpenText Fortify DAST and instructions for installing and activating the product license.
OpenText™ Dynamic Application Security Testing User Guide dast-ugd-<*version*>.pdf	This document describes how to configure and use OpenText Fortify DAST to scan and analyze Web applications and Web services. **Note** This document is a PDF version of the OpenText Fortify DAST 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.
OpenText™ Dynamic Application Security Testing and OAST on Docker User Guide dast-docker-ugd-<*version*>.pdf	This document describes how to download, configure, and use OpenText Fortify DAST and Fortify OAST that are available as container images on the Docker platform. The OpenText Fortify DAST image is intended to be used in automated processes as a headless sensor configured by way of the command line interface (CLI) or the application programming interface (API). It can also be run as an OpenText Fortify ScanCentral DAST sensor and used in conjunction with Application Security. Fortify OAST is an out-of-band application security testing (OAST) server that provides DNS, SMTP, and HTTP/HTTPS services for the detection of OAST vulnerabilities.
OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide lim-ugd-<*version*>.pdf	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.
OpenText™ Dynamic Application Security Testing Tools Guide dast-tgd-<*version*>.pdf	This document describes how to use the OpenText Fortify DAST diagnostic and penetration testing tools and configuration utilities packaged with OpenText Fortify DAST and Fortify WebInspect Enterprise.

OpenText™ Dynamic Application Security Testing Agent Installation and Rulepack Guide dast-agent-igd-<*version*>.pdf	This document describes how to install the OpenText DAST Agent and describes the detection capabilities of the OpenText DAST Agent Rulepack Kit. OpenText DAST Agent Rulepack Kit runs atop the OpenText DAST Agent, allowing it to monitor your code for software security vulnerabilities as it runs. OpenText DAST Agent Rulepack Kit provides the runtime technology to help connect your dynamic results to your static ones.

Fortify WebInspect Enterprise

The following documents provide information about Fortify WebInspect Enterprise. These documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-webinspect-enterprise.

Document / file name	Description
OpenText™ Fortify WebInspect Enterprise Installation and Implementation Guide WIE_Install_<*version*>.pdf	This document provides an overview of Fortify WebInspect Enterprise and instructions for installing Fortify WebInspect Enterprise, integrating it with Application Security and OpenText Fortify DAST, 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.
OpenText™ Fortify WebInspect Enterprise User Guide WIE_Guide_<*version*>.pdf	This document describes how to use Fortify WebInspect Enterprise to manage a distributed network of OpenText Fortify DAST sensors to scan and analyze Web applications and Web services. **Note** 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 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.
OpenText™ Dynamic Application Security Testing Tools Guide dast-tgd-<*version*>.pdf	This document describes how to use the OpenText Fortify DAST diagnostic and penetration testing tools and configuration utilities packaged with OpenText Fortify DAST and Fortify WebInspect Enterprise.

3. Providing for secure deployment

Just as you apply security precautions to analyzed source code, you must also secure access to the OpenText Application Security Software analysis products that access the source code. Moreover, the concentrated summarization of security vulnerabilities that the OpenText Application Security Software products provide might mandate an even higher level of secure deployment. The topics in this section describe some of the ways to securely deploy Application Security.

This section contains the following topics:

- Securing access to facilities
- Securing Tomcat server
- Setting Tomcat server attributes to protect sensitive data in cookies
- Using HTTPS and SSL communications
- About securing passwords and user roles
- Managing computer services and accounts

3.1. Securing access to facilities

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

3.2. Securing Tomcat server

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

Using secure cipher suites

OpenText recommends that you use secure SSL/TLS cipher suites in Tomcat.

- APR-based SSL connections
  Use the SSLCipherSuite directive. For detailed information, see the SSL CipherSuite Directive and Cipher Suites and Enforcing Strong Security.
- JSSE-based SSL connections
  Use the `ciphers` and the `honorCipherOrder` attributes. For details, go to the Apache Tomcat 10 Configuration Reference - The HTTP Connector.

Because of trade-offs between improved security and improved interoperability, better performance, and so on, there is no correct cipher suite choice. However, Apache provides information that can help you make your choice in the Apache Tomcat Ciphers documentation.

3.3. 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, OpenText recommends that you add the following attributes 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. OpenText 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.

3.4. Using HTTPS and SSL communications

OpenText strongly recommends that you configure Application Security and OpenText Application Security Software client products (including Fortify Audit Workbench, fortifyclient, and the Secure Code Plugins) to use HTTPS and Secure Sockets Layer (SSL) for all communications.

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 Application Security. The certificate is trusted because these root CA certificates are in the keystore that OpenText Application Security Software client products use.

However, by default, Application Security, OpenText Application Security Tools, and the fortifyclient utility 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 Application Security, 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, ensure 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 Application Security and OpenText Application Security 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 "<tools_install_dir>/jre/bin"
  keytool -importcert -alias SSC -keystore ../lib/security/cacerts -file
  "YourCertFile.cer" -trustcacerts
  ```

  where
  - *<tools_install_dir>* is the installation directory for the OpenText Application Security Tools
  - `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 Tomcat server uses, as follows:

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

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

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 Application Security. Do not simply use the short hostname or `localhost`.

When you create a connector in the `server.xml` file for HTTPS, ensure 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.

3.5. About securing passwords and user roles

After you deploy Application Security and sign in for the first time, you can create additional local administrator accounts as appropriate for your environment. Do not delete the pre-defined admin account

The account security features include:

- Ability for administrators to suspend accounts that have become temporarily inactive
- Automatic lock-out of accounts based on failed log-on attempts

If you are using LDAP to authenticate Application Security users, configure your LDAP server to use secure LDAP communications.

See also

Signing in to Application Security

Managing user accounts

LDAP user authentication

3.6. Managing computer services and accounts

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

4. Deploying Application Security

This chaptercontent describes how to prepare for and deploy Application Security for the first time.

This section contains the following topics:

- Deployment overview
- High-level deployment tasks
- Downloading and unpacking Application Security files
- About the Application Security database
- About deploying Application Security in Kubernetes
- About the directory

4.1. Deployment overview

Application Security is packaged as a Web Archive (WAR) file. It runs in Tomcat server and requires a supported third-party database.

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

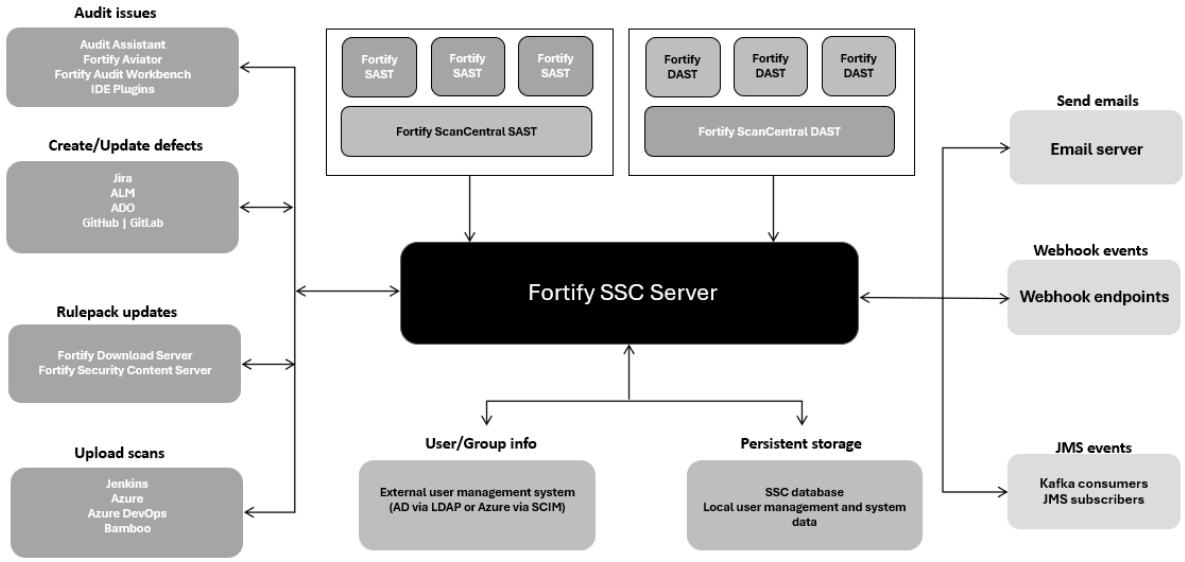


Tip

Advanced users only. Instead of using the Setup wizard, you can set up an autoconfig file before you deploy Application Security to automate the configuration. After you do, the Setup wizard retrieves your configuration settings at server startup and automates the configuration. For instructions on how to set up the automatic configuration, see Automating Application Security configuration.

For system requirements information, see the *OpenText™ Application Security Software System Requirements* document.

The following figure illustrates the interoperability of the Application Security with the required and optional components, providing centralized management.



The following table describes components in the illustration.

Component	Description
Required components	
Application Security	Application Security is delivered as a Web Archive (WAR) file run by Tomcat server or as a Helm chart for Kubernetes deployment.
Application Security database	Database to store user and artifact data. Before you put Application Security into production, you must install a supported third-party database. **Important** You must not deploy multiple Application Security instances that share the same database schema. Ensure each Application Security instance operates with its own dedicated database schema to maintain data integrity.
Rulepack update server	Server used to acquire and update OpenText SAST Application Security Content.
Application Security Customer Portal	Server used to acquire off-cycle seed bundles and quarterly OpenText SAST Application Security Content releases.
Optional components	
OpenText Fortify SAST (Fortify Static Code Analyzer)	OpenText Fortify SAST scans source code and identifies issues.
OpenText Fortify ScanCentral SAST	OpenText Fortify SAST users can use OpenText Fortify ScanCentral SAST to offload processor-intensive code analysis tasks from their build machines to a group of machines (sensors) provided for this purpose.
OpenText Fortify DAST (Fortify WebInspect)	Analysis agent that connects with OpenText DAST Agents to retrieve potential dynamic issues.
OpenText Fortify ScanCentral DAST	Tool that enables you to configure and run dynamic scans of your web applications with OpenText Fortify DAST from Application Security.
Fortify Audit Workbench and Secure Code Plugins	Tools to collaboratively audit analysis results on Application Security. These tools can also scan source code and upload analysis results.

Component	Description
Jenkins Plugin Azure DevOps Extension	Plugins to scan source code with OpenText Fortify SAST and upload analysis results.
Defect tracking server	Defect tracking server for bug submission directly to Jira, ALM, Azure DevOps Server, or a customized bug tracking system. For information about how to create a customized bug tracking system, see Authoring bug tracker plugins.
Parser plugin	Plugins to enable display of open source security data from OpenText Fortify SCA (Debricked) and Sonatype. You can also connect third-party parser plugins.
Email server	Third-party SMTP email server to send alerts to application collaborators.
Third-party LDAP authentication server	External user management system to use LDAP authentication.
Kubernetes	Container orchestration platform supported for Application Security deployment.

4.2. High-level deployment tasks

The following table lists the high-level tasks you need to perform for Application Security deployment.



Note

If you are upgrading Application Security, see Upgrading Application Security.

Task	Description	Information and instructions
Preparing for deployment and initial configuration Gather the distribution file, license file, the database credentials, and seed bundles required for deployment and the initial configuration.		
1	Download the installation package and the `fortify.license` file.	Downloading and unpacking Application Security files
2	Install and configure the database server software you plan to use.	About the Application Security database
3	(Optional for advanced users only) Set up an autoconfig file before you deploy Application Security to automate the deployment and configuration.	Automating Application Security configuration
Deploying in Tomcat server		
4	Deploy Application Security in Tomcat server.	Copy the WAR file to the `<tomcat>/webapps/` directory and start Tomcat server.
Performing the initial configuration		
5	Perform the initial configuration (provide the license file, create the database tables, initialize the database schema, configure some core settings, seed the database, and so on).	There are two ways to do this: • Use the Setup wizard to perform the initial configuration Configuring Application Security for the first time • *Advanced users only* Automatic initial configuration Automating Application Security configuration
6	Sign into Application Security for the first time to set up a non-default Administrator account.	Signing in to Application Security
7	Complete the core configuration settings such as configuring single sign-on, administering users, registering LDAP entities, managing LDAP user roles, and creating custom attributes that users can assign to their applications.	Additional Application Security configuration

Task	Description	Information and instructions
8	Perform additional tasks such as setting up bug tracking integration, managing parser plugins, user account administration, and updating security content.	Additional installation-related tasks

4.3. Downloading and unpacking Application Security files

Acquire the installation package and the `fortify.license` file from the Software Licenses and Downloads (SLD) portal. A helpful how-to video on YouTube™, OpenText Software Fulfillment Training playlist, also provides instructions on how to download OpenText Application Security Software.

To unpack the Application Security installation files:

1. Extract the contents of the installation package into a temporary directory in a secure location.
2. Locate the distribution file (`Fortify_<version>_Server_WAR_Tomcat.zip`) and extract all the contents into a directory in a secure location.
   This includes the `ssc.war` file, which contains the resources and tools you need for tasks such as configuring Application Security 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_distribution_dir>* directory.

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

   Note
   Although you are not required to copy the resource files to the *<ssc_distribution_dir>* directory, the procedures in this document assume that you saved the files to that location.

   The seed bundles are described in the following table.

Seed bundle file name	Description
Fortify_Process_Seed_Bundle-2025_Q2_<*build*>.zip	Process template seed bundle used to seed database tables. It provides a default admin user account and issue template data.
Fortify_Report_Seed_Bundle-2025_Q2_<*build*>.zip	Report seed bundle used to seed database tables. It provides the default set of reports.
Fortify_PCI_Basic_Seed_Bundle-2025_Q2_<*build*>.zip	(Optional) The PCI basic seed bundle adds a Payment Card Industry (PCI) Data Security Standard (DSS) process template and its associated report to the default set of issue templates and reports. After October 2022, the PCI Software Security Framework (SSF) became the standard for evaluation. Use the PCI SSF basic seed bundle to learn how software security issues can affect evaluation under the PCI SSF standards.
Fortify_PCI_SSF_Basic_Seed_Bundle-2025_Q2_<*build*>.zip	(Optional) The PCI SSF basic seed bundle adds a Payment Card Industry (PCI) Software Security Framework (SSF) process template and its associated report to the default set of issue templates and reports. PCI SSF was introduced in June 2019 as a set of new standards to evaluate systems developed by payment software vendors. After October 2022, the PCI Software Security Framework (SSF) became the standard for evaluation. Use the PCI basic seed bundle for evaluation under PCI DSS.

4. Copy the `fortify.license` file to the <*ssc_distribution_dir*> directory.

See also

High-level deployment tasks

4.4. About the Application Security database

If you are deploying a new instance of Application Security, you must first install and configure the third-party database server software. For database requirements, see the *Application Security Software System Requirements* document.

Important

- requires that all database schema collations be *case-sensitive*.
- If you are installing a SQL Server or MySQL database, your installation requires special attention. For more information, see Using a SQL Server Database or Configuring a MySQL Database.

Later, when you configure Application Security for the first time, you will use the Setup wizard to configure connectivity to the database and then seed the database (see Configuring Application Security for the First Time).

This section contains the following topics:

- About JDBC drivers
- Installing and configuring the database server software
- Monitoring disk I/O
- Database user account permissions
- Database-specific configuration requirements

- About the Application Security database tables and schema
- About seeding the Application Security database
- Permanently deleting a Application Security database

4.4.1. About JDBC drivers

The JDBC drivers for SQL Server, MySQL server, and Oracle Database are bundled with Application Security software.

The MariaDB JDBC driver connects to the MySQL database server. JDBC URL parameters must use MariaDB driver syntax. Note that the MariaDB is not supported as a database for Application Security.

4.4.2. 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 *Application Security Software System Requirements* document.

4.4.3. Monitoring disk I/O

Disk I/O encompasses the input/output operations on a physical disk. If you are reading data from a file on a disk, the processor must wait for the file to be read (the same applies to writing data to a file). Application Security performs I/O-intensive database operations, which affect performance. Ensure that your disk subsystem provides low read/write latency.

Application Security object cleanup actions, such as application versions, artifacts, saved reports, data exports, event logs, and so on, might not result in actual reduction of database storage allocation until the database administrator re-optimizes the database. OpenText recommends regular monitoring and optimization of the Application Security databases.

4.4.4. Database user account permissions

OpenText strongly recommends that you create accounts for users who perform the following tasks on the Application Security database:

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

  > **Important**
  > OpenText strongly recommends that you create a separate user account for executing migration scripts.

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

  > **Important**
  > OpenText strongly recommends that you create a separate user account to create and manage the database.

  A user who creates and manages the database requires permission to do the following:
  - Perform all the tasks for which the user who executes migration scripts has permission

- Create a Application Security database in a dedicated instance
- Back up and then update the existing Application Security dedicated database instance
- Bind a Application Security user account to the dedicated database instance
- Assign a Application Security user account the read-write permission required to create, initialize, and manage the Application Security 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 Application Security database, and then use the account credentials to configure security for your BIRT reports (see Configuring Security for BIRT Reporting).

4.4.5. Database-specific configuration requirements

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

- Using a SQL server database
- Using a MySQL database
- Using an Oracle database

4.4.5.1. Using a SQL server database

To use SQL Server as the Application Security database, perform the following checks:

- Enable the Auto Update Stats Asynchronously (`AUTO_UPDATE_STATISTICS_ASYNC`) option for the database.
  For instructions, see the Microsoft SQL documentation website.
- Ensure that your SQL Server database schema collation is *case-sensitive*. The default installation of SQL Server is *case-insensitive*.

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

- Ensure 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 ensure that its ANSI null default option is set to `ON` .
  To do this, you can either use a `SET` command (set `ANSI_NULL_DFLT_ON` to `ON`) or the Query Editor.

Windows domain authentication

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

1. Ensure that you add `integratedSecurity=true` to the JDBC URL.
2. Obtain the `mssql-jdbc_auth-<version>-<arch>.dll` file.
   For more information, see Connecting with integrated authentication On Windows Microsoft documentation.
3. Place the `mssql-jdbc_auth-<version>-<arch>.dll` file in the directory specified for the `-Djava.library.path` parameter of the `JDK_JAVA_OPTIONS` environment variable.
4. Place the `mssql-jdbc_auth-<version>-<arch>.dll` file in a directory that is included in the `PATH` environment variable (for example, `C:\Windows\System32`).
5. Do one of the following:
   - Use the autoconfig file to configure Application Security (see Automating Application Security configuration).
   - Configure Application Security with SQL authentication, and then remove the `db.username` and `db.password` parameters from the `datasource.properties` file.
6. Ensure that Tomcat is running with the domain account you want to use to connect to the database.

4.4.5.2. Using a MySQL database

Important

MySQL 8.0 is supported up to 25.4 release. Starting with 26.2 release, the supported database version is MySQL 8.4. For migration procedures, see Migrating from MySQL 8.0 to MySQL 8.4.

To use MySQL as the Application Security database, you must configure the MySQL options file. For information about the supported versions of MySQL, see the *Application Security Software System Requirements* document.

Caution

requires that all database schema collations be *case-sensitive*. If your installation is *case-insensitive*, Application Security does not work correctly.

Tip

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

To configure the MySQL 8.4 options file:

1. Stop MySQL server.
2. Go 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`.
   - 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 described in the following table. If a listed setting is not included in the file, add it.

Setting	Value
innodb_buffer_pool_size	512M (OpenText recommends 10GB or more) The best performance is achieved when all data and indexes fit. Together with per-connection memory, the innodb_lock_wait_timeout value must not exceed the total available memory on the server. You can estimate the maximum memory usage as follows: max_connections * max_allowed_packet + innodb_buffer_pool_size An innodb_buffer_pool_size value between 60 and 80 percent of available memory is appropriate. The larger the innodb_buffer_pool_size value, the less disk I/O is needed to access data in tables. On a dedicated database server, you can set this to up to 80% of the machine physical memory size. However, be prepared to scale back this value if you see any of the following: ○ Competition for physical memory causes paging in the operating system. ○ InnoDB reserves additional memory for buffers and control structures, so that the total allocated space is approximately 10% greater than the specified size. ○ The address space must be contiguous, which can cause problems on Windows systems with DLLs that load at specific addresses. ○ The time to initialize the buffer pool is proportional to its size. On large installations, this initialization time might be extensive. For example, on a modern Linux x86_64 server, initialization of a 10 GB buffer pool takes approximately 6 seconds. For more information, see the MySQL 8.4 Reference Manual.
innodb_lock_wait_timeout	300 (recommended) Expressed in seconds
max_allowed_packet	1073741824
sql-mode	"TRADITIONAL", this is equivalent to STRICT_TRANS_TABLES, STRICT_ALL_TABLES, NO_ZERO_IN_DATE, NO_ZERO_DATE, ERROR_FOR_DIVISION_BY_ZERO, and NO_ENGINE_SUBSTITUTION.
innodb_redo_log_capacity	1073741824 For more information, see the MySQL 8.4 Reference Manual.
log_bin_trust_function_creators	1

Additional settings applicable to Microsoft® Azure®

Setting	Value
sql_generate_invisible_primary_key	OFF
default_storage_engine	INNODB

Additional settings applicable to Amazon Web Services

Setting	Value
default_storage_engine	INNODB

Additional settings applicable to Google Cloud Platform™

Setting	Value
default_tmp_storage_engine	INNODB

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

Migrating from MySQL 8.0 to MySQL 8.4

You can migrate a MySQL 8.0 database to MySQL 8.4 using one of the following options.

Scenario 1

Upgrade from Application Security (version 24.4 onwards) with MySQL8.0

1. Stop the Tomcat server.
2. Delete the WAR file from the `<tomcat>/webapps/` directory, and then copy the new WAR file to the `<tomcat>/webapps/` directory.



Note

- `<tomcat>` represents the root directory of the Tomcat instance.
- The current Application Security version uses Tomcat10.1 and Java21. Ensure to upgrade Tomcat and Java to the required versions if older versions are used.

3. Start the Tomcat server.
4. Open a browser and type the Application Security web address to start the Setup wizard.
5. See Configuring Application Security after an upgrade for Upgrade.
6. After the 26.2 Application Security with MySQL 8.0 is up and running, verify that there are no errors in the logs.
7. Stop the Tomcat server.
8. Create a backup of the `datasource.properties` file under `<fortify Home Directory>/ssc/conf` and then remove the `datasource.properties` file.
9. Create an SQL dump of the MySQL 8.0 database (see the https://dev.mysql.com/doc/refman/8.0/en/mysqldump.html section).



Note

- Include the `--routines` and `--triggers` options when creating `mysqldump` to include all functions and procedures.
- Ensure to have a backup of the MySQL 8.0 dump in case you want to use the data when required.

10. On MySQL 8.4, import the dump to create the tables (see the https://dev.mysql.com/doc/refman/8.4/en/programs-client.html section).

> **Note**
> It is recommended to use the same username and database name in MySQL 8.4 as in MySQL 8.0.

11. Start the Tomcat server.
12. Open a browser and type the Application Security web address to start the Setup wizard.
13. See Configuring Application Security after an upgrade for upgrade and update the username, password, and JDBC URL for the MySQL 8.4 configuration.

Scenario 2

Upgrade from MySQL8.0 to MySQL8.4 for 26.2 Application Security

1. Stop the Tomcat server.
2. Delete the WAR file from the `<tomcat>/webapps/` directory, and then copy the new WAR file to the `<tomcat>/webapps/` directory.

   > **Note**
   > `<tomcat>` represents the root directory of the Tomcat instance.

3. Create an SQL dump of the MySQL 8.0 database (see the https://dev.mysql.com/doc/refman/8.0/en/mysqldump.html section).

   > **Note**
   > - Include the `--routines` and `--triggers` options during `mysqldump` to include all functions and procedures.
   > - Ensure to have a backup of the MySQL 8.0 dump in case you want to use that data.

4. Upgrade MySQL 8.0 to MySQL 8.4, update the configuration and server parameters, and restart the MySQL server.
5. Start the Tomcat server.
6. Open a browser and type the Application Security web address to start the Setup wizard.
7. See Configuring Application Security after an upgrade and update the configuration database for MySQL 8.4, if required.
8. Run the migration script on your database (see Preparing to run the database upgrade script).
   Databases containing more than 1 TB of data may take five or more hours to migrate.
9. Use the Setup wizard to reseed the database.

4.4.5.3. Using 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
- Partitioning an Oracle database for improved performance

4.4.5.3.1. Preventing the “No more data to read from socket” error

If you use Oracle as the Application Security 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. Go 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.

4.4.5.3.2. 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 can enhance database server performance, improving data manageability and availability.

Users are advised to work with their own DBAs to identify and implement database optimizations, including partitioning, best suited to their environment. OpenText does not validate or provide technical support for specific database optimizations or enhancements.

Before implementing database partitioning or other database optimizations, OpenText strongly recommends that you do the following:

1. Back up your database.
2. Test and validate any changes in a non-production environment before modifying your production database.

Though OpenText does not provide guidance for customer database optimizations when partitioning a database, ensure the following:

1. Number of partitions must allow for growth in your data.
2. Consider a record distribution of less than one million records per partition.
3. Partitioning a database can take time, ensure you allocate enough application downtime in order to partition the data.
4. After partitioning, consider increasing the number of job execution threads for optimization.
    1. Job execution threads are configured in the `<fortify.home>/<app_context>/conf/app.properties` file by the `jobs.threadCount` property.
5. Partition optimizations have the possibility of conflicting with migrations scripts. In those cases, the customer's DBA may need to manually adjust the migration scripts and/or partition scripts to work with any applied optimizations during upgrades of the product.

4.4.6. About the Application Security database tables and schema

The Application Security distribution directory (*<ssc_distribution_dir>*) contains an initialization SQL script for each supported third-party database type. During the initial configuration (see Configuring Application Security for the first time), run this script for your database type to create the database tables and initialize the database schema for Application Security.

Before you configure Application Security for the first time, ensure that you review the information described in the following sections:

- Database user account permissions
- Database-specific configuration requirements

4.4.7. About seeding the Application Security database

When you sign in to Application Security for the first time, Application Security 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 Application Security 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 Application Security operational.



Important

For a fresh Application Security instance that does not already have an `admin` user account, seeding no longer creates the default Administrator account with a hardcoded password. Instead, seeding creates the `admin` user account using the initial password and email address that you provide either through autoconfig `init.admin.password` and `init.admin.email` appProperties (see Automating Application Security configuration), or through the Setup wizard. If neither of these initialization values is provided for a fresh instance, initialization fails. If an `admin` user account already exists, such as when you upgrade from an earlier release, seeding does not remove or change the password of the existing `admin` user account.

Application Security requires two of the downloaded seed bundles (see Downloading and unpacking Application Security files):

- The issue template seed bundle (`Fortify_Process_Seed_Bundle-2025_Q2_<build>.zip`) provides a default admin user account and issue template data.
- The report seed bundle (`Fortify_Report_Seed_Bundle-2025_Q2_<build>.zip`) provides the default set of reports.

You can also install the optional PCI basic bundles `Fortify_PCI_SSF_Basic_Seed_Bundle-2025_Q2_<build>.zip` and `Fortify_PCI_Basic_Seed_Bundle-2025_Q2_<build>.zip`, which add Payment Card Industry process templates and associated reports to the default set of templates and reports.

The seed bundle files are included in the Application Security installation package. After your initial deployment, you can download off-cycle seed bundles from the Application Security Customer Portal under the **PREMIUM CONTENT** > **FORTIFY EXCHANGE**. Quarterly security content releases can also include updated seed bundles.

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

After you finish seeding the database, you can modify any user-configurable data entities that were created in the seeding process from the Application Security user interface. For more information, see Additional Application Security configuration.

See also

Seeding the database with report seed bundles delivered with quarterly OpenText SAST Application Security Content releases

4.4.8. Permanently deleting a Application Security database

If, at some point, you plan to remove Application Security altogether, you can remove the Application Security database. To permanently delete a Application Security 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 Application Security database schema and all the data in the database. Ensure you have backed up any data you want to save before running this script.

To delete the Application Security database schema and all the data in the database:

1. Go to the `<ssc_distribution_dir>/sql/` directory, and open the subdirectory for the third-party database you plan to use with Application Security:
   - `mysql`
   - `Oracle`
   - `sqlserver`
2. Copy the `drop-tables.sql` script from the subdirectory that matches your Application Security 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 Application Security.
4. Review the caution in the introduction to this topic.

5. Remove the Application Security database schema and all the data in the database by running the following script:

```
drop-tables.sql
```

4.5. About deploying Application Security in Kubernetes

You can configure and use the `helm-ssc` Helm chart for complete Application Security container orchestration in Kubernetes: You can find this Helm chart at https://hub.docker.com/r/fortifydocker/helm-ssc.

> **Note**
>
> Helm charts might not be available immediately after product release. When Helm charts for the current release are available, Helm chart documentation will be available on the Application Security Documentation website.

For steps to prepare for and perform a Application Security Kubernetes deployment, refer to Deploying SSC in Kubernetes.

For information about supported versions of the required software, see the *Application Security Software System Requirements* (optional) document.

Deploying Application Security to a Kubernetes cluster

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

For an air-gapped deployment, you must push the Application Security container image to a private registry that is accessible from your Kubernetes cluster.

To deploy Application Security to a Kubernetes cluster:

1. Create a Docker Hub account, and then supply your account name to Customer Support.
   Customer Support can give you access to the Fortify Docker repository.
   To request access to the Application Security Docker image published in the Fortify Docker repository, send an email with the following information to mfi-fortifydocker@opentext.com:
   - First Name
   - Last Name
   - Company Name
   - Docker ID
   - Customer ID
2. (For an air-gapped installation, or a private registry. A running Docker server and Docker client are assumed to be in place.) Transfer the Application Security container image to your private registry, as follows:
   1. Log in to the Docker Hub using `docker login`.
   2. Log in to your private registry using `docker login <priv_reg_host_and_port>`, where `<priv_reg_host_and_port>` represents the host and port of your private registry.
   3. Transfer the Application Security container image, as follows:

      1. ```
         docker pull "fortifydocker/ssc-webapp:<tag>"
         ```

      2. ```
         docker tag "fortifydocker/ssc-webapp:<tag>" "
         <priv_reg_host_and_port>/<priv_reg_path>/ssc-webapp:<tag>"
         ```

      3. ```
         docker push "<priv_reg_host_and_port>/<priv_reg_path>/ssc-webapp:<tag>"
         ```
         ```

> **Note**
> To determine the value to use for *<tag>*, go to the `<ssc_helm_dir>` directory and open the `ssc-<chart_version>+<ssc_version>.tgz` file. Use the `<ssc_version>` value (tag for the latest published image build) from the TGZ file name.
> There are also tags for exact image builds in the format `<ssc_version>.<imageBuildNumber>`
> You can list available image tags in the docker hub. If you use `<imageBuildNumber>`, you must specify it in the `image.buildNumber` Helm chart value.

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

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

   `  - name: regcred`

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

5. (Optional) Prepare a `secret.key` file to encrypt sensitive data.
   1. If you are deploying Application Security for the first time, you must locate the password tool in the `bin` directory of the standard distribution and run the following command to generate a new keystore:
      `<ssc_distribution_dir>/bin pwtool secret.key`
      A new `secret.key` file is generated.
      Press **Enter** and type a string for encryption.
   2. If you are migrating a non-containerized Application Security to a Kubernetes cluster, locate your existing secret.key in the following directory:
      `<fortify.home>/<app_context>/conf`
      For more information on the secret.key location, see About the <fortify.home> Directory.
6. Enter any other required parameters to the `values.yaml` file.
   - The `urlHost` must contain the fully-qualified DNS name intended for accessing Application Security. The address for accessing the Application Security installation is `<https://<hostname>:<service.httpsPort>/<sscPathPrefix>`. For example, `https://ssc.example.com:443/ssc`. If the port is 443, you can omit it from the URL (`https://ssc.example.com/ssc`).
   - For ease of use, OpenText recommends that you set the `service.type` parameter to `LoadBalancer`.
   - To apply changes to the Application Security secret referenced by `secretRef.name`, you must manually remove the ssc-webapp pod (it is later automatically re-created).



Note

If necessary, you can change most values you specify for parameters in the `values.yaml` file later, and then redeploy Application Security to implement the changes. Depending on the Kubernetes cluster, the exception might be parameters for a `persistentVolumeClaim`.

Customizing the Tomcat access logs

To change the default format for Tomcat access logs on the `ssc-webapp` container image, set the `HTTP_SERVER_ACCESS_LOG_PATTERN` environment variable to the Tomcat Access Log Valve pattern. For information about the patterns supported, see the Apache Tomcat Configuration Reference website.

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

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

Troubleshooting deployment to a Kubernetes cluster

This section provides troubleshooting tips if you encounter errors during an attempted deployment.

If you crash during the installation phase, run:

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

To display logs after installation, run:

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

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

```
kubectl get pods
```

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

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

```
kubectl get services
```

To list those names, run:

```
helm list
```

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

```
helm get values <installation_name>
```

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

```
kubectl describe --help
```

If everything looks fine, but Application Security does not run as expected, and logs alone do not provide enough information, run the following to inspect the container file system, check the state of the environment, and perform advanced debugging tasks:

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

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

For a visual guide to troubleshooting your deployment, see A visual guide on troubleshooting Kubernetes deployments. For guidance on debugging common containerized application issues, see Troubleshooting Applications.

4.6. About the directory

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

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

- On Windows systems: `%USERPROFILE%\.fortify`
  Applies to both a standard user and a Windows service user.

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

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

- On Linux systems: `$HOME/.fortify`

4.6.1. Changing the default location

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

Example:

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

Note

To change the <*fortify.home*> directory location after Application Security is configured (see Configuring Application Security for the first time), ensure that you copy or move the contents of the existing <*fortify.home*> directory to the new location before you restart the server with the updated `fortify.home` system property value.

4.6.2. Directory contents

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

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

where

- `<app_context>`
  represents the application server context in which Application Security is deployed. For details, see Automating Application Security configuration.
- `app.properties`
  is a file that contains the application properties that the customer can configure. If you automate the Application Security configuration, this file is generated based on the `appProperties` key in the autoconfig file on every startup. For more information, see Automating Application Security configuration.
- `datasource.properties`
  is a file that contains the database connection properties. If you automate the Application Security configuration, this file is generated based on the `datasourceProperties` key in the autoconfig file on every startup. For more information, see Automating Application Security configuration.
- `log4j2.xml`
  is a file that contains the default log configuration. Although you can change this configuration manually, OpenText strongly recommends that you use the log4j2 configuration override feature instead (see Configuring logging).
- `secret.key`
  is an encryption key file used to encrypt and decrypt sensitive configuration information in Application Security. Application Security never overwrites this file. However, the file is generated if it is missing from the `<fortify.home>/ <app_context>/conf/` directory.
  If you deployed Application Security version older than 23.1.0, OpenText recommends that you migrate your `secret.key` to the new format. To run Application Security in FIPS environment, you must migrate your `secret.key` to the new format.
  For more information, see Migration of secret.key file.

  Note
  The `datasource.properties` file and some database fields contain encrypted entries that rely on the `secret.key` file. If you move your Application Security instance from one computer to another, you must also move the `secret.key` file (not just your database files).
- `version.properties`
  is a file that stores information about current and previous versions of Application Security for application upgrade purposes.
- `logs`
  is a directory that contains Application Security log files and plugin log files.

- `init.token`
  is a file that contains a new security token that is generated each time the Setup wizard is loaded (start of server in configuration mode). The user who configures Application Security uses this token to access the Setup wizard (see Configuring Application Security for the first time).
- `plugin-framework`
  is a directory that contains unpacked plugins and is fully managed by Application Security.

  Note
  `plugin-framework` is automatically managed by Application Security and does not contain anything that would require back up.

- `fortify.license`
  is the Application Security license file.

Important
The `<fortify.home>/<app_context>/conf/` directory must always contain the following files:

- `app.properties`
- `datasource.properties`
- `log4j2.xml`
- `secret.key`
- `version.properties`

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

4.6.3. Migration of secret.key file

Application Security versions 23.1.0 or later use a different format of the secret.key file to run in an FIPS environment. The secret.key must be migrated externally of the FIPS environment.

To verify the version of the `secret.key` and determine if you need to migrate your secret.key file, open your `secret.key` file in a text editor.

The updated format of the `secret.key` contains the following text, which indicates that you do not need to migrate the secret.key:

`BEGIN FORTIFY SECRET KEY V1`

Retrieving the secret.key file

In non-containerized deployments, copy the `secret.key` file from the `<fortify.home>/<app_context>/conf/` directory. For information on the location, see About the <fortify.home> directory.

In containerized deployments, if you created the `secret.key` file using Kubernetes secrets, extract the `secret.key` from the Kubernetes secret. Otherwise, use the `kubectl cp` command to copy the `/fortify/ssc/conf/secret.key` file from the `container/fortify volume` to your local file system.

Migrating the secret.key file

Locate the migration tool in the `<ssc_distribution_dir>/bin/` directory and run the following command:

```
<ssc_distribution_dir> /bin/pwmigtool <secret.key_file_to_migrate>
```

The migration tool renames the legacy secret.key file to `<secret.key_file_to_migrate>.pwtool-migration-backup`.

Applying the migrated secret.key file

In non-containerized deployments, replace the `secret.key` file in the `<fortify.home>/<app_context>/conf/` directory and restart Application Security.

In containerized deployments, if you provisioned the `secret.key` file using Kubernetes secret, update the secret. Otherwise, use the `kubectl cp` command to replace the `/fortify/ssc/conf/secret.key` file in the `container/fortify volume`.

Delete the Application Security `webapp` pod to restart.

5. Configuring Application Security for the first time

After you deploy Application Security for the first time and then enter the Application Security URL in a browser window, the Setup wizard opens. Use the Setup wizard to complete the steps for the initial server configuration. The Setup wizard is available to administrators only after you first deploy Application Security, after you upgrade it, or after you place Application Security in maintenance mode (see Placing Application Security in maintenance mode).

To configure Application Security for the first time:

1. After you deploy a new version of the Application Security WAR file to Tomcat server, open a browser window and type your Application Security server URL (
   `<protocol>://<hostname>:<port>/<app_context>`
).

   > **Note**
   > For a standard deployment, the default Application Security URL is `<protocol>://<hostname>:<port>/ssc`. For a deployment to a Kubernetes cluster, the default URL is `<protocol>://<hostname>:<port>` (without `ssc` at the end).
   > If you deploy Application Security using a distributed WAR file without renaming the `ssc.war` file, `<app_context>` is `ssc` unless it is overwritten by the Tomcat server configuration.

2. On the upper-right of the webpage, click **ADMINISTRATORS**.
3. Open the `<fortify.home>/<app_context>/init.token` file in a text editor.
   If Tomcat is running as a 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. In the Setup wizard sign in, paste the string you copied from the `init.token` file into the **Security Token** box, and then click **SIGN IN**.
6. Read the information on the Setup wizard **START** page, and then click **NEXT**.
7. On the **CONFIGURATION** page, under **UPLOAD FORTIFY LICENSE**, do the following:
   1. Click **UPLOAD**.
   2. Browse to and select your `fortify.license` file, and then click **UPLOAD**.

   The Setup wizard displays the default path of the configuration directory where your configuration files (`app.properties`, `datasource.properties` and `version.properties`) will reside.
8. Read the warning note about sensitive information in the configuration file directory, select the **I have read and understood this warning** check box, and then click **NEXT**.
   For information on how to change the location of this directory, see About the <fortify.home> directory.
9. On the **CORE CONFIGURATION SETTINGS** page, do the following:
   1. Under **FORTIFY SOFTWARE SECURITY CENTER URL**, type the URL for your Application Security server.
   2. Select the **Enable HTTP host header validation** check box to ensure that the HTTP Host header value matches the value configured in the Application Security URL (`host.url` property).
      Both the host and port must match. This affects both browsers and direct REST API access. If validation is turned off, any HTTP Host header can access Application Security.
   3. To enable global searches, in the **GLOBAL SEARCH** pane, do the following:
      1. Select the **Enable global search** check box.
      2. 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.

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

> **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.

3. Read the warning in the **GLOBAL SEARCH** pane, and then select the **I have read and understood this warning** check box.

10. Click **NEXT**.
11. On the **DATASOURCE** page, do the following:
    1. From the **DATABASE TYPE** list, select the database type you are using for Application Security.
    2. In the **DATABASE USERNAME** box, type the user name for your database account.
       For more information, see Database user account permissions.
    3. In the **DATABASE PASSWORD** box, type the password for your database account.
       Ensure that the database user credentials specified in the **DATABASE USERNAME** and **DATABASE PASSWORD** fields are for a user account that has the permissions required to execute migration scripts. These permissions are described in Database user account permissions.
    4. In the **JDBC URL** box, type the URL for Application Security, keeping in mind the following:
       For MySQL databases:
       - If MySQL server is configured to use the `sha256_password` or the `caching_sha2_password` authentication plugin, you must provide the server RSA public key to the JDBC driver with the `serverRsaPublicKeyFile` option. Alternatively, you can use the less secure `allowPublicKeyRetrieval` option. For more information, go to the MariaDB Connector/J and MySQL server documentation.
       - You must append the following two statements at the end of the JDBC URL:

         ```
         sessionVariables=collation_connection=<collation>
         rewriteBatchedStatements=true
         ```

         where *<collation>* represents your database collation type.
         Examples:

         ```
         jdbc:mysql://<host>:3306/ssc?
         sessionVariables=collation_connection=utf8mb3_bin&rewriteBatchedStatements=true

         jdbc:mysql://<host>:3306/ssc?
         sessionVariables=collation_connection=latin1_general_cs&rewriteBatchedStatements=true
         ```

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

       For SQL Server databases:
       - You must append the following property setting to the end of the JDBC URL:
         `sendStringParametersAsUnicode=false`
         Example:

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

Caution

Application Security includes a SQL Server JDBC driver version that requires an encrypted connection and a trusted server certificate by default. If the connection fails as a result of certificate verification, OpenText recommends that you provide the trust store. If providing a trust store is not an option, you can disable trust verification. If the certificate is trusted but the certificate DNS name does not match the database server hostname, use the `hostNameInCertificate` connection property to provide the correct hostname.

For more information, see `hostNameInCertificate`, `trustServerCertificate`, and `trustStore*` `JDBC URL` properties in the Setting the connection properties article.

5. In the **MAXIMUM IDLE CONNECTIONS** box, type the maximum number of idle connections that can remain in the pool.
   The default value is 50.
6. In the **MAXIMUM ACTIVE CONNECTIONS** box, type the maximum number of active connections that can remain in the pool.
   The default value is 100.
7. 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.
8. To test your settings, click **TEST CONNECTION**.
   If the connection test fails, check the `ssc.log` file in the `<fortify.home>/<app_context>/logs` directory to determine the cause.

12. Click **DOWNLOAD SCRIPT** to download the `create-tables.sql`, and then run the script.

Note

If you automate the Application Security configuration and you have enabled database migration in the `<app_context>.autoconfig` file, you do not need to run the `create-tables.sql` script. For information about how to automate the configuration, see Automating Application Security configuration.

13. After you initialize the database, click **NEXT**.
14. On the **ADMIN ACCOUNT** page, configure the initial `admin` account:

Note

The default Administrator user name is `admin` and cannot be changed during setup.

1. In the **ADMIN EMAIL** box, type the email address for the `admin` account.
2. In the **ADMIN PASSWORD** box, type a password that meets the minimum password strength requirement. The password strength indicator displays the strength of the password and the minimum strength required.

Note

Password strength is enforced by the `password.strength.min.score` property, which defaults to `3` (see, Application configuration options). For information about the `zxcvbn4j` library used to check password strength, see Setting the required password strength for Application Security sign in.

3. In the **CONFIRM PASSWORD** box, type the password again.

Important

This password cannot be recovered after setup. You must record the password and store it securely.

4. Select the **I understand that this password cannot be retrieved in cleartext after setup** check box.
5. Click **NEXT**.

> **Note**
> If an admin account already exists, the Setup wizard skips the ADMIN ACCOUNT step and displays an informational message.

15. On the **DATABASE SEEDING** page, do the following:
    1. Click **BROWSE** to locate and select your `Fortify_Process_Seed_Bundle-2025_Q2_<build>.zip` file, and then click **SEED DATABASE**.
    2. Click **BROWSE** to locate and select your `Fortify_Report_Seed_Bundle-2025_Q2_<build>.zip` file, and then click **SEED DATABASE**.
    3. (Optional) Click **BROWSE** to locate and select your `Fortify_PCI_SSF_Basic_Seed_Bundle-2025_Q2_<build>.zip` file, and then click **SEED DATABASE**.
    4. (Optional) Click **BROWSE** to locate and select your `Fortify_PCI_Basic_Seed_Bundle-2025_Q2_<build>.zip` file, and then click **SEED DATABASE**.

    For descriptions of the available seed bundles, see Downloading and unpacking Application Security files.
16. Click **NEXT**, and then click **FINISH**.
17. On Linux systems only, ensure the fontconfig library, DejaVu Sans fonts, and DejaVu Serif fonts are installed on the server so that users can generate BIRT reports.
18. Restart Tomcat server.

After you finish the initial Application Security configuration, then you can complete the configuration of the core attributes and additional settings. For information, see Additional Application Security configuration.

If you later need to change any of the configuration settings, you can place Application Security in maintenance mode, and then make any necessary changes. For instructions on how to place Application Security in maintenance mode, see Placing Application Security in maintenance mode.

See also

Configuring Application Security after an upgrade

Upgrade Lucene

5.1. Signing in to Application Security for the first time

After you create and initialize your Application Security database, configure Tomcat server, and deploy Application Security in Tomcat, you can sign in to Application Security.

> **Important**
> When you sign in for the first time, enter the initial admin password that you configured during autoconfig or in the Setup wizard (do not enter `admin` as the password).

To sign in to Application Security:

1. In a web browser, type the web address for your Application Security instance.

> **Note**
> For a standard deployment, the default Application Security URL is `https://<hostname>:<port>/ssc`. For a deployment to a Kubernetes cluster, the default URL is `<hostname>:<port>` (without `ssc` at the end).

2. In the **Username** field, type `admin`. In the **Password** field, type the initial admin password that you configured during autoconfig or in the Setup wizard. After your first sign in, you must change this password.
3. Click **SIGN IN**.
4. When prompted, change your password.
   Specify a strong password that does not include your user name or common phrases (names, movie or song titles, dates, or number or letter sequences). After your password is evaluated as strong, save it, and then sign in. See, Setting the required password strength for Application Security sign in.

> **Important**
> Do not delete the default `admin` account, even if you create another account with the Administrator role.

See next

Additional Application Security configuration

Setting the required password strength for Application Security sign in

6. Additional Application Security configuration

After you finish the preliminary Application Security configuration and deploy the `ssc.war` file, complete the configuration from the Application Security Administration view.

This section contains the following topics:

- About integrating components with Application Security
- Configuring Issue Stats thresholds
- Configuring application security training
- Configuring AI Assistant
- Configuring security for BIRT reporting
- Configuring core settings
- Managing Fortify Object Storage
- Blocking data export to CSV files
- Changing the support contact link in the About box
- Adding a Fortify Insight link to the Dashboard
- Customizing the banner for your organization
- Creating a system-wide banner
- Configuring global processing rule defaults
- Configuring email alert notification settings
- Setting the strategy for resolving issue audit conflicts
- Configuring Java Message Service settings
- About Application Security user authentication
- LDAP user authentication
- Implementation of SCIM 2.0 protocol
- Configuring a proxy for integrations
- Enabling the running and management of OpenText ScanCentral DAST scans
- Configuring a Kafka Stream to use with OpenText ScanCentral DAST
- Enabling integration with Fortify ScanCentral SAST
- Configuring job scheduler attributes
- Recurring cleanup jobs
- About data retention
- Configuring secure browser access
- About configuring Application Security to work with single sign-on

- Configuring logging
- Running in a Federal Information Processing Standards (FIPS) environment
- Setting the required password strength for Application Security sign in
- About audit issue history

6.1. About integrating components with Application Security

The following table lists the components you can integrate with Application Security.

Component	Integration instructions
Security training vendors	Configuring application security training
OpenText™ Fortify Audit Assistant	Configuring Fortify Audit Assistant
Java Message Service (JMS)	Configuring Java Message Service settings
LDAP servers	Configuring LDAP Servers
System for Cross-domain Identity Management (SCIM)	Implementation of SCIM 2.0 protocol
OpenText Fortify ScanCentral DAST	Enabling the running and management of OpenText Fortify ScanCentral DAST scans
OpenText Fortify ScanCentral SAST	Enabling integration with OpenText Fortify ScanCentral SAST
Single sign-on (SSO)	About configuring Application Security to work with single sign-on
Bug tracking systems	About bug tracking system integration
Software composition analysis	• Preparing to display OpenText Fortify SCA results • Preparing to display Sonatype results
OpenText Application Security Tools	
Fortify Audit Workbench	OpenText™ Fortify Audit Workbench User Guide
OpenText™ Fortify Plugin for Eclipse	OpenText™ Fortify Plugin for Eclipse User Guide
OpenText™ Fortify Extension for Visual Studio	OpenText™ Fortify Extension for Visual Studio User Guide
OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio	OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio User Guide
OpenText™ Fortify Jenkins Plugin	OpenText™ Fortify Jenkins Plugin User Guide
OpenText™ Fortify Extensions for Visual Studio Code	OpenText™ Fortify Extensions for Visual Studio Code
OpenText™ Fortify Remediation Plugin for Eclipse	OpenText™ Fortify Remediation Plugin for Eclipse User Guide
OpenText™ Fortify Remediation Plugin for IntelliJ IDEA and Android Studio	OpenText™ Fortify Remediation Plugin for IntelliJ IDEA and Android Studio User Guide
OpenText™ Fortify Azure DevOps Extension	Fortify Azure DevOps Extension User Guide

Important

If you integrate Application Security with other components, ensure that you minimize clock skew between communicating machines. OpenText recommends that you synchronize computer clock times using, for example, Network Time Protocol (NTP). If that is not possible, OpenText suggests that you maintain a clock skew of less than five minutes, compared on a UTC basis. Otherwise, communication requests to Application Security can fail.

6.2. Configuring Issue Stats thresholds

The **Issue Stats** page on the **Dashboard** view shows summary information about issues for the application versions, including the number of days that it is taking to review and fix them. To provide a visual indication of 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, Application Security applies the following rules:

- Application Security 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, Application Security uses the date and time on which the issue was first audited.
- For issues that were not audited but were removed, Application Security uses the removal date as the audit date.
- To calculate issue dates, Application Security 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 on March 5, the days to review is 5 – 2 + 1, or 4 days.

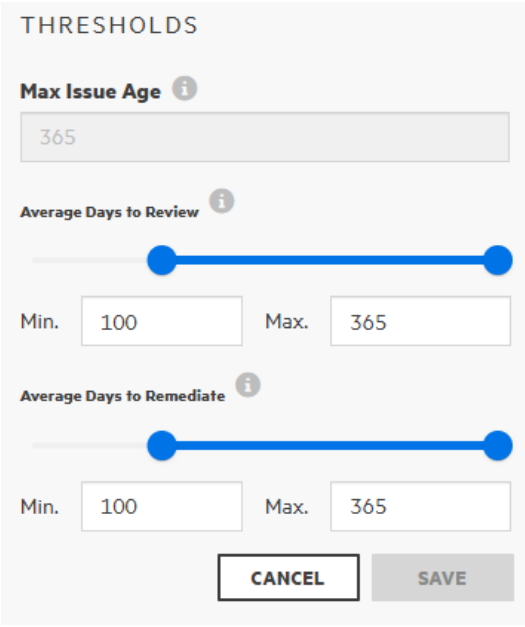
After it applies all these rules and makes time and date adjustments, Application Security calculates the average of two values—(auditTime - foundDate) and (removedDate - foundDate)—to get average number of days to audit and remediate issues.

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 green, any values greater than 365 days (maximum) in red, and values in between in yellow.

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

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



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

6.3. Configuring application security training

If your organization has access to an application security training platform, you can integrate that training with Application Security. 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 Application Security:

1. On the header, select **Administration**.
2. On the navigation pane, expand **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 Application Security and to obtain the corresponding training URL, contact Customer Support.
5. In the **Training URL** box, type your application security training URL.
6. Click **SAVE**.

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

See also

Auditing analysis results

6.4. Configuring AI Assistant

AI Assistant provides a single location in Application Security where administrators configure supported AI assistants. The page includes the following tabs:

- Audit Assistant: Contains the Audit Assistant configuration.

- Aviator: Contains the Aviator configuration (if available in your environment).

Accessing AI Assistant

1. Sign in as an Administrator.
2. In the header, select **Administration**.
3. In the navigation pane, expand **Configuration**, and then select **AI Assistant**.

Selecting AI Assistant tabs

You can enable either Audit Assistant or Aviator at a time. If you enable an AI assistant while another AI assistant is already enabled, Application Security displays a warning message before making any changes.

- Select **Yes** to switch assistants. Application Security disables the currently enabled assistant and enables the assistant you selected.
- Select **No** (or press **Esc**) to cancel. Application Security makes no changes and restores the previous selection.

See also

Configuring Fortify Audit Assistant

Fortify Audit Assistant Best Practices

Using Fortify Audit Assistant

Configuring Aviator

6.4.1. About Fortify Audit Assistant

Fortify Audit Assistant is an optional tool to help determine whether or not the issues returned from a scan represent true vulnerabilities. Application Security can work with Fortify Audit Assistant to help determine whether the issues returned in OpenText Fortify SAST analysis results represent true vulnerabilities.

To make its determinations, Fortify Audit Assistant needs data to establish a baseline for its predictions. This data is based on the decisions OpenText Fortify on Demand auditors made during scan audits about how to characterize various issues. The data, which is pooled and anonymized, can be used in conjunction with training data based on decisions your auditors have made. Fortify Audit Assistant assessments of the actual threats that issues represent become more accurate as it receives more training data.

The following sections describe how to <madcap:change changes="2"> obtain an authentication token from </madcap:change><meta class="data-nv" data-nv="AuditAssistant" data-nv-value="Fortify Audit Assistant" data-productid="2174" data-replace-parent="false" data-version="25.2"/><madcap:change changes="2">, and then</madcap:change> use <madcap:change changes="3">an authentication token from </madcap:change><meta class="data-nv" data-nv="AuditAssistant" data-nv-value="Fortify Audit Assistant" data-productid="2174" data-replace-parent="false" data-version="25.2"/><madcap:change changes="2">that token</madcap:change> to configure a connection to <meta class="data-nv" data-nv="SSC_Short" data-nv-value="Fortify Software Security Center" data-productid="2174" data-replace-parent="false" data-version="25.2"/>. This section also describes the best practices for <meta class="data-nv" data-nv="AuditAssistant" data-nv-value="Fortify Audit Assistant" data-productid="2174" data-replace-parent="false" data-version="25.2"/> when upgrading to the latest version of <meta class="data-nv" data-nv="AuditAssistant" data-nv-value="Fortify Audit Assistant" data-productid="2174" data-replace-parent="false" data-version="25.2"/> powered by the G2 engine.Later sections describe how to set up training, submit data, and review results.

See also

Configuring Fortify Audit Assistant

Fortify Audit Assistant Best Practices

Using Fortify Audit Assistant

6.4.1.1. Configuring Fortify Audit Assistant

Application Security can work with Fortify Audit Assistant to help determine whether or not the issues returned in Fortify Static Code Analyzer scan results represent true vulnerabilities.

Important

In Fortify Audit Assistant, create one or more Generation 2 (G2) prediction policies. You must create prediction policies that work with the G2 prediction model. For detailed instructions on how to define prediction policies in Fortify Audit Assistant, see the Fortify Audit Assistant Help in the Fortify Audit Assistant Documentation.

Only one AI assistant can be enabled at a time. If Aviator is enabled and you try to enable Audit Assistant, Application Security displays a warning message before making any changes. For more information, see Configuring AI Assistant.

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

1. Sign in as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Configuration**, and then select **AI Assistant**.
4. Select the **Audit Assistant** tab.
5. Configure the settings on the **Audit Assistant** page as described in the following table.

Field	Description
Enable Audit Assistant check box	Select this check box to enable Fortify Audit Assistant.
Authentication token	(Required) Paste the authentication token you obtained from Fortify Audit Assistant here. For instructions on how to get a token, select **How do I get a token?**.
Fortify Audit Assistant server URL	(Required) Specify the URL for the Fortify Audit Assistant server.
Use SSC proxy for Audit Assistant	(Optional) If you configured a proxy for all Application Security integrations (see Configuring a proxy for Application Security integrations, you can select this check box to use that proxy for Fortify Audit Assistant.

6. To test the connection to the Fortify Audit Assistant server, click **TEST CONNECTION**.
   After the connection is successfully tested, you can go ahead and configure the following settings in the **Audit settings** section.
7. Click **REFRESH POLICIES** to populate the **Default prediction policy** list with the current server policies on the Fortify Audit Assistant server.

   Note

   Fortify Audit Assistant prediction policies set for individual application versions can become invalid if available policies are changed on the Fortify Audit Assistant server. Application Security verifies new policies it receives from Fortify Audit Assistant every time a user clicks **REFRESH POLICIES**.) If Application Security 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. Application Security updates the policies based on the changes you submit in the mapping table.

8. From the **Default prediction policy** list, select the name of the prediction policy to apply to all application versions. (Policies are defined in Fortify Audit Assistant.)
9. To specify prediction policies at the application version level and override the default global prediction policy, select **Enable specific application version policies**.
   Otherwise, Fortify Audit Assistant uses the default global prediction policy you specified in the previous step. To specify the policy for an application version, see Configuring Fortify Audit Assistant options for an application

version.

10. To enable Application Security to automatically send issues not yet audited to Fortify Audit Assistant for assessment, select the **Enable auto-predict** check box.
    After you do, you must enable this functionality on a per-application version basis (see Configuring Fortify Audit Assistant options for an application version). For information about the auto-predict feature, see About Audit Assistant auto-prediction.
11. To enable the application of the analysis values that Fortify 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 basis (see Configuring Fortify Audit Assistant options for an application version).
    <img data-zoom="true"
    src="file/images/general/fssc/SSC_Project/ssc_project_resources_imagesEnable_autoapply.png" style="border: none !important;"/>

    Important
    Before you can use the auto-apply feature, you must first map Fortify Audit Assistant analysis tag values to Application Security Analysis tag values (see Mapping Fortify Audit Assistant analysis tag values to Application Security custom tag values).
12. Click **SAVE**.

See also

Using Fortify Audit Assistant with Application Security

Fortify Audit Assistant workflow

Mapping Fortify Audit Assistant analysis tag values to Application Security custom tag values

6.4.1.2. About Fortify Audit Assistant auto-prediction

By setting auto-predict to yes, you can configure Application Security to automatically send issues for Fortify Audit Assistant predictions 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 Fortify 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 Fortify Audit Assistant for assessment. After Fortify Audit Assistant has assessed an issue, it does not revisit that issue.

Auto-prediction enablement for an application version is a two-step process. First, an Administrator enables it system wide in the Fortify Audit Assistant configuration (see Configuring Fortify Audit Assistant). After this, users need to enable auto-prediction on a per-application-version basis (see Enabling auto-apply and auto-predict for an application version).

6.4.2. Configuring Aviator

Aviator is an AI assistant that can be enabled and managed from Application Security. When you enable Aviator, you can view the tags and comments generated by OpenText™ Application Security Aviator for Vulnerability Remediation in Application Security UI and remediation through the following APIs:

- `/projectVersions/{parentId}/remediations`
- `/projectVersions/{parentId}/remediations/{id}`

For information about OpenText™ Application Security Aviator for Vulnerability Remediation, see the *OpenText™ Application Security Aviator for Vulnerability Remediation User Guide*.

Note
If an issue includes a remediation, verify it through the Issues API using the `hasAviatorRemediation` key.

Accessing the Aviator configuration

1. Sign in as an Administrator.
2. In the header, select **Administration**.
3. In the navigation pane, expand **Configuration**, and then select **AI Assistant**.
4. Select the **Aviator** tab.

Enabling or disabling Aviator

1. In the **Aviator** tab, select the **Enable Aviator** check box to enable Aviator.
2. Click **SAVE**.

Only one AI assistant can be enabled at a time. If Audit Assistant is enabled and you try to enable Aviator, Application Security displays a warning message before making any changes. For more information, see Configuring AI Assistant.

See also

Working with Aviator auto-remediation results

6.5. Configuring security for BIRT reporting

OpenText recommends that you create a separate, read-only database account specifically for BIRT 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 the database tables and views listed in the following table.

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

3. Sign in to Application Security as an Administrator.
4. On the header, select **Administration**.
5. On the navigation pane, expand **Configuration**, and then click **BIRT Reports**.
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 that the database user account has access to the database, click **VALIDATE CONNECTION**.
8. Click **SAVE**.

See also

Allocating memory for report generation

Setting report generation timeout

6.5.1. Allocating memory for report generation

To allocate memory for security for Application Security reports:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Configuration**, and then click **BIRT Reports**.
3. Under **Set up BIRT execution**, select the value in the **Maximum heap size (MB)** box, and then type a new value.
4. Click **SAVE**.

6.5.2. Setting report generation timeout

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

1. On the header, select **Administration**.
2. On the navigation pane, expand **Configuration**, and then click **BIRT Reports**.
3. Under **Set up BIRT execution**, select the value in the **Execution timeout (minutes)** box, and then type a new value.
4. Click **SAVE**.

6.6. Configuring core settings

In addition to the initial configuration you performed with the Setup wizard, you must also configure several core attributes. These attributes include user account timeout and lockout settings, the display of user information, maximum events per OpenText™ DAST Agent issue, the base URL for the runtime event description server, and an 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.

To configure Application Security core settings:

1. Sign in as an Administrator
2. On the header, select **Administration**.
3. On the navigation pane, expand **Configuration**, and then select **Core**.

On the **Core** page, configure the settings described in the following table.

Field	**Description**
Absolute session timeout (minutes)	Number of minutes a user can be continuously active before automatic logout occurs. The default value is `240`.
Days before password reset	Number of days a Application Security password is valid before the user must change it. The default value is `30`.
Login attempts allowed before a user is locked out	Number of times a local user can try to sign in to Application Security using invalid credentials before the user's account is locked. If Application Security locks a user out, that user is prevented from attempting a new login for the number of minutes specified in the **Lockout time (minutes)** box. For information about how to unlock a user account, see Unlocking local user accounts. The default value is `3`. **Note** This setting does not apply to LDAP users. If the account lockout threshold was configured using the Group Policy editor, the LDAP user account could be locked out in Active Directory if consecutive login attempts have failed.
Lockout time (minutes)	If a user attempts and fails to sign in to Application Security the number of times specified for **Login Attempts before Lockout**, Application Security locks the user account for the number of minutes specified in the **Lockout time (minutes)** box. The default value is `30`.

User lookup strategy	If LDAP is enabled, select one of the following user lookup strategies from this list: • **Local users first, fallback to LDAP users (compatibility)** Search local users first, then search LDAP users. To avoid potential authorization errors and user confusion, ensure that usernames are not duplicated on the LDAP server and local storage. • **LDAP users first, fallback to local users** Search LDAP users first, then local users. To avoid potential authorization errors and user confusion, ensure that user names are not duplicated on the LDAP server and local storage. • **LDAP users exclusive, fallback to local administrator** (Recommended strategy for SSO) Search LDAP users only, and allow local administrator access.
Display user first/last names and emails in user fields, along with login names	Select this check box to display the following user information, when applicable: login name, first and last names, and email address.
Maximum events per WebInspect Agent Issue	Maximum number of events to log within a single OpenText DAST Agent issue. After that threshold is reached, new events related to the same issue are ignored. The default value is `5`.
Inactive session timeout (minutes)	Number of minutes a user can be inactive before Application Security automatically logs the user off. The default value is `30`.
Locale for Rulepacks	Type one of the following: • ja (Japanese) • zh_CN (simplified Chinese) • zh_TW (traditional Chinese) • es (Spanish) • pt_BR (Portuguese Brazilian) **Note** There is no need to specify a value for English.

Rulepack update URL	URL for the Rulepack update server. The default value is `https://update.fortify.com`. **Important** Do not change the default value of the **Rulepack Update URL** field unless your Customer Support representative directs you to do so.
Use SSC proxy for Rulepack update	Select this check box to enable use of the Application Security proxy, if the Rulepack update server is behind it. **Note** You must enable and correctly configure the Application Security proxy. For information, see Configuring a proxy for Application Security integrations.
User administrator's email address (for user account requests)	Email address of the user who is to receive system email alerts and notifications when email notifications are enabled. Requests for new user accounts are sent to this address when the **Can't access or need an account?** link is available on the sign in dialog box.
Enable export to CSV from the Dashboard and AUDIT views	By default, users can export Application Security data displayed in the **Dashboard** view and the **AUDIT** page to comma-separated values (CSV) files. You can block this functionality by clearing this check box. **Note** If you are changing only this setting on the **Core** page, a server restart is not required to implement the change.

- Click **SAVE**.
- Restart the server.

See also

Unlocking local user accounts

6.6.1. About configuring a proxy for Rulepack updates

By default, Application Security downloads the current versions of OpenText Secure Coding Rulepacks you subscribe to from the Rulepack update server.

If your organization uses a proxy to access external resources, OpenText recommends that you configure a proxy for Rulepacks updates (as well as for bug tracking and, if you use it, Fortify Audit Assistant). For instructions on how to

configure a single proxy for use with all HTTP(s) protocol-based Application Security integrations, see Configuring a proxy for Application Security integrations.

After you configure a single proxy for use with all HTTP(s) protocol-based integrations, you can enable that proxy for Rulepack updates.

See also

Configuring core settings

6.7. Managing Fortify Object Storage

Fortify Object Storage (FOS) stores FPR files and other supported objects outside the Application Security database. Depending on the deployment, FOS supports local file system and Amazon S3 or S3-compatible object storage (`StoreType = FILESYSTEM` or `S3`).

> **Note**
>
> The local file system is not supported for production deployments. Use only Amazon S3 for production deployments.

FOS is optional. Existing integrations continue to use the Application Security APIs to upload and download FPR files.

FOS operating modes

- **LEGACY_ONLY**: Writes are stored only in legacy storage. If content already has a copy in FOS, such as content created while operating in `DUAL_WRITE` mode, reads continue to use the FOS copy when available and fall back to legacy storage if necessary.
- **DUAL_WRITE**: Writes use both legacy storage and FOS. Use this mode during migration and validation.
- **FOS_ONLY**: Uses FOS exclusively. Enable this mode only after migration completes and health checks pass.

Use `DUAL_WRITE` to migrate existing data and validate the provider. You can change from `DUAL_WRITE` to `LEGACY_ONLY` when rollback is required. In `LEGACY_ONLY`, delete the FOS data only after confirming that legacy reads succeed.

Configure strict `dual-write` behavior

By default, an FOS write failure in `DUAL_WRITE` logs a warning without failing the operation. To require both writes to succeed, configure:

```
fortify.object-store.namespaces.<namespace>.dual-write.require-both: true
```

Set the property to `false` to retain the default behavior. Configure this property separately for each namespace.

Transition to `FOS_ONLY`

Before changing a namespace to `FOS_ONLY`:

1. Configure the storage provider and verify its health.
2. Set the namespace to `DUAL_WRITE`.
3. Complete the migration and verify that its state is `COMPLETE`.
4. Confirm `fosOnlySafe: true`.
5. Change the namespace to `FOS_ONLY`.

Monitor FOS

Use the read-only endpoints under `/api/ops/fos`. Requests require authentication and either `PERM_SYSTEM_SETTING_VIEW` or `PERM_SYSTEM_SETTING_MANAGE`.

- `GET /api/ops/fos`: View FOS status, health, and namespace configuration.
- `GET /api/ops/fos/health`: Check FOS health.
- `GET /api/ops/fos/config`: View resolved configuration.

- `GET /api/ops/fos/storage` : View storage usage, object counts, deduplication savings, reference status, and reaper backlog.
- `GET /api/ops/fos/migration` : Monitor migration and FOS-only readiness.
- `GET /api/ops/fos/providers` : Check provider connectivity and identity.

When FOS is disabled, the health endpoint returns a status of `UP` with the detail `Object store is disabled` . FOS does not return a separate `DISABLED` status.

The endpoints use database aggregates and one cached bucket-metadata request. They do not enumerate the backend.

Storage-reference status

- **PENDING**: Upload is in progress. Investigate a growing count.
- **COMMITTED**: Object is available for reading.
- **FAILED**: Upload failed. Investigate any non-zero count.
- **TOMBSTONED**: Object is unreferenced and awaiting deletion.
- **DELETING**: Object deletion is in progress. Investigate a persistent backlog.

The reaper removes residual staging files and objects that are ready for deletion.

Audit events

FOS records significant operations through the existing Application Security audit framework. Audit records must not contain credentials, provider secrets, or other sensitive information.

FOS audit events record storage failures, delete failures, migration activity, storage reclamation, provider health changes, and FOS configuration applied during startup. Examples include:

- `FOS_STORE_FAILED`
- `FOS_DUAL_WRITE_DEGRADED`
- `FOS_DELETE_FAILED`
- `FOS_REAPER_CYCLE_FAILED`
- `FOS_STORAGE_RECLAIMED`
- Migration start, completion, and failure events
- Provider health change events
- `FOS_CONFIGURATION_APPLIED`

Successful storage operations, delete operations, and reaper cycles are not audited by FOS. The configured FOS mode is recorded during startup by the `FOS_CONFIGURATION_APPLIED` event. Changing the mode does not generate a separate audit event.

FPR integrations

Existing Application Security interfaces continue to support FPR uploads and downloads, including manual and API uploads, OpenText Fortify ScanCentral SAST, OpenText Fortify ScanCentral DAST, FCLI, IDE plugins, and Fortify Audit Workbench.

FPR artifacts are unavailable after they are deleted or purged.

Migration

Migration copies existing FPR content from the Application Security database to the configured FOS backend. The original database content remains available after migration unless the leftover-blob reclaim process is enabled separately. Migration does not transfer content from one database to another.

Supported source databases include:

- MySQL
- Microsoft® SQL Server®
- Oracle® Database

Use `/api/ops/fos/migration` to monitor migration progress. Enable `FOS_ONLY` only when migration is complete and the namespace is reported as safe for FOS-only operation.

FPR Processing administration

Administrators configure Fortify Object Storage (FOS) by setting the applicable `fortify.object-store.*` properties in `fos.properties` or `app.properties`. Changes to object storage settings require an application restart before they take effect. Administrators can also initiate migration of existing FPR content to the configured FOS backend.

6.8. Blocking data export to CSV files

By default, users can export Application Security data displayed in the **Dashboard** view and the **AUDIT** page to comma-separated values (CSV) files. You can block this functionality.

To prevent users from exporting Application Security data to CSV files:

1. Sign in to Application Security as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, click **Configuration > Core**.
4. Clear the **Enable Export to CSV from the Dashboard and AUDIT views** check box.
5. Click **SAVE**.

See also

Configuring core settings

Exporting the Dashboard summary table

Exporting data to comma-separated values files

6.9. Changing the support contact link in the About box

By default, the About box displays a link to the Customer Support portal. You can replace that link with a link to the support portal for your organization.



To display your support portal in the About box:

1. Sign in to Application Security as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Configuration**, and then select **Customization**.

4. Select the **Enable using the support URL for your organization in the About box** check box.
5. In the **Support URL for your organization** box, enter the web address for your organization's support portal.

6. In the **Text displayed for your support URL** box, type the text to display for the link to your organization's support portal.
7. Click **SAVE**.

See also

Customizing the banner for your organization

Adding a Fortify Insight link to the dashboard

6.10. Adding a Fortify Insight link to the Dashboard

If you purchased Fortify Insight, you can add a Fortify Insight link to your Dashboard.

To add the Fortify Insight link to your **Dashboard** view:

1. Sign in as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, click **Configuration > Customization**.

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

See also

Customizing the banner for your organization

Changing the support contact link in the About box

Creating a system-wide banner

6.11. Customizing the banner for your organization

You can customize the banner to display information about your organization's Application Security website either when customers sign in, or when they switch between views (**Dashboard**, **Applications**, **Reports**, and so on).

> **Caution**
>
> Each time you upgrade your Application Security instance, you must recreate the banner.

To create a custom sign in experience for your users:

1. Go to the `<ssc_deploy_dir>/WEB-INF/lib/` directory.
2. Extract the contents of the `ssc-htmlui-<version>.jar` file into a new directory (referred to as `<new_directory>` in the remaining steps).
3. Go to the `<new_directory>/META-INF/resources/html/login/` directory.
4. Open the `login.html` file in a text editor.
5. Uncomment the text `<!--<center><font color="red">Add your custom banner here</font></center>-->`, and then specify the HTML elements to set the look, feel, and content of the message displayed where indicated.
   Space limitations restrict the message text to a single line. Additional lines interfere with the user interface. The following example adds a banner with red text to the top center of the Application Security website upon login:

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

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

Important
Do not include `<new_directory>` itself in the new archive.

8. Restart the Application Security server.

To create a message banner displayed each time a user switches views:

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

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

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

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

   Important
   Do not include `<new_directory>` itself in the new archive.

8. Restart the Application Security server.

See also

Adding a Fortify Insight link to the dashboard

Creating a system-wide banner

6.12. Creating a system-wide banner

As an Administrator, you can create a system-wide banner that is displayed centered below the header on all pages in the application. Your banner can be up to 1,024 characters in length. If your banner content takes up more than two lines, there is a **Show More** link to reveal the remainder of the message.

To create a system-wide banner:

1. Sign in to Application Security as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Configuration**, and then select **Customization**.

4. Under **Customized Banner**, select the **Display a custom banner system-wide** check box.
5. In the **Enter the text to display in the banner** box, type the text for your banner.

6. Click **SAVE**.

Note

When you click on the hyperlink in the banner, the following message is displayed:
"You are about the leave Fortify Software Security Center. Do you want to continue?"

After you confirm, the hyperlink will open in a new browser tab.

See also

Customizing the banner for your organization

Adding a Fortify Insight link to the dashboard

6.13. Configuring global processing rule defaults

Administrators can configure the global file-count and line-count thresholds used by FPR processing rules. You can change these values in the user interface without editing a server properties file or restarting Application Security.

To configure the global processing rule defaults:

1. Sign in to Application Security as a user with the **Manage system settings** permission.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Configuration**, and then select **Customization**.
4. Under the processing rule customization parameters, set the values in the following table.

Customizing parameters

Parameter	Valid range	Default
File count increase/decrease percentage	1 to 100	10
File count minimum value	1 to 100,000	1
Line count increase/decrease percentage	1 to 100	10
Line count minimum value	1 to 100,000	1

5. Save your changes.

Changes take effect for subsequent FPR uploads without restarting Application Security. The global values apply to application versions that use the global processing rule defaults. Per-project-version overrides take precedence.

To review the processing rules for an application version, see Setting analysis result processing rules for application versions.

6.14. Configuring email alert notification settings

To use Application Security to send email alert notifications to your teams, do the following:

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

Note

For information about how to configure the receipt of email alerts, see Enabling and disabling receipt of email alerts.

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

Important

To enable team members who do not have an account to request access to Application Security, you must enable and configure the email service settings.

1. Sign in to Application Security as an Administrator
2. On the header, select **Administration**.
3. On the navigation pane, expand **Configuration**, and then select **Email**.
4. On the **Email** page, configure the email service settings described as follows, and then click **Save**.

EMAIL SERVICE CONFIGURATION ATTRIBUTES

Field	Description
Enable email	Select this check box to enable Application Security to send email messages of all types and to add the **Can't access or need an account?** link to the sign in dialog box. Selecting this check box also enables the **Authentication provider** field. This check box is cleared by default.
Authentication provider	Select the authentication method Application Security uses to connect to the SMTP server. The available options are **Basic** and **OAuth2.0**. The default value is **Basic**. The configuration fields are displayed depend on the selected authentication provider.

For Basic authentication:

Email service configuration attributes

Field	Description
From email address	Enter the email address that Application Security uses to identify emails sent from Application Security. For example, `fortifyserver@example.com`.
Default encoding of the email content	Enter the encoding method to be used for the email content. The default value is **UTF-8**.
SMTP server	Enter the fully qualified domain name of the SMTP server that Application Security uses to send email. For example, `mail.example.com`.
SMTP server port	Enter the port number for the SMTP server. The default value is **25**.
SMTP username	If authentication is required on the SMTP server, enter the username that Application Security uses to authenticate with the SMTP server.
SMTP password	If authentication is required on the SMTP server, enter the password associated with the SMTP username.

For OAuth2.0 authentication:

Email service configuration attributes

Field	Description
From email address	Enter the email address that Application Security uses to identify emails sent from Application Security. For example, `fortifyserver@example.com`.
Client ID	Enter the OAuth client ID that Application Security uses for authentication.
Client secret	Enter the client secret associated with the OAuth client ID.
Token endpoint URI	Enter the URI of the token endpoint that Application Security uses to obtain an access token.
Scopes	Enter the space-separated OAuth scopes to request when obtaining an access token.
Client authentication method	Select how the client credentials are sent to the token endpoint. The available options are **Client Secret Basic** and **Client Secret Post**.
SMTP server host	Enter the host name of the SMTP server that Application Security uses to send email. For example, `mail.example.com`. If SSL/TLS is enabled, enter the fully qualified domain name (FQDN) that corresponds to the SMTP server identity in its certificate. For more information, see *RFC 2595, Server Identity Check*.
SMTP server port	Enter the port number that Application Security uses to connect to the SMTP server. The default value is **587**.
Default encoding of the email content	Enter the encoding method to be used for the email content. The default value is **UTF-8**.

Connection security

Email service configuration attributes

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

6.14.1. Configuring whether to receive email alerts

To configure whether to receive email alerts:

1. Sign in as an Administrator.

2. From the **Profile menu** in the header, select **Preferences**.

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

See also

Configuring email alert notification settings

Creating alerts

Deleting alerts

6.15. Setting the strategy for resolving issue audit conflicts

If multiple auditors are working on the same issue using different products (Application Security, Fortify Audit Workbench, or any of the Secure Code Plugins), they might assign different values to a given custom tag. Previously, if Application

Security 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 Application Security.

> **Note**
> Conflict resolution is not necessary if these auditors work within the same Application Security instance.

Example of the default strategy for resolving audit conflicts

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

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

Application Security 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 Application Security.

On a different Fortify Audit Workbench instance, user B sets custom tag values for the same issues that user A audited and uploads the results to Application Security. Application Security 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: Application Security ignores the audit results from user B and retains the values set by user A.

Application Security applies this strategy across all application versions.

You can change this strategy so that Application Security 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 Application Security uses to resolve audit conflicts:

1. Sign in to Application Security as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Configuration**, and then select **Issue Audit**.
4. From the **Issue audit conflict resolving strategy** list, select one of the following:
    - **Conflicts are resolved in favor of the SSC changes** (the default)
    - **Conflicts are resolved in favor of the most recent changes**
5. Click **SAVE**.
6. To implement your changes, restart Application Security server.

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

6.16. Configuring Java Message Service settings

If you want to publish system events to the Java Message Service (JMS), configure the JMS integration attributes in the Administration view.

To configure JMS settings:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Configuration**, and then select **JMS**.
3. On the **JMS** page, configure the settings as described in the following table.

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

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

6.17. About Application Security user authentication

By default, when a user logs on to Application Security or uses one of the OpenText Application Security Tools to upload Fortify project results (FPR) files, Application Security 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 Application Security user accounts and roles. You can augment the Application Security default database-only authentication using LDAP or a SCIM 2.0 API client. For Information about LDAP user authentication, see LDAP user authentication. For Information about SCIM 2.0 user provisioning, see Implementation of SCIM 2.0 protocol.

6.18. LDAP user authentication

Active Directory/LDAP integration enables Application Security to authorize users based on their existing corporate credentials. In addition, assignment by group or organizational unit enables Application Security to take advantage of the existing joiners/leavers processes. A new person who joins a group automatically has access to Application Security. A person who leaves a group automatically loses access.

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

Important

- OpenText recommends that, before you configure LDAP servers, you create at least one local Administrator account in case you encounter problems with your LDAP server.
- Although OpenText supports the use of multiple LDAP servers, it does not support the use of multiple LDAP servers behind a load balancer, unless those servers are identical.

See also

Registering LDAP entities

About managing LDAP user roles

6.18.1. Preparing to configure LDAP authentication

Before you configure Application Security 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 JXplorer.

Create an LDAP account for Application Security to use.

Note

For information about how to configure the primary source for looking up users, see Configuring core settings.

Important

Never use a user account name to provide Application Security access to an LDAP server.

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

  Note

  OpenText recommends that no user names in the Application Security be duplicated on an LDAP server.

- Gather and record required Information.
- OpenText recommends that you disable the referrals feature.
  See About the LDAP server referrals feature and Disabling LDAP referrals support.

See also

Configuring LDAP servers

6.18.2. Requirements for multiple LDAP servers

To use more than one LDAP server, the following requirements apply:

- **Usernames must be unique across all of the LDAP servers:**
  OpenText strongly recommends that usernames be unique across all LDAP configurations. Application Security searches for users based on the usernameAttribute specified for a given LDAP server configuration. Because the searches are performed across all the servers, it is important that the searches return just a single result. Be sure to use username attributes that result in unique search hits across all your configured LDAP servers. For example, if you use multiple Active Directories, it might make sense to use `userPrincipalName` as the username attribute in your configurations instead of the default `sAMAccountName`, which might not be unique across AD servers.
  If this requirement is not satisfied...
  In some circumstances, it might be difficult for administrators to avoid duplicate usernames. If Application Security finds a given username in more than one LDAP server during login, it tries to resolve this by using the password with all instances of the username, and then uses the instance that the password authenticates first. In most cases, a user with a non-unique username can successfully sign in to Application Security and access most of the user interface functionality. However, some functionality, including report generation, token-based authentication, and OpenText Fortify ScanCentral DAST integration, is not supported for such users.
- **Separate LDAP server configurations must manage completely independent namespaces (trees)**
  This requirement ensures unique lookup of LDAP DNs by Application Security. The simplest (and recommended) way to achieve this is to ensure that none of the configured baseDNs is a suffix of any of the others.
  In more complex cases, it might be possible to delegate a subtree to be managed by a second LDAP server configuration. In that case, however, all transitive DN references (for example, group member DNs) must also be managed by the second LDAP server. For example, if you have one LDAP server configuration with the base DN `DC=acme,DC=com`, but the `OU=org,DC=acme,DC=com` subtree is managed by another LDAP server, you can set up a second LDAP configuration to manage just the `OU=org,DC=acme,DC=com` LDAP subtree. But you *must* ensure that none of the LDAP objects registered in Application Security from the first LDAP server reference (directly or transitively) the `OU=org,DC=acme,DC=com` subtree, and vice versa.
  If this requirement is not satisfied...
  If an LDAP object DN matches the base DN of more than one LDAP server, Application Security performs a lookup against the LDAP server whose base DN best matches the given LDAP object DN. This might lead to Application Security using the data of unintended LDAP object in processing and result in unexpected behavior.

6.18.3. 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 redirects a client request to another server. The server sends the referral 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 Application Security requests an LDAP object and this object is a referral, Application Security 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, OpenText recommends that you disable referrals support in the LDAP library. Disabling this option on the Application Security server side makes Application Security-to-LDAP communication much faster. For instructions, see Disabling LDAP referrals support.

Note

For a complete description of referrals, go to Referrals in the LDAP in the Oracle documentation.

6.18.4. Disabling LDAP referrals support

To disable referrals support:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Configuration**, and then select **LDAP Servers**.
3. 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** area.
6. From the **LDAP referrals processing strategy** list, select **ignore**.
7. Click **SAVE**.

6.18.5. Configuring LDAP servers

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

Important

Before you configure the properties on the **LDAP** page, you must prepare for LDAP authentication as described in LDAP user authentication. That section includes requirements and recommendations for configuring multiple LDAP servers.

Important

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

To configure an LDAP server connection for Application Security:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Configuration**, and then select **LDAP Servers**.
3. On the **LDAP servers** page, click **NEW**.
4. In the **CREATE NEW LDAP CONFIGURATION** dialog box, configure the settings described in the following table.

Field	Description
BASIC SERVER PROPERTIES	
Enable this LDAP configuration	Select this check box to make this LDAP server available for Application Security to use.
Server name	Type a unique name for this server. **Important** If you configure multiple LDAP servers, ensure that you specify a unique server name for each.

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

Base DN	Type the base distinguished name (DN) for LDAP directory structure searches. **Important** If you configure more than one LDAP server for Application Security, then you must set a unique base DN for each of them. For example, the base DN for `companyName.com` is `dc=companyName,dc=com`. All DN values are case-sensitive, must not contain extra spaces, and must exactly match LDAP server entries. If you specify no value, Application Security searches from the root of LDAP objects tree. With multiple LDAP servers, the base DN must be unique for each. If the base DN for one server is empty, it cannot be empty for another LDAP server.

Bind user DN	Type the full distinguished name (DN) of the account Application Security uses to connect to the authentication server. Use a dedicated LDAP service account for the bind account. Do not use this account as a standard user account to login to Application Security. This account must be a minimum privilege, read-only authentication server account that you created for exclusive use by Application Security. **Important** For security reasons, never use a real user account name in a production environment. If you use Active Directory, specify the domain name and username in the following format: `<domain_name>\<username>`
Bind user password	Type the password for the bind user DN account.
Show password	Select this check box to show entered passwords.

Relative search DNs (1 per line)	(Optional) Type the relative distinguished name (RDN). An RDN defines the starting point from the base DN for LDAP directory searches. OpenText recommends that you search from the base DN. However, if your LDAP directory is so large that searching for Application Security 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 Application Security for security reasons.
	For example, to search within the base DN companyName.com and all entries under that base DN, specify the following to recursively search all entries under that path:
	`cn=users`
	or
	`cn=users,ou=divisionName`

Ignore partial result exception	To avoid search failures when search results include more records than the LDAP server can return, leave this check box selected. You can also enable this setting 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 setting enabled, Application Security silently returns only 500 records.
LDAP server type	From this list, select the type of LDAP server you are connecting with Application Security (either **ACTIVE_DIRECTORY** or **OTHER**).
SECURITY	

SSL trust check	If the domain controller is enabled for SSL, leave this check box selected to verify that the certificate presented by the LDAP server was issued by a trusted authority. If the domain controller is not configured for SSL, clear this check box.
Hostname validation	If the domain controller is enabled for SSL, leave this check box selected to ensure that the LDAP server hostname matches the hostname for which the certificate was issued. If the domain controller is not configured for SSL, clear this check box.
Enable user status mapping	(Microsoft Active Directory only) Select this check box to enable Application Security to retrieve status information for users on this LDAP server. The information enhances authentication checks during token-based and SSO-based authentication schemes.
BASE SCHEMA	
Object class attribute	Type the class of the object. For example, if this is set to `objectClass`, Application Security looks at the `objectClass` attribute to determine the entity type to search. The default value is `objectClass`.
Organizational unit class	Type the object class that defines an LDAP object as an organizational unit. The default value is `container`.
User class	Type the object class that identifies an LDAP object type as a user. The default value is `organizationalPerson`.
Organizational unit name attribute	Type the group attribute that specifies the organizational unit name. The default value is `cn`.
Group class	Type the object class that identifies an LDAP object type as a group. The default value is `group`.
Distinguished name (DN) attribute	Type the value that determines the attribute Application Security looks at to find the distinguished name of the entity. The default value is `distinguishedName`.
USER LOOKUP SCHEMA	
User firstname attribute	Type the user object attribute that specifies a user's first name. The default value is `givenName`.
User lastname attribute	Type the user object attribute that specifies a user's last name. The default value is `sn`.
Group name attribute	Type the group attribute that specifies the group name. The default value is `cn`.
User username attribute	Type the user object attribute that specifies a username. The default value is `sAMAccountName`.

User password attribute	Type the user object attribute that specifies a user's password. The default value is `userPassword`.
Group member attribute	Type the group attribute that defines the members of the group. The default value is `member`.
User email attribute	Type the user object attribute that specifies a user's email address. The default value is `mail`.
User memberOf attribute	Type the name of an LDAP attribute that includes the LDAP group names for LDAP users.
USER PHOTO	
User photo enabled	Select this check box to enable the retrieval of user photos from the LDAP server.
User thumbnail photo attribute	The thumbnailPhoto attribute for Active Directory
User thumbnail MIME default attribute	**Thumbnail MIME default attribute**
ADVANCED INTEGRATION PROPERTIES	
Cache LDAP user data	Select this check box to enable LDAP user data caching in Application Security. You can refresh the LDAP cache manually from the Administration view in Application Security. For instructions, see Refreshing LDAP entities manually. **Note** OpenText recommends that you leave LDAP user caching enabled. Application Security periodically updates the LDAP cache automatically.
Cache: Max threads per cache	Type the maximum number of threads dedicated for each update process (user action). Each time a user clicks **Update**, a new update process starts. The default value is `4`.
Cache: Initial thread pool size	Type the initial number of available cache update threads. This value configures 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. Not all LDAP servers support paging. Ensure that your LDAP server supports this feature.

Page size of LDAP search request results	If your LDAP server limits the size of the search results by a certain number of objects and **Enable paging in LDAP search queries** is selected, type a value that is less than or equal to your LDAP server limit. The default value is `999`.
LDAP referrals processing strategy	If you have only one LDAP server, OpenText recommends that you select **ignore**so that LDAP works faster. If you have a multi-domain LDAP configuration and you use LDAP referrals, select `follow`. The default value is `ignore`. **Note** If referrals are not used on your LDAP server, seeAbout the LDAP server referrals feature.
LDAP authenticator type	From this list, select one of the following LDAP authentication types to use: ○ **BIND_AUTHENTICATOR**— Authentication directly to the LDAP server ("bind" authentication). ○ **PASSWORD_COMPARISON_AUTHENTICATOR**—The password the user supplies is compared to the one stored in the repository. For more information about LDAP authentication types, go to https://spring.io/projects/spring-security.
LDAP password encoder type	Select a value from this list only if the LDAP authentication method is password comparison. You must select the encoder type that the LDAP server uses. Application Security compares encoded passwords. If, for example, the LDAP server uses LDAP_SHA_PASSWORD_ENCODER to encode passwords, but you select **MD4_PASSWORD_ENCODER**, password comparisons will fail.
Enable nested LDAP groups	Select this check box to enable nested group support for LDAP in Application Security (wherein a given group member might itself be a group). **Note** Use nested LDAP groups only if absolutely required. Enabling nested LDAP groups forces Application Security to perform extra tree traversals during authentication. OpenText strongly recommends that you clear this check box if you do not plan to use nested groups.

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

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

> **Important**
> If you configure multiple LDAP servers, ensure that you specify a unique server name and a unique Base DN for each.
> Although OpenText supports the use of multiple LDAP servers, it does not support the use of multiple LDAP servers behind a load balancer, unless those servers are identical.

See also

Editing an LDAP server configuration

Importing an LDAP server configuration

LDAP user authentication

Registering LDAP entities

Deleting an LDAP server configuration

About managing LDAP user roles

6.18.5.1. Editing an LDAP server configuration

To edit an LDAP server connection:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Configuration**, and then select **LDAP Servers**.
3. On the **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.
6. To check the validity of the configuration, click **VALIDATE CONNECTION**.
7. To save the configuration after successful validation, click **SAVE**.

See also

Registering LDAP entities

LDAP user authentication

About managing LDAP user roles

6.18.5.2. Deleting an LDAP server configuration

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

To delete an LDAP server configuration:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Configuration**, and then select **LDAP Servers**.
3. Do one of the following:
   - On the **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 **LDAP Servers** page, click the LDAP server connection that you want to delete, and then, click **DELETE**.
4. To confirm that you want to proceed with the LDAP configuration, click **OK**.
5. To force all LDAP users to re-authenticate, restart the Application Security server.

See also

LDAP user authentication

Registering LDAP entities

About managing LDAP user roles

6.18.5.3. Importing an LDAP server configuration

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

To import your legacy LDAP server configuration:

1. On the header, click **Administration**.
2. On the navigation pane, select **Configuration**, and then scroll down and select **LDAP Servers**.
3. On the LDAP Servers header, click **IMPORT**.
4. In the **IMPORT LEGACY LDAP CONFIGURATION** dialog box, manually copy the content of your legacy `ldap.properties` file for the LDAP configuration to import, and paste it into the text box.
   If Application Security detects problems with the copied content, it displays a message and a link to click for more information.

   Note

   The encoded Bind User DN (`ldap.user.dn`) and Bind User Password (`ldap.user.password`) values are not imported. You must enter these manually (see Configuring LDAP servers).

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

See also

Registering LDAP entities

LDAP user authentication

About managing LDAP user roles

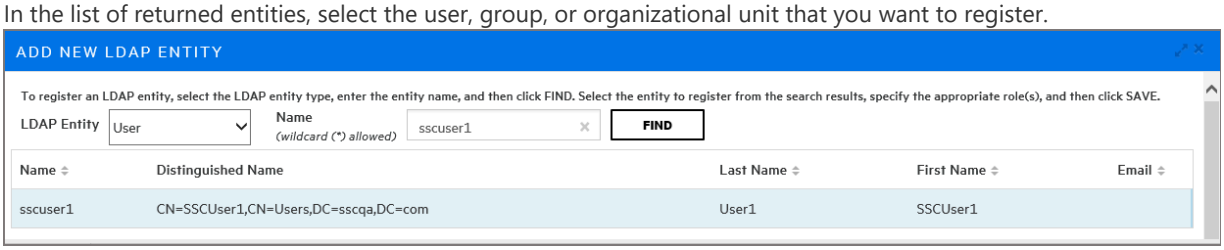
6.18.5.4. Registering LDAP entities

As an Administrator, you can add LDAP groups, organizational units, and users to the list of Application Security users. Application Security automatically updates access control as users join and leave groups.

To register an LDAP organizational unit, group, or user with Application Security:

1. Sign in to Application Security as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Users**, and then select **LDAP Entities**.
4. On the **LDAP** toolbar, click **+ADD**.

5. From the **LDAP Entity** list, select the type of LDAP entity you want to register (**Group**, **User**, or **Organizational Unit**).
6. In the list of returned entities, select the user, group, or organizational unit that you want to register.



7. In the **Roles** section, select the check boxes that correspond to the roles you want to assign to the selected entity.
8. To give 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.

   1. Click **+ ADD**.
   2. From the **Application** list in the **SELECT APPLICATION VERSION** dialog box , select the name of an application that you want the LDAP entity to access.
      Application Security lists all active versions of the application.
   3. To display inactive versions of the application, select the **Show inactive versions** check box.
   4. Select the check boxes for all of the versions that you want the entity to access.
   5. Click **DONE**.

   The **Access** section lists the application versions you selected.
9. 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**.

Application Security adds the entities to its list of users and periodically refreshes the LDAP server cache automatically.

For information about how to configure LDAP servers, see Configuring LDAP servers.

See also

LDAP user authentication

About managing LDAP user roles

6.18.5.5. Refreshing LDAP entities manually

Application Security 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. Sign in as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, select **Users**, and then select **LDAP Entities**.
4. In the list of LDAP entities, select the check box for the LDAP entity to refresh.
5. On the **LDAP** toolbar, click **REFRESH**.

For information about how to configure LDAP servers, see Configuring LDAP servers.

See also

LDAP user authentication

Registering LDAP entities

About managing LDAP user roles

6.18.5.6. Handling LDAP entries marked "Invalid"

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



Note

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

To update the DN value for an LDAP entity:

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

See also

Configuring LDAP servers

6.18.6. Enabling persistence of the LDAP cache

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



Note

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

To enable the LDAP cache to persist after server shutdown:

1. Shut down Application Security.
2. Open the `<fortify.home>/<app_context>/conf/app.properties` file in a text editor.

- Set the `ldap.cache.persistence.enabled` property to `true`.
- Save and close your `app.properties` file.
- Restart Application Security.

Changing the default cache refresh interval

The default cache refresh interval is five hours. If large LDAP groups are registered with Application Security, a frequent cache refresh can place an extra load on Application Security and the LDAP server and thereby affect performance.

To reduce the impact, you can increase the interval, as follows:

1. Shut down Application Security.
2. Open the `<fortify.home>/<app_context>/conf/app.properties` file in a text editor.
3. Add the following line:

   ```
   ldap.cache.refresh.interval.hours=<whole_number_between_1_and_12>
   ```

4. Restart Application Security.

6.19. Implementation of SCIM 2.0 protocol

When you enable System for Cross-domain Identity Management (SCIM) in Application Security, a SCIM 2.0 API client pushes users and groups to Application Security using the SCIM 2.0 protocol for provisioning and managing identity data. This means that you do not have to go through the Application Security Administration view to add users. Instead, you configure users and groups from the SCIM 2.0 API client.



Note

You can integrate with any SCIM 2.0 API client. However, if you do, you must test its interoperability with Application Security independently. Only Microsoft Entra ID integration is officially supported.

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

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

Supported SCIM resources

Application Security supports the following SCIM resources:

- User (`urn:ietf:params:scim:schemas:core:2.0:User schema`)
  Application Security accepts all standard attributes of the User Schema, but stores only a subset of these (see User attribute mappings). Also accepts Enterprise User extension attributes
  (`urn:ietf:params:scim:schemas:extension:enterprise:2.0:User schema`) but does not store them.
- Group (`urn:ietf:params:scim:schemas:core:2.0:Group schema`)
  Application Security accepts all standard attributes from the Group Schema, but stores only a subset of these (see Group attribute mappings).

Optional features supported:

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

User attribute mappings

The following table shows how SCIM user attributes map to Application Security user attributes.

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

Group attribute mappings

The following table shows how SCIM group attributes map to Application Security group attributes.

SCIM group attribute	Application Security group attribute	Comment
meta.created	created	Read-only
meta.lastModified	lastModified	Read-only
id	N/A	Read-only, Unique, Opaque
displayName	name	Required
members	N/A	Must reference existing users and / or groups

See also

Using SCIM 2.0 and SAML 2.0 to configure a connection to Microsoft Entra ID for user provisioning

Configuring Application Security to work with SAML 2.0-compliant single sign-on

6.19.1. Using SCIM 2.0 and SAML 2.0 to configure a connection to Microsoft Entra ID for user provisioning

You can use the System for Cross-domain Identity Management (SCIM) protocol to provision Application Security with user accounts from Microsoft Entra ID. The following table lists the tasks required to use this feature, in the order in which they must be performed.

Task	For details
Enable SCIM from Application Security.	Enabling SCIM for provisioning of externally managed users and groups
In Microsoft Entra, go to Microsoft Entra ID and create an enterprise application.	Microsoft Entra ID documentation **Note** When Entra ID prompts you to indicate what you want to do with the new application, select the **Integrate any other application you don't find in the gallery (Non-gallery)** option.
From Entra ID, assign users and groups to the new application.	Microsoft Entra ID documentation
From Entra ID, provision the application. Note the following: • Set **Provisioning Mode** to **Automatic**. • Use the Application Security URL for the **Tenant URL** value, and append to it the following string: `/api/scim/v2?aadOptscim062020` **Note** `/api/scim/v2` is the URL for the Application Security SCIM endpoint. The `aadOptscim062020` query parameter improves Entra ID compliance with SCIM v2.0. • For the **Secret Token** value, use the token you created in Application Security (**SCIM Token** - see Enabling SCIM for provisioning of externally managed users and groups.)	Microsoft Entra ID documentation

From Entra ID, change the attribute mappings for data flow between Entra ID and Application Security. Delete all but the following attributes for your users (for groups, you change no attribute mappings): • userName • active • emails[type eg "work"].value • name.givenName • name.familyName • externalID Ensure that you move the **Provisioning Status** toggle to **On**.	Microsoft Entra ID documentation
Entra ID SAML metadata is signed. For Application Security to successfully verify the signature, you must download the SAML signing certificate from Entra and import it into the keystore to be used in the SSO SAML configuration (SAML keystore location). In Entra, go to the created enterprise application. On the SAML-based Sign-on page, download the signing certificate, and then import it into the keystore.	Microsoft Entra ID documentation Configuring Application Security to work with SAML 2.0-compliant single sign-on
Set up SAML single sign-on from Application Security.	Configuring Application Security to work with SAML 2.0-compliant single sign-on
Acquire the metadata XML file from Application Security and save it locally. This file can be accessed only if SAML SSO is enabled in Application Security and successfully initialized.	`<hostname>:<port>/<app_context>/saml/<metadata>`
In Entra, upload the saved metadata file, and then complete the SAML single sign-on setup using data from the uploaded metadata file.	Microsoft Entra ID documentation
From Application Security, assign roles and application versions to externally managed users and groups.	Viewing externally managed users and groups

6.19.2. Enabling SCIM to provision externally managed users and groups

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

1. Sign in as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Configuration**, and then select **SCIM**.
4. Select the **Enable SCIM** check box.
5. In the **SCIM Token** box, enter the SCIM token you want to use as a bearer token to authenticate with the Application Security SCIM API.

Use that token as a Secret Token in Entra ID when you configure the connection between Application Security and Entra ID.

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

6. Click **SAVE**.

See also

Configuring Application Security to work with SAML 2.0-compliant single sign-on

Implementation of SCIM 2.0 protocol

Viewing externally managed users and groups

6.20. Configuring a proxy for integrations

You can configure a single proxy for use with all HTTP(s) protocol-based integrations with Application Security. After you configure the proxy, you can then enable its use for components such as Fortify Audit Assistant, the Rulepack update server URL, and bug tracking plugins.

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

1. On the header, select **Administration**.
2. On the navigation pane, expand **Configuration**, and then select **Proxy**.
   On the **Proxy** page, provide values for the settings described in the following table.

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

3. Click **SAVE**.

See also

Configuring Fortify Audit Assistant

Configuring core settings

Assigning a Bug Tracking System to an Application Version

6.21. Enabling the running and management of OpenText ScanCentral DAST scans

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

To enable integration with OpenText Fortify ScanCentral DAST, you need to do the following in Application Security:

1. Create a service account for OpenText Fortify ScanCentral DAST to authenticate with Application Security. For instructions on how to use this service account in the OpenText Fortify ScanCentral DAST deployment, see the *OpenText™ Fortify ScanCentral DAST Configuration and Usage Guide*. The service account must meet the following requirements:
    - The account must be a local user account that has the Administrator role. Do not use an externally-managed account such as an LDAP- or SCIM-based user account.
    - The account must be a dedicated account that is only used for the integration of OpenText Fortify ScanCentral DAST and Application Security. Do not use the account for access by an OpenText Fortify ScanCentral DAST user.
2. Enable OpenText Fortify ScanCentral DAST integration in Application Security by doing the following:
    1. Sign in to Application Security as an Administrator.
    2. On the header, select **Administration**.
    3. On the navigation pane, expand **Configuration**, and then select **ScanCentral DAST**.
    4. On the **ScanCentral DAST** page, select the **Enable ScanCentral DAST** check box.
    5. In the **ScanCentral DAST server URL** box, type your OpenText Fortify ScanCentral DAST server URL. The OpenText Fortify ScanCentral DAST server URL should resemble one of the following:
       `http://<DAST_API_Host>:<port>/api/`
       `http://<DAST_API_IP>:<port>/api/`
       You can use the https protocol instead.

       Important
       Ensure that you include the trailing `/api/` in the URL.

    6. Click **SAVE**.

See the *OpenText™ Fortify ScanCentral DAST Configuration and Usage Guide* for information about how to perform the following tasks:

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

6.22. Configuring a Kafka Stream to use with OpenText ScanCentral DAST

As an optional configuration, you can deploy the Apache® Kafka® service to synchronize issue audit changes in Application Security with OpenText Fortify ScanCentral DAST.

To configure Application Security to stream audit history changes to Kafka:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Configuration**, and then select **Kafka Stream**.
3. On the **Kafka Stream** page, configure the settings as described in the following table.

Field	Description
Enable streaming audit updates to Kafka	Select this check box to synchronize changes to audit history from Application Security to Kafka.
A comma-separated list of Kafka bootstrap servers	Specifies a comma-separated list of brokers for the Kafka instance. Use the following syntax for this list: `<host1>:<port1>,<host2>:<port2>,...`
The Kafka topic to which audit updates are published	Specifies the Kafka topic for finding audit events.
Kafka Security	
Enable TLS mutual auth for Kafka streaming	Select this check box to enable mutual authentication using two-way SSL protocol to communicate with the Kafka brokers. Application Security supports two-way SSL using TLSv1.2 and TLSv1.3. If you do not select this check box, PLAINTEXT is used as the security protocol to communicate with the Kafka brokers.
Truststore file location	Specifies the path to the trust store file that contains trust store certificates in JKS file format.
Truststore password	Specifies the password for the trust store file.
Keystore location	Specifies the path to the key store file that contains the client's public and private keys in JKS file format.
Keystore password	Specifies the password for the key store file.
Private key password	Specifies the password for the private key.
Enable hostname validation of Kafka server	Select this check box to verify the Kafka server's fully qualified domain name (FQDN) or IP address against the actual hostname or IP address of that Kafka server to ensure that you are connecting to the correct Kafka server.

4. Click **SAVE**.

For more information about generating valid credentials and configuring client security, see the Apache Kafka documentation.

6.23. Enabling integration with Fortify ScanCentral SAST

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



Note

For information about how to install, configure, and use OpenText Fortify ScanCentral SAST, see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

To configure the integration:

1. Sign in to Application Security as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Configuration**, and then select **ScanCentral SAST**.
4. On the **ScanCentral SAST** page, select the **Enable ScanCentral SAST** check box.
5. In the **ScanCentral Controller URL** box, type the URL for your Controller.

   > **Important**
   > The Controller must be the same or later version as Application Security.

6. In the **ScanCentral poll period (seconds)** box, type the number of seconds to elapse between sessions of data polling from OpenText Fortify ScanCentral SAST.
7. In the **SSC and ScanCentral controller shared secret** box, type the shared secret key (unencrypted) so that Application Security can request data from the Controller.
   If you use clear text, this string must match the value stored in the Controller `config.properties` file for the `ssc_scancentral_ctrl_secret` property.
   The Controller verifies the shared secret key when requested for administration console data.
8. Click **SAVE**.
9. Restart the Application Security server.

See also

OpenText Fortify ScanCentral SAST permissions

Viewing OpenText Fortify ScanCentral SAST Controller information

About OpenText Fortify ScanCentral SAST sensor pools

Creating OpenText Fortify ScanCentral SAST sensor pools

6.24. Configuring job scheduler attributes

You can configure scheduling attributes for processing Application Security background jobs.

To configure job scheduler settings:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Configuration**, and then select **Scheduler**.
3. On the **Scheduler** page, configure the settings as described in the following table.

Field	Description
Number of days after which executed jobs are removed	Type the number of days after which finished jobs are removed. The default value is `1` (day). Canceled jobs are removed daily.
Pause job execution	This check box (not selectable from the **Scheduler** page) shows whether job execution has been paused (from the **Maintenance** page) in preparation for server shutdown / system maintenance. To proceed to the **Maintenance** page to select or clear this check box, click the **here** link. A change to this setting takes effect immediately after you save the change from the **Maintenance** page. No server restart is required. After you pause job execution, jobs (artifact processing, report generation, data export requests, and so on) that are currently running continue to completion. Any new jobs submitted are queued for processing after the **Pause job execution** check box is clear and regular processing resumes. **Important** OpenText strongly recommends that you pause job execution immediately before server shutdown, and keep it paused for as short a period of time as possible. This prevents a high volume of jobs from queuing up for processing later. **Caution** Job execution does not automatically resume after the server comes back up after maintenance. To resume job execution, you must return to the **Maintenance** page and clear the **Pause job execution** check box.
Token management	
Token expiration alerts	Type the number of days before token expiration that users are notified of the upcoming expiration. Valid values range from `3` to `30` days, inclusive. The default value is `7` (days). **Note** The start of the day is 12 AM in the Application Security server locale.

Snapshot refresh Use the fields in this area to schedule the snapshot job.
A snapshot is application version information captured at a given moment in time. This information includes variables and performance indicator values, which calculates application versions trends at the scheduled times.

> **Note**
> The values you enter in the **Days of the week**, **Hours**, and **Minutes** boxes are concatenated to create the cron expression the scheduler uses.

Days of the week	Use cron syntax to specify the days of the week on which the historical snapshot job is to be run. You can use a three-letter abbreviation for the day of the week (for example, enter `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, enter `SUN,WED,FRI` or `1,4,6`. **Note** Use uppercase letters for three-letter abbreviations. Spaces between the entries are optional. To specify consecutive days, separate the entries with a dash. For example, enter `MON-FRI` to run the scheduler on week days only. Enter an asterisk (`*`) run the scheduler every day (the default).
Hours	Type the hour, using 24-hour time notation, at which the recurring scheduler job is to start running. For example, enter `1` to start the job at 1 AM. Enter an asterisk (`*`) to run the scheduler every hour. The default value is `0` (midnight).
Minutes	Type the minute at which the recurring scheduler job is to start running. For example, enter `24` to start the job at 24 minutes past the hour that you entered in the **Hours** box. The default value is `0`, which indicates that the job starts running in the first minute.

Index maintenance Use the fields in this area to schedule your Application Security full text search index maintenance. OpenText recommends that you run this job daily.

> **Note**
> The values you enter in the **Days of the week**, **Hours**, and **Minutes** fields are concatenated to create the cron expression the scheduler uses.

Days of the week	Use cron syntax 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, use `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, enter `SUN,WED,FRI` or `1,4,6`.  **Note** Use uppercase letters for three-letter abbreviations. Spaces between the entries are optional. To specify consecutive days, separate the entries with a dash. For example, enter `MON-FRI` to run the scheduler on week days only. Enter an asterisk (`*`) to run the scheduler every day (the default).
Hours	Type the hour, using 24-hour time notation, at which the recurring index maintenance job is to start running. For example, enter `1` to start the job at 1 AM. Enter an asterisk (`*`) to run the scheduler every hour. The default value is `0` (midnight).
Minutes	Type the minute at which the recurring index maintenance job is to start running. For example, enter `24` to start the job at 24 minutes past the hour that you entered in the **Hours** box. The default value is `0`, which indicates the job starts running in the first minute.
Events maintenance	
Days to preserve	Type the number of days after which Application Security removes past events. To specify no event removal, enter `0` (zero). Application Security uses the new value during the next run of the dedicated cleaning job. A new job is created daily at 11:30 PM and if it is not blocked, it starts its work immediately. The default value is `0`, which indicates that no cleanup occurs.
Reports maintenance	

Days to preserve	Type the number of days Application Security is to retain generated reports. The default value is `0`, which indicates that no cleanup occurs. To ensure that the cleanup job is not too time- or resource-intensive, each nightly run clears a maximum of 2000 old reports (and associated entities). Application Security then gradually cleans up the remaining reports over the following days.
Data export maintenance	
Days to preserve	Type the number of days Application Security is to retain exported audit reports. The default value is `2`. **Note** This job is run every day at 11:45 PM (23:45)
Snapshot Cleanup	
Days to preserve	Type the number of days Application Security is to retain snapshots without any associated artifact or project version. The default value is `0`, which indicates that no cleanup occurs.
Days of the week	Use cron syntax to specify the days of the week on which the snapshot cleanup job is to be run. The default value is `1`. You can enter the value as a three-letter abbreviation for the day of the week (for example, use `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, enter `SUN,WED,FRI` or `1,4,6`. **Note** Use uppercase letters for three-letter abbreviations. Spaces between the entries are optional. To specify consecutive days, separate the entries with a dash. For example, enter `MON-FRI` to run the scheduler on week days only. Enter an asterisk (`*`) to run the scheduler every day (the default).

Hours	Type the hour, using 24-hour time notation, at which the snapshot cleanup job is to start running. For example, enter `1` to start the job at 1 AM. Enter an asterisk (`*`) to run the scheduler every hour. The default value is `1` (midnight).
Minutes	Type the minute at which the snapshot cleanup job is to start running. For example, enter `24` to start the job at 24 minutes past the hour that you entered in the **Hours** box. The default value is `0`, which indicates the job starts running in the first minute.
Job execution time limit	Type the number of hours the snapshot cleanup job can run at a time. After this deadline, the job is shut down. The default value is `5`.

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

See also

Setting job execution priority

Configuring background job execution strategy

Canceling scheduled jobs

Recurring cleanup jobs

6.24.1. Setting job execution priority

All new jobs in Application Security 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 job queue. That is, the first job added to the queue is the first job processed. Jobs set with higher priority values are processed before those assigned lower priority.

As a Application Security Administrator or Security Lead, you can change the priority of scheduled jobs that are in the **Prepared** state. The possible job states are Prepared, Running, Finished, Failed, and Canceled.

To set the priority for a scheduled job:

1. On the header, select **Administration**.
2. On the navigation pane, select **Metrics & Tracking**, and then select **Jobs**.
3. On the **Jobs** toolbar, from the **Filter by state** list, select **Prepared**.
4. Click to expand the row for the job you want to re-prioritize.
5. From the **SET PRIORITY** list, select a priority.
   Changing job priority might affect other jobs in the queue. If the priority you set for a job potentially affects other jobs, a message informs you of the potential effect, and prompts you to confirm that you want to continue with the change.
6. To apply the priority change, click **OK**.

The jobs table now reflects the changed priority setting.

See also

Canceling scheduled jobs

Configuring job scheduler settings

6.24.2. Canceling scheduled jobs

As an Administrator or a Security Lead, you can cancel scheduled jobs that are still in the prepared state. The possible job states are Prepared, Running, Finished, Failed, and Canceled.

To cancel a job:

1. Sign in to Application Security as an Administrator or Security Lead
2. On the header, select **Administration**.
3. On the navigation pane, under **Metrics & Tracking**, select **Jobs**.
4. On the **Jobs** toolbar, from the **Filter by State** list, select **Prepared**.
5. Click the row for the job you want to cancel.
6. Click **CANCEL**.
7. To confirm the job cancellation, click **OK**.

See also

Configuring job scheduler attributes

6.25. Recurring cleanup jobs

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

Job name	Description	Affected tables	Default schedule
Data Export Cleanup	Removes exported data (such as CSV files) that were more than the specified number of days old (see Configuring job scheduler settings).	dataexport documentinfo datablob	Daily at 23:45 h For instructions on how to schedule this job, see Configuring job scheduler settings.
Event Log Cleanup	Removes event records older than the number of days specified on the **Scheduler** page.	eventlogentry	Daily at 23:30 h For instructions on how to schedule this job, see Configuring job scheduler settings.
Expired Tokens Cleanup	Removes expired tokens with elapsed expiration dates.	agentcredential	Daily, every six hours, starting at 00:00 h
ID Table Cleanup	Removes IDs, used for filtering while working with user permissions and generating reports.	id_table pv_id_table	Daily at 23:00 h For instructions on how to schedule this job, see Configuring job scheduler settings.
Job Cleanup	Removes finished jobs. Failed jobs are removed after the set number of days, beginning with their start time. Canceled jobs are cleaned up without regard to start time.	jobqueue	Daily at 23:00 h
Orphaned Data Cleanup	Removes metadata associated with attachments that are no longer needed.	documentinfo	Every Sunday at 23:30 h
Orphaned Source Files Cleanup	Removes source files that are no longer referenced by any existing issue.	sourcefile	Daily at 00:00 h Set using job.sourceFileCleanup.cron
Report Cleanup	Removes generated reports that are older than the number of days specified for **Days to preserve** on the **Scheduler** page.	savedreport documentinfo datablob	No cleanup scheduled For instructions on how to schedule this job, see Configuring job scheduler settings.

Job name	Description	Affected tables	Default schedule
Webhook History Cleanup	Removes old webhook event entries.	webhookhistory	Daily at 03:30 h
Index Maintenance	Resolves inconsistencies between global search (fulltext) indexes and existing database entries. For example, resulting from unclean server shutdown or indexing job failures.	N/A	Daily at 00:00 h For instructions on how to schedule this job, see Configuring job scheduler settings.
LDAP Refresh	Updates caches associated with LDAP entities.	N/A	Every 6 hours
Historical Snapshot	Re-creates out-of-date snapshots.	N/A	Daily at 00:00 h For instructions on how to schedule this job, see Configuring job scheduler settings.
Alert Reminder	Sends reminder alerts.	N/A	Daily at 03:00 h
Token Expiry Alerts	Notifies users of any tokens to expire soon.	N/A	Daily at 03:00 h

6.26. About data retention

Administrators can enable data retention and configure the default data retention policy to define the time period for which artifacts are retained in Application Security. You can configure the time period to retain the artifacts and the number of artifacts to retain per application version.

After the defined retention period is reached, the artifacts are eligible for purging from Application Security. You can schedule the data cleanup service that purges artifacts from Application Security when you enable data retention.



Caution

After an artifact is purged, the artifact is permanently removed from Application Security and cannot be recovered.

When you enable data retention, Application Security applies the default data retention policy across all applications. You can also configure individual application versions to opt-out of the default data retention policy.

This section contains the following topics:

- Enabling data retention
- Editing the default data retention policy

6.26.1. Enabling data retention

To enable the Application Security data retention policy:

1. Sign in as an Administrator and select **Administration**.

2. On the navigation pane, expand **Policies**, and then select **Data Retention Policy**.
   The **Data Retention** page lists the default data retention policy and any application versions that have no data retention policy applied.

3. Configure the settings on the **Data Retention** page as described in the following table.

Field	**Description**
Enable Data Retention Policy	Select this check box to enable the data retention feature.
Allow application versions to opt-out of the default policy	Select this check box to allow individual application versions to opt-out of the default policy.
Days of the week	(Required) Type one or more days of the week to run the data cleanup service. Use the values `1` to `7` to specify the day of the week (Sunday to Saturday) where `1` represents Sunday and `7` represents Saturday Use cron syntax to specify one or more days of the week as described in the following examples: ○ Single Day—To run the service only on one day of the week, enter a single digit. For example, enter `3` to run the service only on Tuesdays at the time specified in the **Hours** box. ○ Multiple Days—To run the service on multiple days, separate the entries with a comma. For example, enter `1,4,6` to run the service on Sunday, Wednesday, and Friday at the time specified in the **Hours** box. ○ Range of Days—To specify consecutive days, separate the entries with a dash. For example, enter `2-6` to run the service from Monday through Friday at the time specified in the **Hours** box. ○ Every Day—Enter an asterisk (`*`) to schedule the service every day at the time specified in the **Hours** box. **Note** To minimize the impact on the responsiveness of the system, OpenText strongly recommends that you enable the cleanup service only when the system is idle.

Hours	(Required) Type the time of day the data cleanup service will run. Use the values `0` to `23` to specify the time of day, using 24-hour time notation, where `0` represents 12 AM and `23` represents 11 PM. Use cron syntax to specify one or more hours in the day as described in the following examples: ○ Single Hour—To run the service only at a certain hour of the day, enter a single digit. For example, enter `3` to run the service between 3 AM and 3:59 AM on the specified days defined in the **Days of the week** box. ○ Multiple Hours—To run the service multiple times a day, separate each hour with a comma. For example, enter `4,18` to run the service at between 4 AM and 4:59 AM and again between 6 PM and 6:59 PM on the days specified in the **Days of the week** box. ○ Range of Hours—To run the service at consecutive hours in a day, separate the entries with a dash. For example, enter `3-6` (equivalent to `3,4,5,6`) to run the service between 3 AM to 6:59 AM on the days specified in the **Days of the week** box. ○ Multiple Hour Ranges—To run the service for consecutive hours in a day more than once or for consecutive hours in a day and at certain hours, separate the multiple range or values with a comma. For example, enter `3-5,17-19` to run the service between 3 AM and 5:59 AM and from 5 PM to 7:59 PM on the days specified in the **Days of the week** box. ○ Every Hour—Enter an asterisk (`*`) to schedule the service every hour on the days specified in the **Days of the week** box. **Note** To minimize the impact on the responsiveness of the system, OpenText strongly recommends that you enable the cleanup service only when the system is idle. Also, avoid scheduling the service from 10 PM to 3 AM (which corresponds to the cron values `22`, `23`, `0`, `1`, and `2`), because that is the period when other Application Security nightly maintenance jobs are scheduled to run by default.

4. Click **SAVE**.

See also

Editing the default data retention policy

6.26.2. Editing the default data retention policy

When you first enable the data retention policy, OpenText recommends that you leave the policy properties set to the maximum allowed values for a time to allow individual application versions to opt-out of the policy before the policy dictates to begin removing artifacts. You can edit the default data retention policy based on your requirements.

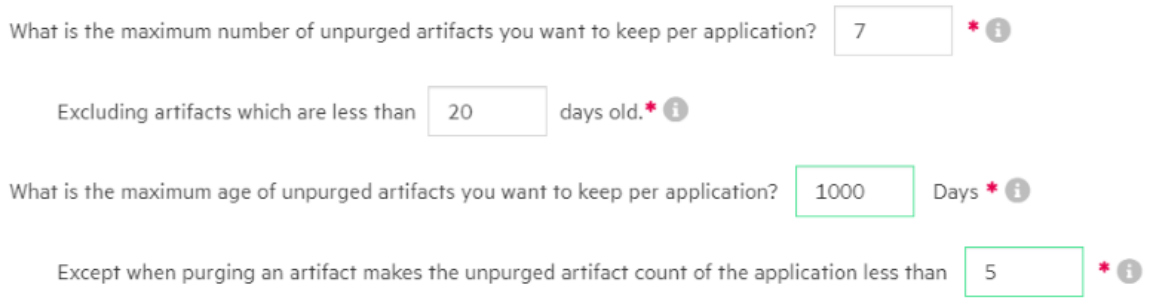
Purging artifacts under the default data retention policy depends on the following two rules.

- Rule 1—Number of artifacts > Maximum number of unpurged artifacts AND Artifacts Age > Minimum Age of the artifacts
- Rule 2—Age > Maximum Age AND Number of artifacts > Minimum number of unpurged artifacts

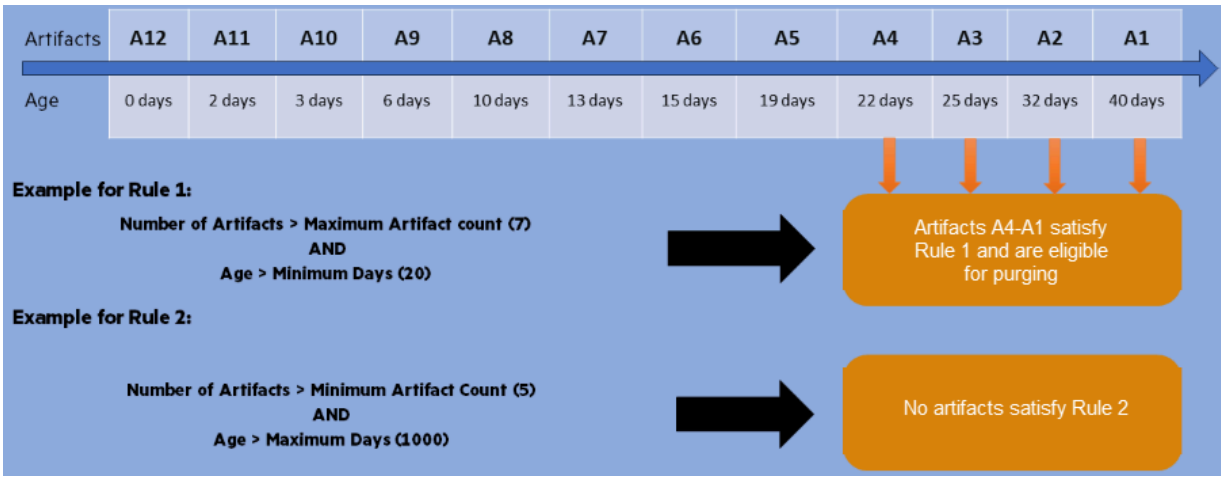
Data retention policy guidelines are evaluated for each analysis type and artifacts must satisfy at least one of the rules to be eligible for purging. If none of the rules are satisfied, the artifacts are retained regardless of the maximum artifact count or age that you specify.

To edit the default data retention policy:

1. Sign in as an Administrator and select **Administration**.
2. On the navigation pane, expand **Policies**, and then select **Data Retention Policy**.
3. On the **Data Retention** page, next to **Default data retention policy** click the **Edit Policy** button .
4. In the **Edit Policy** dialog box, configure the data retention policy settings based on your requirements.
   Consider the following scenario:
   An application version contains 12 artifacts, has a data retention policy enabled, and the default data retention policy is set with the following values:

   The following diagram shows how artifacts become eligible for purging under the default data retention policy for this scenario.

   Application Security purges the artifacts that satisfy at least one rule. Application Security purges artifacts A1 to A4.
5. Click **SAVE**.

6.27. Configuring secure browser access

To configure security for browsers that access the Application Security domain:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Configuration**, and then select **Security**.
3. On the **Security** page, configure the settings as described in the following table.

Field	**Description**
Content-Security-Policy	Specify what (if any) level of CSP to use. Using the HTTP Content-Security-Policy header controls, the resources browsers can load and what actions they can perform on pages loaded from Application Security. This helps guard against cross-site scripting attacks. Select one of the following options: ○ To restrict access to only the base URL configured by the `host.url` property (set using the Setup wizard), select **Strict**. ○ To enable a less restrictive policy than strict CSP, select **Relaxed**. This is the default setting. It allows access to the Application Security domain from any host:port. ○ To disable the Content-Security-Policy header, select **Disabled**. Although OpenText recommends that you *not* disable the Content-Security-Policy header, this option is available if CSP causes unexpected problems.
Set value for Strict-Transport-Security header	Type the value for the Strict-Transport-Security header. This header signals browsers to use HTTPS instead of HTTP to communicate with Application Security. **Important** 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. The Strict-Transport-Security header is sent only through a secure channel determined by Tomcat server.
Set value for Public-Key-Pins header	Type the value for the Public-Key-Pins header. This decreases the risk of man-in-the-middle (MITM) attacks. **Important** 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. The Public-Key-Pins header is sent only through a secure channel determined by Tomcat server.

4. Click **SAVE**.

6.28. About configuring Application Security to work with single sign-on

The following table lists the supported single sign-on solutions, and provides links to the instructions on how to configure Application Security to work with the following single sign-on (SSO) solutions.

Supported single sign-on solutions

SSO solution	Instructions
SAML 2.0-compliant single sign-on	Configuring Application Security to work with SAML 2.0-compliant single sign-on
HTTP headers	Configuring Application Security to work with single sign-on and single logout solutions that use HTTP headers
X.509 certification	Configuring Application Security to use X.509 certification-based SSO

Configuration restrictions

The following restrictions apply to configuring Application Security to work with SSO solutions:

- You can only use the SSO solutions that Application Security supports to give users access to the user interface.
- At any given time, you can configure only one SSO solution for use with Application Security.
- A user who wants to access Fortify Audit Workbench, fortifyclient, or any of the Secure Code Plugins, must use an LDAP or local Application Security user account and password to sign in.
- (X.509 SSO solution only) If you want users (local and LDAP) to be able to sign in using their user names and passwords, you must directly enable it.
  To improve application security, if X.509 SSO authentication is enabled, Application Security prevents both LDAP and local users from using user names and passwords to sign in locally. Users can only use the configured SSO method or an API token to access Application Security. To enable local login with the X.509 SSO solution configured, an Administrator must use the `sso.localAuthenticationEnabled` property located in the `app.properties` file. For information, see Configuring Application Security to use X.509 certification-based SSO.

See also

About session logout

6.28.1. Configuring SAML 2.0-compliant single sign-on

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

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



Note
Before you remove or replace the identity provider (for example, Okta), remove the users from Application Security first.

To configure Application Security to work with SSO that uses SAML 2.0:

1. If you are using an LDAP directory for users in Application Security and IdP, configure Application Security to use LDAP authentication. Otherwise, IdP users must match local users. For information, see LDAP user authentication.
2. If your IdP runs with SSL (https), configure Application Security to run with SSL. Otherwise, protocol switching while authenticating against IdP could interfere with authentication.

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

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

   Make a note of the values for the alias and both passwords. You must provide them later in the Application Security Administration view.
4. Get SAML metadata from the IdP server and store it on the Application Security file system.
5. Open the metadata file and make a note of the entityID for your IdP EntityDescriptor (<EntityDescriptor entityID="THE_VALUE_YOU_ARE_LOOKING_FOR">).
   Also check to see whether the metadata is signed (the <Signature> section is present). If the metadata is signed, the signature is verified with the PKIX validation algorithm and uses all public keys present in the keystore as trust anchors.
   Ensure that you include the root CA certificate and intermediary CA certificates of the signature in your keystore.
6. Sign in to Application Security and, on the header, select **Administration**.
7. On the navigation pane, expand **Configuration**, and then select **SSO**.
   You can configure only one single sign-on solution at a time.
8. From the **Enabled SSO** list, select **SAML**.
9. Provide the information described in the following table.

Field	Description
IdP metadata location	Location of your identity provider metadata (the metadata obtained in step 4). Examples ○ On Windows systems: `file:///C:/fortify/federation-metadata.xml` ○ On Linux systems: `file:///home/fortify/federation-metadata.xml` **Note** If you are integrating with Entra ID, enter the value shown in the **App Federation Metadata Url** field In Azure. (In the left pane in Azure, under **Manage**, select **Single sign-on**, and then select **SAML**. You can see the **App Federation Metadata Url** field under **SAML Signing Certificate**.) **Note** If your IdP is behind a proxy server, you must download IdP metadata to your local file system and reference it locally. Current SAML implementation does *not* support getting metadata over http proxy.
Default IdP	entityID of your IdP EntityDescriptor (from IdP metadata) **Note** If you are using the SCIM protocol to provision Application Security with user data from Entra ID, use the value shown in the **Azure AD Identifier** field in Entra ID. (You can see this field on the SAML-based Sign-on page under **Set up <*application_name*>**.)
SP entity ID	Service provider entity ID value must be a URL that does not exceed 1024 characters, and is globally unique across federations. OpenText recommends that you use the web address of a running Application Security instance.

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

10. Click **SAVE**.

Note
Select the **Enable IdP metadata signature verification** checkbox after generating the metadata, that is, after step15.

11. Verify that the `host.url` property in `<fortify.home>/<app_context>/conf/app.properties` designates a URL that the IdP server can access.
The URL is used as a base URL to construct <*AssertionConsumerService*> and <*SingleLogoutService*> locations in Application Security SAML metadata.

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

    Important

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

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

    Note

    Single logout initiated from Application Security works correctly, regardless of the cookie policy settings.

    To make single logout work in Chrome or Chromium-based browsers, you must change the `SameSite` policy for session cookies to `None`.

    Important

    This denotes a less secure policy than the default, so you must determine whether making the change is the best approach for your organization. To change the policy for container deployments, use the `HTTP_SERVER_SAME_SITE_COOKIES` environment variable. For non-container deployments, add `<CookieProcessor sameSiteCookies="none"/>` to the context section of your Tomcat configuration. For details, see the the Apache Tomcat 10 Configuration Reference documentation.

14. Restart Application Security.
15. Generate the Application Security (SP) metadata at `<hostname>:<port>/<app_context>/saml/metadata/<SP_alias>`.
16. Only if the IdP metadata is signed (the <Signature> section is present) (see, step 5), perform the following substeps else proceed with step 17:
    1. In the Application Security go to the **SSO** configuration page and select the **Enable IdP metadata signature verification** checkbox to verify the IdP metadata signature using the IdP provided public key (X.509 Certificate).
    2. Click **SAVE**.
    3. Restart Application Security.
17. Open the metadata generated in the previous step (step 15) and verify that the location URLs in `<AssertionConsumerService>` and `<SingleLogoutService>` are accessible from the IdP server.
18. Upload the Application Security metadata to the IDP server.
19. 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 Application Security.

Note

For information about how to obtain extra logging information related to SSO authentication, see Enabling debug logging for single sign-on authentication.

6.28.1.1. Troubleshooting SAML SSO integration

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

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

Issue: Users are authenticated with IdP, but Application Security does not authorize them.

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

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

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

See also

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

6.28.2. Configuring single sign-on and single logout solutions that use HTTP headers

To configure Application Security to work with SSO that uses headers:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Configuration**, and then select **SSO**.
   You can configure only one single sign-on solution at a time.
3. From the **Enabled SSO** list, select **HTTP**.
4. Provide the information described in the following table.

Field	Description
HTTP header for username	Type the HTTP header to use for SSO logons. The default value is *username*.
IdP login page	Type the URL for the identity provider login page.
SSO Logout page	Type the logout page address to which users are redirected after logging out of Application Security.
SSO Logout Response Header	Type the dynamic directive header.
SSO Logout Response Code	Type the dynamic directive code.
SSO Logout Response Text	Type the dynamic directive message.

5. Click **SAVE**.
6. Configure Application Security to use LDAP authentication.
   For details, see LDAP user authentication.
7. Restart the server.



Note

For information about how to obtain extra logging information related to SSO authentication, see Enabling debug logging for single sign-on authentication.

See also

Configuring Application Security to work with single sign-on

6.28.3. Configuring X.509 certification-based single sign-on

To configure Application Security to use X.509 certification-based SSO:

1. Configure X.509 client certification in Tomcat.

For information about certificateVerification and related options, see the Apache Tomcat documentation.

2. Sign in to Application Security as an Administrator.
3. On the header, select **Administration**.
4. On the navigation pane, expand **Configuration**, and then click **SSO**.
   You can configure only one single sign-on solution at a time.
5. From the **Enabled SSO** list, select **X.509**.
6. In the **X.509 certificate username pattern** box, type a regular expression for Application Security to specify how to retrieve the username from the client certificate, then do one of the following:
   - To retrieve the username from the X.509 certificate Subject field, use a regular expression with capturing groups. The regular expression is then used to match the username from the Subject field value.
     Example: To match the CN attribute of the certificate Subject field, specify the `CN=(.*?)` pattern.
   - To retrieve the username from the X.509 certificate Subject Alternative Name (SAN) extension Other Name, use `$0!OID$regex` pattern, where:
     - `OID` represents the identifier of the Other Name from which to retrieve the username. Only Other Names that contain string values are supported.
     - `regex` represents the regular expression with capturing group to use to retrieve the username from the Other Name value.

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

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

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

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

> **Important**
>
> If you configured X.509 certification-based SSO, and you want users (local and LDAP) to be able to sign in using their user names and passwords, you must directly enable it.

To enable user name and password login when you have X.509 SSO configured:

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

6.28.4. Enabling debug logging for single sign-on authentication

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

To obtain extra logging information related to SSO authentication:

1. Open the `<fortify.home>/<app_context>/conf/log4j2.xml` file in a text editor.
2. For SSO solutions that use HTTP headers, add the following logger definition to the `log4j2.xml` file:

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

3. For SAML 2.0-compliant single sign-on solutions, locate the section marked `<!-- SSO SAML -->`, and then change the level of each logger in that section to an appropriate debug value.

See also

Configuring Application Security to work with single sign-on

6.29. Configuring logging

Application Security uses Apache Log4j™ 2 for its logging services. The logging configuration is located in the `<fortify.home>/<app_context>/conf/log4j2.xml` file.

> **Important**
>
> Application Security manages the `log4j2.xml` file and it might be overwritten during restarts or upgrades. Do not use it for permanent configuration changes.

Changes to the configuration file while Application Security is running take effect in approximately 10 seconds (as defined by the value of the `monitorInterval` attribute in the configuration). You cannot add a new logger definition to the configuration and set a level for it. Only changes to existing loggers are picked up dynamically.

To implement persistent logging configuration changes, set up a custom Log4j2 configuration override file. Changes to the override configuration file without a Application Security restart follow the same rules as the main configuration file as previously described. The configuration from the provided `log4j2.xml` and the custom Log4j2 files are merged and in case of conflicts, the override configuration file takes precedence.

To create a custom Log4j2 override configuration file:

1. Copy the main `log4j2.xml` file and create an override configuration file.
2. Make changes to the override configuration file.
   You can add new appenders or loggers and modify existing ones in the override configuration file.
   The custom override configuration file format uses the same format as the main configuration file.
3. Set the `COM_FORTIFY_SSC_LOG4J2_OVERRIDE` system environment variable or the `com.fortify.ssc.log4j2.override` JVM system property to the absolute path for your custom Log4j2 configuration file.

You can use a Log4j2 override file to customize logging for troubleshooting. For example, you can use an override file to enable additional logging for SAML debugging.

When you deploy Application Security in Kubernetes, specify the location of the Log4j2 override file in the Application Security Helm chart by setting the `COM_FORTIFY_SSC_LOG4j2_OVERRIDE` environment variable:

```
environment:
 - name: COM_FORTIFY_SSC_LOG4j2_OVERRIDE
   value: /fortify/debug/saml-debug.xml
```

In this example, `/fortify/debug/saml-debug.xml` specifies the location of the Log4j2 override file used for SAML debugging.

Mirroring logs to the console

To mirror Application Security logs to the console, set the `COM_FORTIFY_SSC_LOG_CONSOLE` system environment variable to `true` before startup.

Application Security maps this environment variable to the `com.fortify.ssc.log.console` JVM system property at startup. If the JVM system property is already set, that value takes precedence.

When you enable this setting, Application Security applies the logging change within approximately 10 seconds, based on the configured `monitorInterval` value.

6.30. Running in a Federal Information Processing Standards (FIPS) environment

FIPS is a set of standards and guidelines for cryptographic modules and algorithms used by the U.S. government and other organizations. To be FIPS-compliant means that you are meeting the minimum security requirements defined by FIPS

publications. You can run Application Security in a FIPS-compliant environment running on Red Hat Enterprise Linux 9 (RHEL 9). While there is no configuration required to run Application Security in a FIPS environment, you must ensure that LDAP servers, SMTP servers, and webhooks are configured as secure connections or you will receive an error in Application Security.

For instructions on how to configure FIPS-compliant cryptography, see the RHEL 9 documentation.

Before you run Application Security in a FIPS environment:

- Ensure that you are using Application Security version 24.4.0 or later. Otherwise, you must migrate the Application Security keystore that stores a `secret.key` file to encrypt sensitive data.
  For more information, see About the <fortify.home> directory.
- Ensure that LDAP servers, SMTP servers, and webhooks are configured as secure connections.



Note

The Application Security container does not support enabling FIPS mode for Java.

6.31. Setting the required password strength for Application Security sign in

You can use the `password.strength.min.score` property (located in `<fortify.home>/<app_context>/conf/app.properties`) to adjust the required password strength. You can also import additional password dictionaries at `app.properties#password.strength.dictionary.location`.

The following table lists each valid property value and the strength it represents.

Password strength properties

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

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

Application Security uses the `zxcvbn4j` password generator (developed by Dropbox) to check password strength when creating new users or self-service password changes. Rather than the traditional hard-coded rules about password requirements, this library is inspired by password crackers and estimates password strength conservatively through pattern matching and other techniques. It recognizes and weighs:

- 30K common passwords
- Common names and surnames according to US census data
- Popular English words
- Common dates
- Repeats (`aaa`)
- Sequences (`abcd`)

- Keyboard patterns (`qwertyuiop`)
- L33t speak

See also

About session logout

Additional Application Security configuration

6.32. About audit issue history

You can view the changes in the attributes of an issue as you upload new scans for an audit. The issue history provides a list of all the changes made to an attribute value and the date and time the changes were made.

The issue history includes all the attributes that Application Security extracts from uploaded scans. Issue history only includes attributes that you can use for searching or filtering in the **AUDIT** page.

To enable audit issue history, see Enabling audit issue history.

The **Issue History** tab provides information for the following issue attributes:

Issue attributes		
analyzer	issueInstanceId	remediation_effort
accuracy	kingdom	rule
audience	likelihood	severity
category	line	sink
class	manual	source
codesnippet	mapped_category	sourcefile
confidence	min_virtual_call_confidence	sourceline
engine_priority	package	source_context
file	primary_context	taint
impact	probability	url



Note

- When you enable audit issue history, Application Security saves the list of attributes whose values have changed along with their old values and new values for any new uploaded FPR.
- Uploading scans that are older than the newest uploaded scan in an application version does not generate new changes for the issue history.
- Deleting FPRs from an application version results in the deletion of the issue history entries that were created by the upload of that FPR.
- Copying an application version does not include the existing issue history.

See also

Auditing Scan Results

6.32.1. Enabling audit issue history

To enable audit issue history:

1. Open the `<fortify.home>/<app_context>/conf/app.properties` file in a text editor.
2. Set the value of the `issue.attrChangelog.enabled` property to `true`.
3. Save and close the `app.properties` file.
4. Restart Application Security server.

Note

You can also enable audit issue history in the automatic Application Security configuration. The automatic configuration overrides any changes made to the `app.properties` file. For instructions, see Automating Application Security configuration.

See also

Audit Issue History

7. Additional installation-related tasks

This section describes additional tasks related to a new Application Security installation.

This section contains the following topics:

- About bug tracking system integration
- Adding and managing parser plugins
- About Application Security user administration
- Global search functionality in Application Security
- Placing Application Security in maintenance mode
- Pausing and resuming job execution
- About OpenText SAST Application Security Content
- Enabling OpenText SAST and OpenText Application Security Tools upgrades from Fortify Audit Workbench

7.1. About bug tracking system integration

Your team can submit bugs to your bug tracking system during issue auditing. Application Security supports integration with the following bug tracking systems:

- OpenText™ ALM Quality Center
- Azure DevOps Server

  Important

  - The **Repro Steps** field in Azure DevOps, which displays bug descriptions, is hidden by default for issue work items. If you use an Azure DevOps 2019.1 or later version, and you use the Basic process, you must customize Issue work items to see the **Repro Steps** field.
  - You must use a personal access token generated from Azure DevOps in the **Password** box at login. For more information about personal access tokens, see the Microsoft Azure DevOps Services documentation.

- Jira Software Server
- Jira Software Cloud
  You must use your Jira authentication token in the **Password** box at login.

If your organization uses a bug tracking system other than those that OpenText supplies, you can author a new plugin for that system. For instructions, see Authoring bug tracker plugins.

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.

7.1.1. Adding bug tracker plugins

As an Administrator, you can connect Application Security to third-party bug tracker plugins.

> **Important**
>
> You cannot use a proxy that has authentication and an HTTPS bug-tracker domain. 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. On the header, select **Administration**.
2. On the navigation pane, expand **Plugins**, and then select **Bug Tracking Plugins**.
3. On the **Bug Tracking** page, click **NEW**.
4. To accept the risk of uploading the plugin, click **OK**.
5. In the **UPLOAD PLUGIN BUNDLE** dialog box, click **BROWSE**, and then locate and select the JAR file for your plugin. You can use either a Application Security-provided JAR file, or the JAR file for a bug tracker plugin that you have authored.
   The provided JAR files for the bug trackers are in the following locations.

Bug tracker plugin	JAR file
Bug Tracker Plugin for ALM	`<ssc_distribution_dir>/plugins/BugTrackerPluginAlm/com.fortify.BugTrackerPluginAlm-<version>.jar`
Bug Tracker Plugin for Azure DevOps	`<ssc_distribution_dir>/plugins/BugTrackerPluginAzure/com.fortify.BugTrackerPluginAzure-<version>.jar`
Bug Tracker Plugin for Jira	`<ssc_distribution_dir>/plugins/BugTrackerPluginJira/com.fortify.BugTrackerPluginJira-<version>.jar`

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

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

Authoring bug tracker plugins

Assigning a Bug Tracking System to an Application Version

7.1.2. Removing bug tracker plugins

As an Administrator, you can remove third-party bug tracker plugins from the system.

To remove a bug tracker plugin from the system:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Plugins**, and then select **Bug Tracking Plugins**.
3. On the **Bug Tracking** page, expand the row for the plugin you want to remove.
4. Click **Disable**, and then, after the plugin is disabled, click **REMOVE**.

See also

About bug tracking system integration

Adding and managing parser plugins

Authoring bug tracker plugins

7.1.3. Securing logon credentials for bug tracking systems

When you file a bug from Application Security, 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 tracking system for each application.

Each bug tracking system 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. You can provide default values for some parameters.

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

Important

If Application Security is configured to communicate over SSL, you must also import the required bug tracking system certificates to the Java Virtual Machine (JVM) where Application Security is deployed.

7.1.4. Bug tracker parameters

A bug submitted with a bug tracking application requires entry of a standard summary and bug description in the **Submit Bug** dialog box. You can also add values for priority level, a due date for the fix, and the assignee. Application Security 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 or contact Customer Support.

7.1.4.1. ALM Quality Center parameters

In the **Submit Bug** dialog box for the ALM Quality Center bug tracking system, select the parameters that reflect your ALM Quality Center installation:

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

If your ALM Quality Center 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 Quality Center integration to remember. For changeset discovery to be functional, the following conditions must be met:

- Tag each OpenText Fortify SAST scan with a build-label, which Application Security 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 OpenText Fortify SAST to translate the source code.
- Enable the ALI extension for the individual project in ALM Quality Center 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 Quality Center.

- ALM Quality Center 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 Quality Center bug, you must have the ALM Quality Center browser plugin installed and use a browser compatible with ALM Quality Center,

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

7.2. Adding and managing parser plugins

As an Administrator, you can connect Application Security to third-party parser plugins.

Tip

You can write your own parser plugin. For instructions, see the Sample parser plugin page on GitHub.

To add a parser plugin to the system:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Plugins**, and then select **Parser Plugins**.
3. On the **Parsers** page, click **NEW**.
4. To acknowledge the warning about the risk of uploading third-party plugins and continue, click **OK**.
5. In the **Upload Plugin Bundle** dialog box, click **BROWSE**, and then locate and select the bundle file (JAR file) for your plugin.
6. Click **START UPLOAD**.
   The **Parsers** page lists the plugin you uploaded.
7. To expand the row that displayed the parser name, click it.
8. To enable the parser plugin, click **ENABLE**.
9. To acknowledge the warning about the risk of enabling untested plugins and continue, click **OK**.

See also

Managing Bug Tracker Plugins

7.2.1. Preparing to display OpenText Core SCA (Debricked) results

You can view open source security data from OpenText Fortify SCA on the **AUDIT** or **OPEN SOURCE** pages in Application Security. To do so, you must first download and install the required parser plugin. After you do, the uploaded open source analysis results are visible.

To prepare Application Security to display OpenText Fortify SCA data:

1. In a browser, go to https://github.com/fortify/fortify-ssc-parser-debricked-cyclonedx/releases.
2. Click **Assets**, and then select the latest version of the parser to download it.
   At the time of writing, the latest version is `fortify-ssc-23.2+-parser-debricked-cyclonedx-1.2.0.zip`.
3. Extract the contents of the downloaded ZIP file to a local directory.
4. Sign in to Application Security as an Administrator.
5. On the header, select **Administration**.
6. On the navigation pane, expand **Plugins**, and then select **Parser Plugins**.
7. On the **Parsers** page, click **NEW**.
8. To accept the risk of uploading the plugin, click **OK**.
9. In the **UPLOAD PLUGIN BUNDLE** dialog box, click **BROWSE**, and then select the extracted JAR file.
   <img data-zoom="true"
   src="file/images/general/fssc/SSC_Project/ssc_project_resources_imagesUpload_Debricked.PNG" style="width:

370px;height: 138px; border: none !important;"/>

10. In the **UPLOAD PLUGIN BUNDLE** dialog box, click **START UPLOAD**.
    The **Parsers** page now lists the OpenText Fortify SCA parser plugin.
11. After the upload is complete, expand the row for the OpenText Fortify SCA parser plugin, and then click **ENABLE**.
12. To accept the enable plugin warning message, click **OK**.

See also

Uploading scan artifacts

Viewing open source data

7.2.2. Preparing to display Sonatype results

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

To obtain Fortify SourceAndLibScanner, go to https://marketplace.microfocus.com/cyberres/content/fortify-sourceandlibscanner. For information about how to use SourceAndLibScanner to upload open Sonatype <meta class="data-nv" data-nv="AnalysisResults" data-nv-value="analysis results" data-productid="2405" data-replace-parent="false" data-version="25.2"/> to <meta class="data-nv" data-nv="SSC_Short" data-nv-value="Fortify Software Security Center" data-productid="2174" data-replace-parent="false" data-version="25.2"/>, see the OpenText™ Fortify SourceAndLibScanner User Guide, which is packaged with the Fortify SourceAndLibScanner utility.

To prepare Application Security to display uploaded Sonatype data:

1. In a web browser, go to https://marketplace.opentext.com/cybersecurity/content/sonatype-for-fortify-ssc.
2. On the **Sonatype for Fortify SSC** page, click **GET NEWEST**.
3. Unzip the `SonatypeFortifyBundle-<version>.zip` file contents to a local directory.
4. Sign in to Application Security as an Administrator.
5. On the header, select **Administration**.
6. On the navigation pane, expand the **Plugins** section, and select **Parser Plugins**.
7. On the **Parsers** page, click **NEW**.
8. To accept the risk of uploading the plugin, click **OK**.
9. In the **UPLOAD PLUGIN BUNDLE** dialog box, click **BROWSE**, and then select the `sonatype-plugin-<version>.jar` file.
10. Click **START UPLOAD**.
11. After the upload is complete, expand the row for the Sonatype Vulnerability Parser, and then click **ENABLE**.
12. To accept the risk of enabling the plugin, click **OK**.

See also

Uploading scan artifacts

7.3. About Application Security user administration

This section provides information about the different types of Application Security user accounts and how to create these accounts for your users.

Topics covered in this section:

- Administrator accounts
- User account types
- About creating user accounts
- Preventing destructive library and template uploads to Application Security
- Viewing permissions for Application Security roles
- About managing LDAP user roles

7.3.1. Administrator accounts

Users who have Administrator accounts have complete access to all Application Security user and application version data and can manage the entire Application Security 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.

OpenText recommends that you create only the administrator-level accounts necessary to create and edit local or LDAP Application Security user accounts. The Security Lead and lesser accounts can perform all other application-related activities.

Application Security permits the explicit addition of administrator-level accounts to application versions. This enables an Administrator to be assigned issues from the **AUDIT** page.

See also

Viewing permission information for Application Security roles

7.3.2. User account types

In addition to the administrator-level account used to administer user accounts, Application Security 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 they have 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 an OpenText™ Fortify WebInspect Enterprise instance from Application Security and can retrieve issue audit information. This role is intended for Fortify WebInspect Enterprise use only.
- **ScanCentral SAST Controller**—Users assigned the ScanCentral SAST Controller role can upload scans to Application Security using OpenText Fortify ScanCentral SAST on behalf of the users who have permission to run scans but do not have the "Upload analysis results" permission. This role is intended for use only when configuring a OpenText Fortify ScanCentral SAST Controller. For instructions on using this role in the OpenText Fortify ScanCentral SAST configuration, see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

See also

About Creating User Accounts

Unlocking local user accounts

7.3.3. About creating user accounts

As an Administrator, you can edit, delete, or suspend local user accounts. OpenText recommends that after you sign in to Application Security 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 an Administrator, you can delete or suspend all user accounts except for the last remaining administrator-level account. Application Security automatically disables the suspend and delete features for such an account.

For information about how to configure user account timeout and lockout settings, see Configuring core settings. For more information about user account permissions, see Account administration.

See also

Creating local user accounts

Viewing Permission Information for Application Security Roles

Unlocking local user accounts

7.3.4. Preventing destructive library and template uploads to Application Security

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 Application Security. To prevent templates that execute arbitrary and potentially destructive commands from being uploaded to Application Security, ensure that you:

- Assign access permissions to trusted users only.
- Check all custom templates for arbitrary SQL queries and commands before you upload them to Application Security.

7.3.5. Viewing permissions for Application Security roles

To view detailed information about the actions that users assigned the different Application Security roles can perform:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Users**, and then select **Roles**.
   The **Roles** page lists the names and descriptions of all the roles in the system.
3. Click the row for the role you are interested in to reveal the details for the role.
   The **Permissions** table lists all of the permissions granted to users assigned that role.

See also

Managing user accounts

About creating user accounts

Pre-configured roles

Unlocking local user accounts

7.3.6. About managing LDAP user roles

A relative distinguished name (RDN) further qualifies a base distinguished name (DN). For example, if the base DN for a given LDAP directory is `dc=domainName, dc=com,` and the full DN is `cn=group1,ou=users,dc=domainName,dc=com,` then the RDN is `cn=group1,ou=users.`

The topics in this section describe how to use LDAP RDNs to determine user roles.

7.3.6.1. Group membership in Application Security

For Application Security 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 signs in, Application Security looks up the user in the LDAP directory. Application Security 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, Application Security assigns the user all roles.

Application Security supports nested groups. For example, if a user is a member of group A and group A is a member of group B, Application Security recognizes that the user is a member of both groups.



Important

Use nested LDAP groups only if absolutely necessary. Enabling nested LDAP groups forces Application Security to perform extra tree traversals during authentication. OpenText strongly recommends that you clear this check box if you do not plan to use nested groups.

See also

Handling failed LDAP user logins

7.3.6.2. Handling failed LDAP user logins

If you configured nested LDAP groups for your Application Security server, and LDAP authentication fails during an attempted login because of incorrect credentials, then the sign in includes a message about bad credentials. However, if the log contains the text "user is not authorized," check the following:

- Is the user registered in Application Security and assigned a role? Check with the LDAP administrator to determine whether the user is actually a member of the group to which they are assumed to belong.
- If user does belong to the LDAP group, check to see whether the group is registered with Application Security and assigned a role.
- Special case: If the user belongs to the LDAP group that is registered to Application Security, but was added to the group only within the last few hours, refresh the LDAP cache manually or wait a few hours for it to automatically refresh.

To manually request an LDAP cache refresh:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Users**, and then select **LDAP Entities**.
3. Select the check box for the LDAP server.
4. On the **LDAP** page header, click **REFRESH**.
5. To determine whether the LDAP cache refresh has completed, from the Administration view, check either the **Event Logs** page or the **Jobs** page.



Note

An LDAP cache refresh can take a long time to complete.

See also

Group membership in Application Security

7.3.6.3. About mapping Application Security roles to LDAP groups

In most environments, the LDAP directory contains some users who do not need access to Application Security. Also, certain groups of users might require different access permissions.

Before you configure LDAP user authorization, you must decide which LDAP groups to associate with the Application Security roles (Administrator, Manager, Developer, and Auditor). OpenText recommends that you create new LDAP groups that map directly to the different Application Security roles. For example, you might create a FORTIFY_ADMINS group and a FORTIFY_DEVELOPERS group.

7.4. Global search functionality in Application Security

Application Security 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 automatically immediately indexed.

> **Note**
> Indexing uploaded FPR files is not immediate because it is performed as a separate Index New Issues job, which is scheduled to occur at the end of an artifact upload job.

The *index maintenance* job, which is performed once a day, keeps the index healthy. You can change its run time from the **Administration** view. OpenText recommends that you schedule this job to run once a day. For instructions on how to re-schedule executed jobs, see Configuring Job Scheduler Settings.

To enable global searching on your Application Security server, you must provide Tomcat server with read and write access to the search index directory. You can enable global searches during configuration at first sign in or after an upgrade.

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

Configuring Application Security for the first time

Configuring Application Security after an upgrade

Upgrade Lucene

Troubleshooting search index issues

7.4.1. Troubleshooting search index issues

As an indicator of search index health, the search index directory (specified in the Setup wizard or automatic configuration) includes the marker file `healthy.index`. If this file is not present in the search index directory, Application Security attempts to recreate the index on each startup.

If attempts to create the initial index repeatedly fail, remove the entire index directory, and then restart Application Security.

If you are working with a large database (hundreds of GB), the Full Reindex job might fail because of limited system memory. If this occurs, increase the Java heap size for Application Security and then restart Application Security. For minimum and recommended values for Java heap size, see the *Application Security Software System Requirements* document.

7.5. Placing Application Security in maintenance mode

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

To place Application Security in maintenance mode:

1. Sign in as an Administrator
2. On the header, select **Administration**.
3. On the navigation pane, expand **Configuration**, and then select **Maintenance**.
4. On the **Maintenance** page, select the **Set to maintenance mode** check box, and then click **SAVE**.
5. Restart the server.

> **Note**
> The `autoconfig` file is in Kubernetes secrets and cannot be deleted.

6. Open the *<fortify.home>/<app_context>/init.token* file in a text editor.
7. Copy the contents of the init.token file to the clipboard.
8. Open a web browser window and type the web address for your Application Security instance.
9. Click **ADMINISTRATORS**.
10. Paste the string you copied from the init.token file in the **Security Token** field, and then click **SIGN IN**.
    The Application Security Setup wizard displays all of the current configuration settings. For information about server configuration, see Configuring Application Security for the first time.
11. After you successfully complete the server configuration, restart Tomcat.

> **Note**
> Alternatively, you can set the following Java option to re-initialize the Setup wizard after you complete the setup: -Dcom.fortify.ssc.forceInit

> **Note**
> If your Application Security instance appears to be stuck in maintenance mode, try one of the possible solutions described in If Application Security is stuck in maintenance mode.

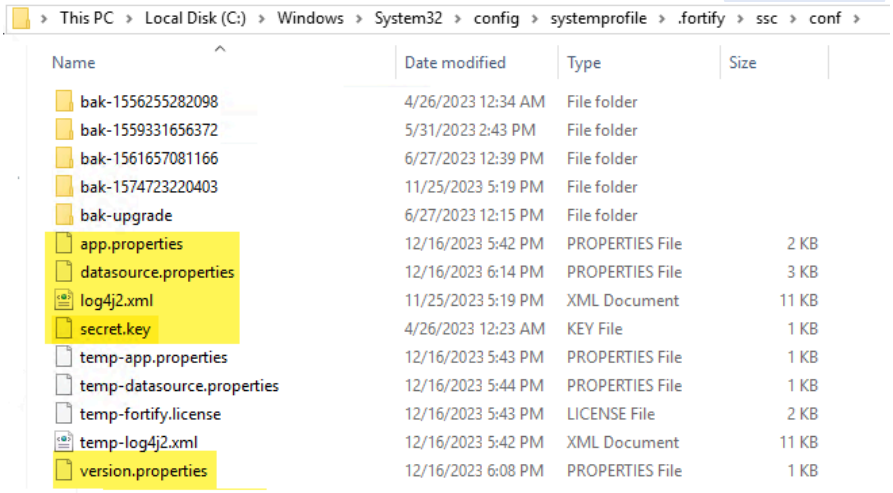
To facilitate server maintenance, you can pause job execution, which allows running jobs to finish but prevents new jobs from executing. For details, see Pausing and resuming job execution.

7.5.1. If Application Security is stuck in maintenance mode

Application Security goes into maintenance mode when it is placed there by an Administrator (see Placing Application Security in maintenance mode), or it cannot locate the version.properties in the *<fortify.home>/<app_context>*/conf/ directory.

If your Application Security instance is stuck in maintenance mode, try one of the following:

- Reconfigure Application Security. For instructions, see Configuring Application Security for the first time.
- Go to the *<fortify.home>/<app_context>*/conf/ directory and, in the version.properties file, set maintenance.mode to false.
- Restore the missing files from your original installation files from the <fortify.home> / <app_context>/conf/ directory.



> **Note**
> The datasource.properties file and some database fields contain encrypted entries that rely on the secret.key file. So, if you are moving your Application Security instance from one computer to another, you must also move the secret.key file (not just your database files).

7.6. Pausing and resuming job execution

If, for any reason, you need to shut down the server, you can temporarily pause user activity and stop the running of new jobs for all users in the system, while allowing Application Security to just finish jobs in progress. This helps to ensure that no data are corrupted or lost when the server is shut down.

To pause job execution on the server:

1. Sign in to Application Security as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Configuration**, and then select **Maintenance**.
4. On the **Maintenance** page, select the **Pause job execution** check box, and then click **SAVE**.
   Immediately after you save the setting:

   > **Important**
   > To prevent the queuing of many jobs, OpenText recommends that you avoid leaving this setting enabled for long periods of time. After you pause job execution, ensure that you allow time for queued jobs to process completely before you shut down the server.

   - All jobs in progress are allowed to complete.
   - All new jobs that users subsequently submit are queued for running later, after the **Pause jobs execution** check box is cleared.
   - Application Security displays a banner to notify users that job execution has been paused.
     <img data-zoom="true"
     src="file/images/general/fssc/SSC_Project/ssc_project_resources_imagesJobsPausedBanner.png"
     style="border: none !important;"/>
5. The next time you start the server, return to the **Maintenance** page, clear the **Pause job execution** check box, and then click **SAVE**.

See also

Placing Application Security in Maintenance Mode

7.7. About OpenText SAST Application Security Content

OpenText Application Security Software products use a knowledge base of rules to enforce secure coding standards applicable to the codebase for analysis. OpenText SAST Application Security Content consists of OpenText Secure Coding 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 OpenText Fortify SAST and the OpenText Secure Coding 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 OpenText Secure Coding Rulepacks. For instructions on how to write custom rules, see the *OpenText™ Static Application Security Testing Custom Rules Guide*.
  For information on how to manage OpenText Secure Coding Rulepacks, see:
  - Updating Rulepacks from the Rulepack update server
  - Importing OpenText SAST Application Security Content
  - Deleting Rulepacks
  - Exporting Rulepacks
  - Seeding the database with report seed bundles delivered with quarterly OpenText SAST Application Security Content releases
- External metadata provides mappings from the OpenText Application Security Software vulnerability categories to alternative categories (such as CWE, OWASP Top 10, and PCI).
  OpenText recommends that you *not* modify the external metadata file. If you do, your changes are overwritten whenever you update your Rulepacks with quarterly releases. You can, however, create a custom external metadata 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 OpenText SAST Application Security Content. For instructions on how to create your own custom rules or custom external metadata, see the *OpenText™ Static Application Security Testing Custom Rules Guide*.
The provided external metadata mappings file is located in the `<ssc_deploy_dir>/WEB-INF/Core/config/ExternalMetadata/` directory.
For information on how to manage your external metadata, see:

- Extending a current mapping
- Creating a new mapping

It is important that you work with the newest OpenText Secure Coding Rulepacks available. OpenText recommends that you periodically update your OpenText SAST Application Security Content.

7.7.1. Updating Rulepacks from the Rulepack update server

It is important to work with the latest Rulepacks available. To ensure that you have the latest Rulepack, you can import it from the Rulepack update server.

> **Note**
>
> You can use the Application Security proxy to update Rulepacks, if the Rulepack update server is behind it. For information about how to set up a consolidated proxy for Application Security, see Configuring a proxy for Application Security integrations.

To import the latest Rulepacks:

1. Sign in to Application Security as an Administrator or Security Lead
2. On the header, select **Administration**.
3. On the navigation pane, under **Metrics & Tracking**, select **Rulepacks**.
4. On the **Rulepacks** page, click **UPDATE FROM SERVER**.
   Application Security displays information about what the Rulepacks update involves.
5. To continue with the update, click **OK**.
   After the update is complete, Application Security displays a list of imported rules.
6. Click **CLOSE**.

See also

Deleting Rulepacks

Seeding the database with report seed bundles delivered with quarterly OpenText SAST Application Security Content releases

Exporting Rulepacks

Importing OpenText SAST Application Security Content

7.7.2. Exporting Rulepacks

You can, if necessary, move Rulepacks from one Application Security instance to another, or between Application Security 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. Sign in as an Administrator or Security Lead.
2. On the header, select **Administration**.
3. On the navigation pane, under **Metrics & Tracking**, select **Rulepacks**.
4. On the **Rulepacks** page, select the check boxes for the Rulepacks you want to export, and then click **EXPORT**.

Note
If a Rulepack that you select has multiple versions, only the latest version is exported.

See also

Importing OpenText SAST Application Security Content

Deleting Rulepacks

7.7.3. Importing OpenText SAST Application Security Content

You can import security content, including custom Rulepacks created using the OpenText™ Fortify Custom Rules Editor, extended mapping files, and custom mapping files so that they are available to OpenText Fortify SAST and Fortify Audit Workbench.

To import security content:

1. Sign in as an Administrator or Security Lead.
2. On the header, select **Administration**.
3. On the navigation pane, under **Metrics & Tracking**, select **Rulepacks**.
4. On the **Rulepacks** page, select **IMPORT**.
5. In the **IMPORT RULEPACK** dialog box, click **+ ADD FILES**.
6. Find and select the files to upload.
7. Click **START UPLOAD**.
8. Click **CLOSE**.

Note
If you upload an FPR file that contains an extended mapping, and that mapping is not present on the server, Application Security displays a processing warning.

See also

Exporting Rulepacks

Deleting Rulepacks

7.7.4. Deleting Rulepacks

You can remove old Rulepacks from Application Security.

To delete Rulepacks:

1. Sign as an Administrator or Security Lead.
2. On the header, select **Administration**.
3. On the navigation pane, under **Metrics & Tracking**, select **Rulepacks**.
4. On the **Rulepacks** page, select the check boxes for the Rulepacks to delete, and then click **DELETE**.
5. To confirm deletion of the selected Rulepacks, click **OK**.
6. If the deletion fails, click **more** to open the **DETAILS** window to find out what caused the failure.

See also

Exporting Rulepacks

Importing OpenText SAST Application Security Content

Updating Rulepacks from the Rulepack update server

7.7.5. Extending an existing mapping

You can extend existing mappings with the `<ExternalListExtension>` element. 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>EEE3F9E7-28D6-4456-8761-3DB99436F4EE</ExternalListID>
<ExternalCategoryDefinition>
        <Name>APP100 CAT 1</Name>
        <Description>
        Description for App100 CAT 1.
        </Description>
        OrderingInfo>1</OrderingInfo>
</ExternalCategoryDefinition>
<Mapping>
        <InternalCategory>
        Poor Style: Indentifier Contains Dollar Symbol ($)
        </InternalCategory>
        <ExternalCategory>App100 CAT 1</ExternalCategory>
</Mapping>
</ExternalListExtension>
```


Important

After you extend your mapping file, you must upload it to Application Security. For instructions, see Importing OpenText SAST Application Security Content.

If you upload an FPR file that contains an extended mapping, and that mapping is not present on the server, Application Security displays a processing warning.

See also

Creating a new mapping

About OpenText SAST Application Security Content

7.7.6. Creating a new mapping

You can use the `<ExternalList>` element to create a custom external metadata file in the following format:

```
<ExternalList>
<ExternalListID>3C6ECB67-BBD9-4259-A8DB-B49328927248</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>
<OrderingInfo>1</OrderingInfo>
</ExternalList>
```


Important

After you create your custom mapping file, you must upload it to Application Security. For instructions, see Importing security content.

If you upload an FPR file that contains a custom mapping, and that mapping is not present on the server, Application Security displays a processing warning.

See also

Extending a current mapping

About OpenText Application Security Software security content

7.8. Enabling OpenText SAST and OpenText Application Security Tools upgrades from Fortify Audit Workbench

Anyone using Fortify Audit Workbench can check on the availability of new OpenText Fortify SAST and OpenText Application Security Tools version from Fortify Audit Workbench. 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, an Administrator must first set up the auto upgrade capability on the Application Security host machine.

To make new OpenText Fortify SAST and OpenText Application Security Tools installers available to Fortify Audit Workbench users for upgrades:

1. On the Application Security host, open the *<ssc_deploy_dir>* / WEB-INF/internal/securityContext.xml file in a text editor.

2. Locate and uncomment the following line:

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

3. Save and close the `securityContext.xml` file.
4. Copy the OpenText_SAST_<*version*> or OpenText_Application_Security_Tools_<*version*> installer files to the `<ssc_deploy_dir>/update-site/installers/` directory.
5. In the `<ssc_deploy_dir>/update-site/installers/` directory, create an update XML file for each product you want to update:
    1. To enable OpenText Fortify SAST updates, create an update XML file (such as `update-sast.xml`) using the following example:

```
<installerInformation> <versionId>2640</versionId> <!--The version of the installer file
with periods removed--> <version>26.4.0</version> <!--The version of the installer file-->
<platformFileList> <platformFile> <filename>OpenText_SAST_windows-x64_26.4.0.exe</filename>
<platform>windows-x64</platform> </platformFile> <platformFile>
<filename>OpenText_SAST_linux-x64_26.4.0.run</filename> <platform>linux-x64</platform>
</platformFile> <platformFile> <filename>OpenText_SAST_osx-x64_26.4.0.app.zip</filename>
<platform>osx</platform> </platformFile> </platformFileList> <downloadLocationList>
<downloadLocation> <url>http://localhost:8080/update-site/installers/</url>
</downloadLocation> </downloadLocationList>
</installerInformation>
```

    2. To enable OpenText Application Security Tools updates, create an update XML file (such as `update-tools.xml`) using the following example:

```
<installerInformation> <versionId>2640</versionId> <!--The version of the installer file
with periods removed--> <version>26.4.0</version> <!--The version of the installer file-->
<platformFileList> <platformFile> <filename>OpenText_Application_Security_Tools_windows-
x64_26.4.0.exe</filename> <platform>windows-x64</platform> </platformFile> <platformFile>
<filename>OpenText_Application_Security_Tools_linux-x64_26.4.0.run</filename>
<platform>linux-x64</platform> </platformFile> <platformFile>
<filename>OpenText_Application_Security_Tools_osx-x64_26.4.0.app.zip</filename>
<platform>osx</platform> </platformFile> </platformFileList> <downloadLocationList>
<downloadLocation> <url>http://localhost:8080/update-site/installers/</url>
</downloadLocation> </downloadLocationList>
</installerInformation>
```

6. Restart Tomcat server.



Note

For more information about the AutoUpdate tool used for the upgrade functionality, see the Install Builder User Guide.

Fortify Audit Workbench users can now check for and install new OpenText Fortify SAST or OpenText Application Security Tools versions. For information about how to perform the upgrades from Fortify Audit Workbench, see the *OpenText™ Fortify Audit Workbench User Guide*.

8. Upgrading Application Security

To perform a direct upgrade to the latest Application Security version, you must have one of the last three versions already installed. If you have an older version, you must first upgrade to one of the following versions. The following versions are supported for a direct upgrade:

- 26.2.x
- 25.4.x
- 25.2.x
- 24.4.x

This section contains the following topics:

- Upgrade prerequisites
- Preparing to upgrade the database
- Upgrade tasks
- Upgrade Lucene
- Updating and deploying the WAR file
- Configuring Application Security after an upgrade
- Updating expired licenses
- Seeding the database with report seed bundles in quarterly OpenText SAST Application Security Content releases

8.1. Upgrade prerequisites

Perform the following prerequisites as needed for your upgrade:

- If you are upgrading from a version earlier than 24.2.x, ensure that you have Java version 17 installed *before* you upgrade.
- Full OpenText Fortify ScanCentral SAST-related functionality in Application Security requires updated Controller and sensors. If you do not need sensor metrics, you can use existing sensors. You can use existing OpenText Fortify ScanCentral SAST clients without limiting functionality.

  Important
  You must upgrade the Controller before you upgrade the sensors and clients, *and* before you upgrade the Application Security server. For information about how to upgrade, see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

See also
Preparing to upgrade the database

8.2. Preparing to upgrade the database

The Application Security database migration process creates larger transactions than those created during regular use. For 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, OpenText recommends that you review and, if necessary, increase the database resources and settings required to accommodate the migration process.

If you are upgrading from version 23.1.0 or earlier to version 23.2.0 or later, you need to be aware that during migration the ID column type in the `scan_issue` table is changed from INT to BIGINT for MySQL and SQL Server databases to avoid reaching the maximum 32b integer limit.

If you have already applied the recommended workaround for SQL Server to reset the identity value on the `scan_issue` table to a negative number with `DBCC CHECKIDENT (scan_issue, reseed, -2147483648)`, then you must perform an additional manual migration step. Reset the identity value back to a positive number after the migration. To perform the reset, run the query: `DBCC CHECKIDENT (scan_issue, RESEED)`. The user running the query must be either an owner of the schema that contains the table or must have the sysadmin, db_owner, or db_ddladmin fixed database role.

If you are upgrading a MySQL database, see Setting the Innodb Buffer Pool Size when upgrading a MySQL database.

8.2.1. Setting the Innodb buffer pool size when upgrading a MySQL database

If you are upgrading a MySQL database, OpenText recommends that you set the `innodb_buffer_pool_size` variable to at least 2.5 GB. After the upgrade, revert to your previous setting.

See also

Using a MySQL database

8.2.2. Preparing to run the database upgrade script

The Application Security database upgrade scripts require the same database permissions that the database creation scripts require.

Before you run the database upgrade script, perform the following tasks:

- Back up your existing Application Security database using your database client tool.
- Acquire the database account information that was used to create the existing Application Security database. See Database user account permissions.



Note

Databases that contain over 1 TB of data might take five or more hours to migrate.

8.3. Upgrade tasks

Upgrade to a new version of Application Security by performing the tasks described in the following table in the order listed.

Task	Description
1	Stop Tomcat server.
2	Delete the WAR file from the `<tomcat>/webapps/` directory, and then copy the new WAR file to the `<tomcat>/webapps/` directory (see Updating and deploying the WAR file). **Note** *<tomcat>* represents the root directory of the Tomcat instance.
3	Start Tomcat server.
4	Open a browser and enter your Application Security web address to start the Setup wizard.
5	Use the Setup wizard to generate the migration SQL script (see Configuring Application Security after an upgrade).
6	Run the migration script on your database (see Preparing to run the database upgrade script). Databases that contain over 1 TB of data might take five or more hours to migrate. **Important** (SQL Server databases only) After you migrate Application Security to a new SQL Server database version and back up and restore the database, you must change the compatibility level (from SQL Server Management Studio) to reflect the SQL engine version that currently hosts the Application Security database.
7	Use the Setup wizard to reseed the database.
8	Restart Tomcat server.
9	Bug tracker plugins are not included in the `ssc.war` file. After you upgrade and start Application Security, remove old bug tracker plugins, and then install new plugins from the current installation package. For more information, see About Bug Tracker integration.

8.4. Upgrade Lucene

Application Security 26.2 version includes an updated Lucene version. Because Lucene index formats can change across major or minor upgrades, full-text (global search) indexes created by an earlier Application Security version do not work

after migrating to 26.2 Application Security . The supported approach is to delete the existing full-text index contents and allow Application Security 26.2 to recreate/reindex them.

- Fresh installation of Application Security 26.2: After enabling full text search, indexes are created and functional.
- Migration to Application Security 26.2: Previous full text search indexes are dysfunctional. After you delete the content of the full text index folder and restart Application Security , new indexes are created.

Migration from 25.2 to 26.2

1. In the previous Application Security version, disable full text search by editing the property file `<fortify.home>/<app_context>/conf/app.properties`.
2. Delete the content of the full text search index folder.
3. Restart Application Security (previous version).
4. Verify that the index folder is not created.
5. Upgrade to Application Security 26.2 and enable full text search again (in the property file).
6. Restart Application Security 26.2.
7. Verify that new indexes are created and full text search is functional.



Note

Re-indexing of huge data can take a long time. During testing on big data, record:

- Database size used for testing.
- Time required for indexes to be created and become functional after restart.

Verification (post-upgrade)

In the Application Security UI and using the REST API, run the same full text searches you used previously and confirm results match the previous behavior and range.

8.5. Updating and deploying the WAR file

To update the Application Security WAR file:

1. Undeploy the currently deployed Application Security WAR file.
   For instructions, see the documentation for Tomcat server.
2. Deploy the new Application Security WAR file.

After you deploy the new WAR file, complete the configuration tasks on the Setup wizard steps and in the **Administration** view. For information and instructions, see Configuring Application Security after an upgrade and Additional Application Security configuration.

8.6. Configuring Application Security after an upgrade

After you upgrade Application Security and enter your Application Security web address in a browser window, the Setup wizard opens. Use the Setup wizard to perform the database data migration and reseed the database.



Note

The Setup wizard is available to Administrators only, and only after the first deployment of Application Security, after an upgrade, or after the server is placed in maintenance mode (see Placing Application Security in maintenance mode).

1. Open the `<fortify.home>/<app_context>/init.token` file in a text editor.
2. Copy the contents of the `init.token` file to the clipboard.
3. Open a web browser and type your Application Security server URL.
4. Click **ADMINISTRATORS**.
5. In the Setup wizard sign in, paste the string you copied from the `init.token` file into the **Security Token** field, and then click **SIGN IN**.

6. If you need to change any configuration settings on the **CONFIGURATION** or **CORE CONFIGURATION SETTINGS** pages, you can do so using the instructions provided in Configuring Application Security for the first time.
7. Click **NEXT** until you reach the **DATABASE SETUP** page.
8. On the **DATABASE SETUP** page, do the following:
    1. In the **DATABASE TYPE** box, select the type that matches the Application Security database type.
    2. In the **DATABASE USERNAME** box, type the username for your Application Security database.
    For more information, see Database user account permissions.
    3. In the **DATABASE PASSWORD** box, type the password for your Application Security database.
    4. In the **JDBC URL** box, type the URL for the Application Security database.

        Caution

        The database name (including letter case) in the JDBC URL must exactly match your Application Security database name.

        The MariaDB JDBC driver connects to the MySQL database server. Any JDBC URL parameters *must* use MariaDB driver syntax. Example of the correct collation parameter syntax:

        ```
        jdbc:mysql://<host>:3306/<database_name>?sessionVariables=collation_connection=
        <collation_name>
        ```

        Replace the parameter `connectionCollation=<collation_name>` with `sessionVariables=collation_connection=<collation_name>`.
    5. To test the connection to your database, click **TEST CONNECTION**.
    If the connection test fails, check the `<fortify.home>/<app_context>/logs/ssc.log` file to troubleshoot the cause.
    6. After the Setup wizard indicates that the connection was successful, read the warning and instructions, and then click **DOWNLOAD SCRIPT**.
    7. Save and run the `ssc-migration.sql` script.
    For instructions, see About the Application Security database tables and schema.

        Note

        Depending on the size of the source database, data migration might take several hours to complete.
9. After you run the `ssc-migration.sql` script, click **NEXT**.
10. On the **DATABASE SEEDING** page, do the following:
    1. Click **BROWSE** to locate and select your process seed bundle ZIP file, and then click **SEED DATABASE**.
    2. Click **BROWSE** to locate and select your report seed bundle ZIP file, and then click **SEED DATABASE**.
    3. (Optional) Click **BROWSE** to locate and select your PCI SSF seed bundle ZIP file, and then click **SEED DATABASE**.
    4. (Optional) Click **BROWSE** to locate and select your PCI basic seed bundle ZIP file, and then click **SEED DATABASE**.
11. Click **NEXT**.
12. Click **FINISH**.
13. Restart Tomcat server.



Tip

If you later find that you need to change any of the configuration settings, you can place Application Security in maintenance mode, and then make any necessary changes. For instructions on how to place Application Security in maintenance mode, see Placing Application Security in maintenance mode.

8.7. Updating expired licenses

For information about how to obtain a Fortify license file, see Downloading and unpacking Application Security files.

To update an annual license that has expired:

1. Stop Tomcat server.
2. Place your downloaded `fortify.license` file in the *<fortify.home>* directory.
3. Restart Tomcat server.

8.8. Seeding the database with report seed bundles in quarterly OpenText SAST Application Security Content releases

OpenText 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 **OpenText™ Security Fortify Premium Content** in your notification document. That section has 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 Application Security Database.



Important

Updated external metadata files can include changes to mappings that reporting depends on. If updated security content includes a new report seed bundle, ensure that you update your rules and mappings *before you run reports*.



Note

Seeding the database blocks the creation of new application versions and the execution of report and analysis results 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:
    1. Log in to the Application Security Customer Portal.
    2. In the navigation pane, select **PREMIUM CONTENT**.
    3. Click the **FORTIFY EXCHANGE** link.
    4. Select and download the latest report seed bundle.
2. Extract the contents of the seed bundle ZIP file.
3. Sign in to Application Security as an Administrator.
4. On the header, select **Administration**.
5. On the navigation pane, expand **Configuration**, and then select **Seed Bundles**.
6. On the **Seed Bundles** page, click **BROWSE**, and then find and select the `ReportBundle.zip` file.
7. Click **SEED BUNDLES**.

See also

About seeding the Application Security database

About OpenText Application Security Software security content

Updating Rulepacks from the Rulepack update server

9. Using Application Security

As development teams perform scans, they submit periodic analysis results into Application Security. Security teams submit periodic results of a dynamic assessment into Application Security.

Application Security correlates and tracks the analysis results and assessment results over time, and makes the information available to developers through Fortify Audit Workbench, or through Secure Code Plugins such as the Fortify Plugin for

Eclipse, the Fortify Extension for Visual Studio, and others.

Users can also submit issues into bug tracking systems and generate analysis reports.

This section contains the following topics:

- Signing in to Application Security
- Requesting access to Application Security
- Changing your password
- Setting preferences system-wide and across application versions
- Viewing keyboard hotkeys
- Accessing the API documentation
- About the Application Security Dashboard

9.1. Signing in to Application Security

To sign in to Application Security, your Administrator must provide you with the web address for your instance, a username, and a password.

To sign in to Application Security for the first time:

1. In a web browser, type the web address for your Application Security instance, as follows:
   `<protocol>://<hostname>:<port>/<app_context>`
   where `<port>` represents the port number that Tomcat server uses.
2. Type your user name and password.
3. Click **SIGN IN**.
4. If Application Security prompts you to change your password, do so.

9.1.1. About session logout

If you signed in to Application Security using local login (through the sign in dialog box with username and password to LDAP or local account), and you then log out, Application Security takes you to the logout screen.

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

> **Note**
>
> Application Security supports single logout for SAML. For more information about single-on and single logout, see Configuring single sign-on and single logout solutions that use HTTP headers.

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

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

> **Note**
>
> To log out of Application Security completely, close all your browser windows.

Inactive session timeout

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

- If you logged in using a local login (through the login dialog box with username and password to LDAP or local account), and your session is about to time out, you see a dialog box that lets you either log out or stay logged in. If you click **LOG OUT** or your session times out due to further inactivity, Application Security logs you out of the session and takes you to the logout screen.
- If you are logged on to Application Security through an SSO provider for which single logout is supported, you see a dialog box that lets you log out of your local user account, perform an SSO logout, or stay logged in.

If you click **LOCAL ACCOUNT LOGOUT** or your session times out due to further inactivity, Application Security logs you out of the session only and then takes you to the logout screen.
If you click **SSO LOGOUT**, Application Security logs you out of the session, and then logs you out of your SSO provider.
For information about how to configure session timeout, see Configuring core settings.

Note

To log out completely from Application Security, close your browser (all tabs).

9.2. Requesting access to Application Security

If you do not yet have a user account, or if you have forgotten your user name or password, you can request assistance from the sign in page.

To request access to Application Security:

1. In a web browser, type the web address for your Application Security instance.
2. Click **Can't access or need an account?**
   This button is available only if your Application Security Administrator has enabled email notification (see Configuring email alert notification settings).
   In addition to Configuring email alert notification settings, you must set **User administrator's email address (for user account requests)** (see Configuring Core settings).
3. Provide the required information and click **SEND**.

9.3. Changing your password

The following procedure describes how to change your password. Note that you can only change your password if you are logged on using a local account.

To change your password:

1. Sign in to Application Security.
2. From the **Profile menu** in the header, select **Change Password**.
   The **SAVE** button in the **Change Password** dialog box is enabled only after you type a strong new password that does not include your username or common phrases (names, movie or song titles, dates, 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 sign in.
3. Provide your old password, type a new one, and then confirm the new one.
4. When the password strength is accepted, click **SAVE**.

9.4. Setting preferences system-wide and across application versions

You can configure preferences for behavior system-wide, and across application versions.

To set system-wide preferences:

1. From the **Profile menu** on the header , select **Preferences**.
2. To set preferences to apply to the entire system, in the **PREFERENCES** dialog box, under **System-wide Preferences**, do the following:
   1. Select the check boxes for the features you want to enable and clear the check boxes for the features you want to turn off.
   2. To apply the YYYY/MMDD date format instead of the default MM/DD/YYYY format, select it from the **Date format** list.
   3. To apply the 24 Hour time format instead of the default 12 hour AM/PM format, select it from the **Time format** list.
   4. To change the theme, select Light, Dark, or Automatic from the **UI Theme** list.

> **Note**
> If you apply the Automatic theme, the theme is based on the operating system or your browser theme.

3. To set preferences for all application versions, do the following:

   > **Note**
   > You can override these settings for a specific application version by making changes to the **Advanced Options** in the **Application Profile**.

   1. To include suppressed issues in the issues list on the **AUDIT** page, select the **Show suppressed issues** check box.
   2. To include removed issues on the **AUDIT** page, select the **Show removed issues** check box.
   3. To include hidden issues on the **AUDIT** page, select the **Show hidden issues** check box.
   4. To display short file names in the issues list on the **AUDIT** page, select the **Use short filenames** check box.
4. Click **SAVE**.

9.5. Viewing keyboard hotkeys

To view the keyboard hotkeys used to navigate the Application Security user interface:

1. Sign in to Application Security.
2. Do one of the following:
   - From the **Profile menu** on the header, select **Hotkeys**.

   - Press **?** on your keyboard.

See also

Setting preferences system-wide and across application versions

9.6. Accessing the API documentation

> **Important**
> Usage of Application Security API calls from external applications can have a negative impact on your Application Security instance and OpenText does not provide support for external applications. If the external calls degrade your instance, OpenText recommends that you discontinue the direct external calls and implement an alternate way of indirectly integrating with Application Security. Professional Services can assist you with this.

To access the Application Security API documentation:

1. On the header, click the **Help** button .



2. Click the **API Documentation** link.

The Application Security API documentation webpage opens in the browser.

Tip

It is useful to leverage a proxy such as the Chrome DevTools to intercept Application Security traffic and determine the appropriate endpoint calls to make to perform user interface actions.

9.7. About the Application Security Dashboard

After you sign in to Application Security, the **Dashboard** view displays data for the application versions to which you have access and that pose the highest potential business risk to your organization.

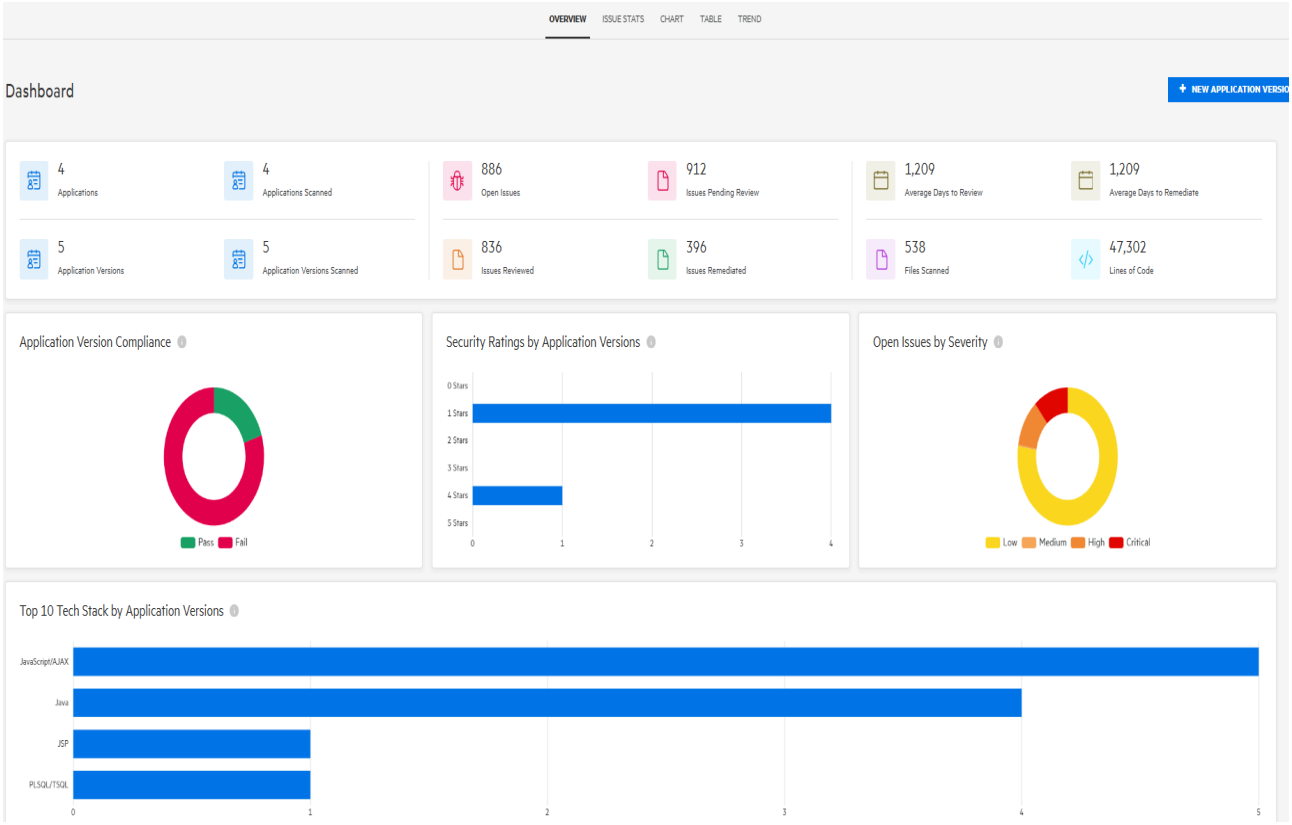
Topics covered in this section:

- Overview
- Issue Stats
- Viewing high-level summary metrics for your application versions
- Viewing high-level summary metrics (graphical representation) for an application version
- Exporting the Dashboard summary table

9.7.1. Overview

When you first sign in to OpenText™ Application Security, the **OVERVIEW** page appears in the **Dashboard** view. This page provides a comprehensive overview of your application security program, with visualizations of the key metrics.

The **OVERVIEW** page displays a summary of application versions, code analysis, and issue management for all the application versions you can access. For standard datasets with up to 500 application versions, all metrics and charts render within a few seconds of navigation. You can manually refresh your browser to ensure the latest data is displayed without duplication or rendering issues.



The **OVERVIEW** page displays the following metrics for all application versions you can access:

Metric	Description
Applications	Total number of applications with versions
Application Versions	Total number of application versions
Applications Scanned	Total number of applications with scanned versions
Application Versions Scanned	Total number of scanned application versions
Open Issues*	Total number of unresolved issues for all application versions
Issues Pending Review*	Total number of issues awaiting review
Issues Reviewed*	Total number of issues that have been reviewed
Issues Remediated*	Total number of issues that have been remediated
Average Days to Review	Average number of days it takes to review issues. This value may include decimal precision to one place.
Files Scanned	Total number of files scanned for all application versions
Average Time to Remediate	Average number of days it takes to remediate issues. This value may include decimal precision to one place.
Lines of Code	Total number of lines of code analyzed

* Issue counts are based on unique instance IDs to avoid multiple counting of the same issue in the aggregates.

Graphical representation

The **OVERVIEW** page includes the following graphical representation:

Application version compliance

The **Application Version Compliance** donut chart displays the compliance status for all application versions based on security ratings.

- Pass: Application versions with security ratings of 3, 4, or 5 stars
- Fail: Application versions with security ratings of 0, 1, or 2 stars

Hover over each segment to view the segment label (Pass or Fail) and the count of application versions.

Security ratings by application versions

The **Security Ratings by Application Versions** horizontal bar chart displays the count of application versions grouped by their security rating (0 to 5 stars). Hover over each bar to view the security rating and the count of application versions.

Open issues by severity

The **Open Issues by Severity** donut chart displays the open issues by severity level:

- Critical
- High
- Medium
- Low

Hover over each segment to view the severity level and the count of issues.

Top 10 tech stacks by application versions

The **Top 10 Tech Stacks by Application Versions** horizontal bar chart displays the top 10 technology stacks (primary programming languages or frameworks) with the highest number of application versions. If fewer than 10 technology stacks exist, the chart displays only the available stacks without empty filler bars. The bars are ordered in descending order by the count of application versions. Hover over each bar to view the technology stack name and the count of application versions.

See also

Creating the first version of a new application

Viewing and marking alerts

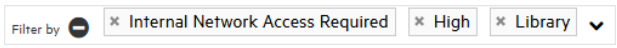
9.7.2. Issue Stats

The **ISSUE STATS** page in the **Dashboard** view shows summary information about issues for the application versions that you can access, including the average 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**. The color bars indicate the duration of issue management.

> **Note**
>
> As 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.

If you click an application version listed in the table, Application Security takes you directly to the **AUDIT** page for that application version. No filters are applied to the data.

The **Dashboard** view provides three settings that you can use alone or in combination to refine the summary data displayed.

Display setting	Description
Group by an application attribute	Select an attribute from the **Group by** list. The default grouping attribute is the application version. In addition to the grouping attribute you selected, the **Dashboard** view displays data that 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.
Aggregate by an application attribute	Select an attribute from the **Aggregate by** list. The **Dashboard** view 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.
Filter by one or more application attributes	Select an attribute from the **Filter by** list. You can filter by multiple attributes, but you must select them one at a time.  The **Dashboard** view displays your data based on the selected filter attributes, and any other attributes you have selected from the **Group by** and **Aggregate by** lists.

To clear your attribute selection from a list, click the **Clear all** button .

You can export Application Security 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.

9.7.3. Viewing high-level summary metrics for your application versions

To view summary metrics for application versions (individually and collectively):

- On the header, select **Dashboard**.

The following three tiles on the **Issue Stats** page (the default Dashboard view in <meta class="data-nv" data-nv="SSC_Short" data-nv-value="Fortify Software Security Center" data-productid="2174" data-replace-parent="false" data-version="25.2"/>) displays consolidated metrics for all of the applications to which you have access:

- The **Issues Remediated** tile 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** tile shows the total number of open issues, and the number of these that have been reviewed.
- The **Application versions** tile 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 application version to which you have access. Clicking an application version listed in the table takes you directly to the **AUDIT** page for that application version.

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

See also

Viewing summary metrics (graphical representation) for an application version

Auditing scan results

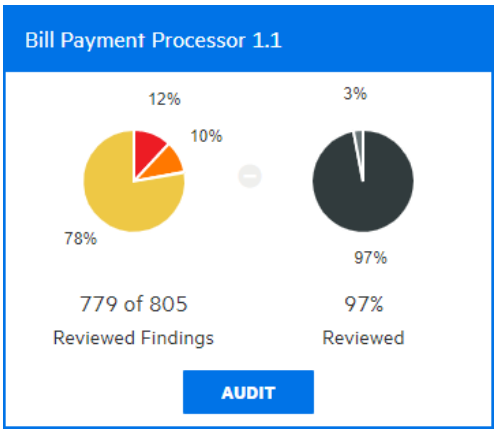
Viewing high-level summary metrics for an application version

9.7.4. Viewing high-level summary metrics (graphical representation) for an application version

You can view a graphical representation of high-level 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** view, click **CHART**.
   Application Security opens to the **REVIEWED** tab.
2. In the list of application versions, point to a colored bar for an application version to see the summary findings for the version.



   In the example shown here, the pie chart on the left shows the security ratings for the 97% of findings (779 of 805) that have been audited to date for this application version. The chart on the right shows the percentage of findings audited (97) and the percentage of the total that has yet to be audited (3).
3. To go to the **AUDIT** page for the application version, click **AUDIT**.

See also

Viewing summary metrics for application versions

Auditing scan results

Viewing summary metrics for an application version

9.7.5. Exporting the Dashboard summary table

You can export data for all application versions to a comma-separated values (CSV) file. To determine how long the system retains your CSV files, see Configuring job scheduler settings.

To export the summary table displayed in the **Dashboard** view:

1. On the header, select **Dashboard**, and then click **ISSUE STATS**.
2. On the **Dashboard** toolbar, click **EXPORT**.

> **Note**
> If the **EXPORT** button is unavailable, then your Administrator has disabled this functionality.

3. In the **File Name** box, type a 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:
    1. On the header, select **Reports**.
    2. Click **DATA EXPORTS**.
    3. In the **Issue Stats** table, point to the row for the exported file, and then click the **Download** button .

See also

Exporting selected data for an application version

10. Managing user accounts

As described in the secure deployment guidelines (see Providing for secure deployment), the primary system Administrator of a new Application Security installation creates a non-default administrator-level account, and then deletes the default Administrator account. Use the non-default Application Security administrator account to create additional Application Security user accounts.

This section contains information about Application Security roles, user account administration, how to register LDAP entities with Application Security, and how to configure an integration with Microsoft Entra ID.

This section contains the following topics:

- About tracking teams
- About roles
- Account administration

10.1. 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. Application Security 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.

10.2. About roles

Roles determine the actions a user can perform in Application Security.

For more fine-grained control over user access to Application Security functionality, you can create custom roles and assign them permissions from the Application Security interface. For instructions on how to create a role, see Creating custom roles.

10.2.1. Preconfigured roles

The following table lists the preconfigured roles you can assign to users in Application Security. The roles are listed in descending order of level of authority. For information about how to view the permissions associated with each

preconfigured role, see Viewing permission information for Application Security roles.

Role	Description
Administrator	Has full access to the system and all results
Security Lead	Security team member who can create application versions and users
Manager	Responsible for guiding developers to work on results Managers cannot create applications but can grant or revoke access to their team members
Developer	Developer responsible for producing security results and taking action to triage or remediate security issues
View Only	Can view results, but cannot interfere with the issue triage or the remediation process. Example users: system automation account or temporary auditor
Application Security Tester	Can perform tasks required to execute dynamic scan requests, including: • View application versions • View and generate reports • Process dynamic scans • Upload analysis results • Audit issues
WebInspect Enterprise System	Can connect a Fortify WebInspect Enterprise instance to Application Security and retrieve issue audit information. This role is intended for use only by a WebInspect Enterprise instance.
ScanCentral SAST Controller	Can upload scans from OpenText Fortify ScanCentral SAST to Application Security on behalf of users who have permission to run scans but do not have the "Upload analysis results" permission. This role is intended for use only when configuring a ScanCentral SAST Controller. For more information, see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.
ScanCentral DAST Controller	This role is intended for use only when configuring a ScanCentral DAST Controller. For more information, see the *OpenText™ Fortify ScanCentral DAST Configuration and Usage Guide*.

See also

About roles

Creating custom roles

10.2.2. Creating custom roles

You can define roles of your own and assign them permissions.

To define and configure permissions for a new role:

1. Sign in as an Administrator
2. On the header, select **Administration**.
3. On the navigation pane, expand **Users**, and then select **Roles**.
4. On the **Roles** page, click **NEW**.
5. In the **CREATE NEW ROLE** dialog box, provide the information described in the following table.

> **Important**
> Except for a new line in the **Name** and **Description** fields, values must not start with the characters `=`, `-`, `+`, or `@`, and must not include control characters. For a complete list of Unicode characters included in the restricted ranges, see Control characters in ASCII and Unicode.

Field	Description
Name	Role name
Description	(Optional, but recommended) Role description
Universal access	To assign the new role access to all application versions, select this check box. **Note** OpenText strongly recommends that you select universal access only for administrator-level users.

6. To add permissions, click **+ADD PERMISSIONS**.
   Permissions specify the functional areas available to users in this role.
7. In the **ADD PERMISSIONS** dialog box, scroll through the table, and select the check boxes that correspond to the permissions that you want to grant to the new role.
8. Click **DONE**.
   If any of the permissions you selected require additional permissions, these are listed with a warning symbol ⚠.
9. To add any required dependencies to the new role, click **ADD MISSING PERMISSIONS**.
   The **CREATE NEW ROLE** dialog box now lists the additional dependent permissions.
10. Click **SAVE**.

> **Tip**
> You can also add missing permissions when you edit a custom role.

Application Security 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.

10.2.3. Deleting custom roles

If a custom role listed on the **Roles** page is not assigned to any user account, you can delete that role.

To delete a role:

1. Sign in to Application Security as an Administrator or Security Lead
2. On the header, select **Administration**.
3. On the navigation pane, expand **Users**, and then select **Roles**.
4. In the table, select the check box for the custom roles you want to delete.
5. In the **Roles** toolbar, click **DELETE**.
6. Click **OK** to confirm the custom role deletion.

See also

Creating custom roles

10.3. 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 Application Security system. OpenText recommends that you create only the administrator-level accounts necessary to create and edit local or LDAP Application Security user accounts. The Security Lead and lesser accounts can perform all other application-related activities.

Application Security permits the explicit addition of administrator-level accounts to application versions. This enables administrators to be assigned issues from the **AUDIT** page.

Topics covered in this section:

- Creating local user accounts
- Editing local user accounts
- Unlocking local user accounts
- Viewing externally managed users and groups

10.3.1. Creating local user accounts

As an Administrator, you can add new local user accounts to Application Security.

> **Important**
>
> You cannot create externally managed users from Application Security. These can only be provisioned using the SCIM API.

To create a Application Security user account:

1. Sign in as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Users**, and then select **Local Users**.
4. In the **Local Users** toolbar, click **+ADD**.
5. In the **CREATE NEW USER** dialog box, provide the information listed in the following table.

> **Important**
>
> Values for fields in the following table marked with an asterisk (*) *must not* start with the characters `=`, `-`, `+`, or `@`, and must not include control characters.

Field	Description
*Username	User name for the account.
*First Name	(Optional, but strongly recommended) First name of user.
*Last Name	(Optional, but strongly recommended) Last name of user.
*Email	(Optional) Email address of user. **Note** Although an email address is not required, the user cannot receive email alerts and notifications unless you provide one.
Password	Password for the new user account. The **Password Strength** indicator displays the relative strength of the password you entered. You can save the user account information only if the password is evaluated as strong or very strong.
Confirm Password	Password for the new user account.
User must change password at next login	Leave this check box selected to require the user to change the password at the next sign in to Application Security.
Password never expires	Select this check box to allow the user to use the originally assigned password until he or she wants to change it. To require the user to change their password every thirty days, leave this check box cleared.
Suspended	Select this check box to suspend access to Application Security for this user account.
Roles	(Optional, but strongly recommended) Select the check boxes for all roles to assign to the user account. **Caution** Although this is optional, a user who has no assigned role cannot access Application Security unless that user belongs to a local group that does have an assigned role.

Access	To specify the applications that the new user can access: **Note** If you have assigned the user account the role of **Administrator** or **WebInspect Enterprise System**, the user has universal access to all Application Security applications. 1. Click **ADD**. 2. From the **APPLICATION** list, select an application to which you want the user to have access. The **VERSIONS** list in the center pane displays all active versions of the selected application. 3. Select the check boxes for all versions that you want the user to be able to access. To select all versions, select the **Select all** check box. The **SELECTED VERSIONS** pane lists the versions you have selected. 4. To add another application version or versions, repeat steps b and c. 5. Click **DONE**.

6. Do one of the following:
   - To save your settings and create another new user account, click **SAVE AND ADD ANOTHER**.
   - To save your settings and close the **CREATE NEW USER** dialog box, click **SAVE**.

See also

Editing local user accounts

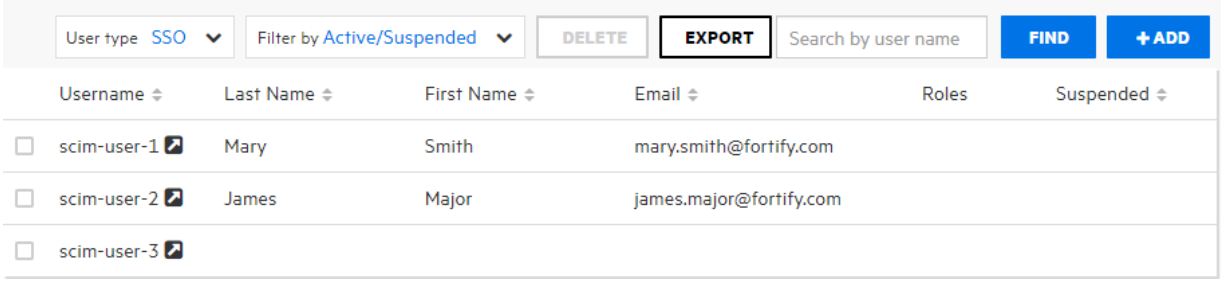
Unlocking local user accounts

10.3.2. Editing local user accounts

The following procedure describes how to edit the account for local user accounts created from Application Security, as well as user accounts provisioned using the SCIM API.

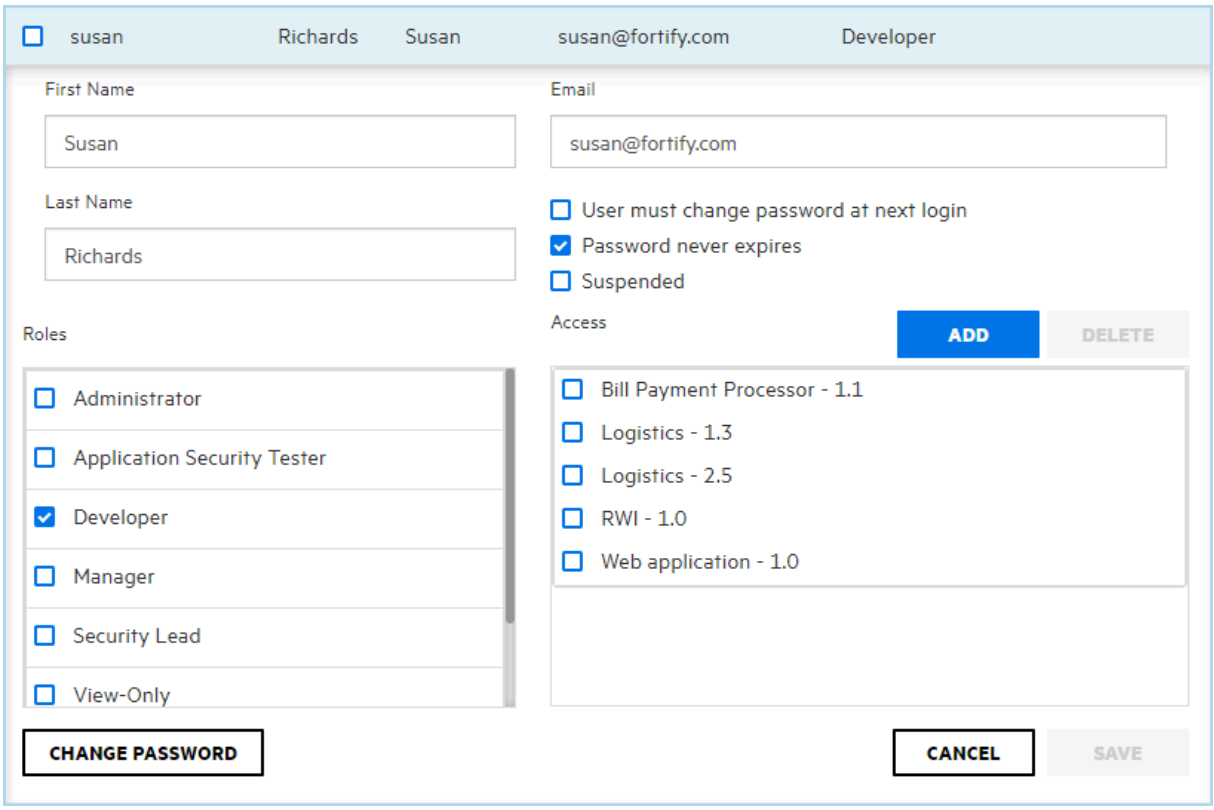
To edit a local user account:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Users**, and then click **Local Users**.
3. To selectively view externally managed users (provisioned using the SCIM API), from the **User type** list, select **SSO**.



4. Locate the user account you want to edit, and then click the row to expand it and view the account details.

5. Click **EDIT**.



6. Make any required changes to values in the **First Name**, **Last Name**, and **Email** boxes.

> **Important**
> Values for the **First Name**, **Last Name**, and **Email** fields must not start with the characters `=`, `-`, `+`, or `@`, and must not include control characters. For a complete list of Unicode characters included in these restricted ranges, see Control characters in ASCII and Unicode.

> **Important**
> From Application Security, the only changes you can make to externally-managed user and group accounts are role and application version assignments. You must perform all other configuration (and deletion) from Entra ID.

7. To change the email address password expiration policy, select or clear the check boxes below the **Email** box.
8. To change the roles assigned to the user, in the **Roles** area, select or clear the check boxes for available roles.
9. To remove the user from application versions, in the **Access** area, select the check boxes for the application versions, and then click **DELETE**. To assign the user to different application versions, click **ADD**, and then specify the application versions the user can access.
10. To change the password for the user, click **CHANGE PASSWORD**, and then specify a new password.
    If this is an externally managed user, the **CHANGE PASSWORD** button is not available.
11. Click **SAVE**.

See also

Unlocking local user accounts

Creating local user accounts

10.3.3. Unlocking local user accounts

After a local user tries unsuccessfully to sign in to three times in a row, Application Security prevents the user from attempting more sign ins. If email notifications are enabled, the user receives an email to advise them that they are locked out and to notify the Application Security Administrator. As an Administrator, you can unlock the account for the user.

> **Note**
>
> The locking and unlocking of user accounts does not apply to users provisioned through the SCIM API.

After a user notifies you that they are locked out of their account, unlock the account as follows:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Users**, and then click **Local Users**.
3. Locate the user account you want to unlock, and then click the row to expand it.
4. Click **UNLOCK USER**.
5. To confirm unlocking of the user account, click **OK**.

See also

Creating local user accounts

Editing local user accounts

10.3.4. Viewing externally managed users and groups

To view externally managed users provisioned using the SCIM API:

1. Sign in as a local Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Users**, and then select **Local Users**.
4. At the top of the **Local Users** page, from the **User type** list, select **SSO**.
   Application Security lists the users provisioned using the SCIM API. The **Externally managed user** symbol is displayed next to each user name listed in the **Local Users** table.

To see the groups pushed from Entra ID:

1. Sign in to Application Security as a local Administrator.
2. In the header, select **Administration**.
3. On the navigation pane, expand **Users**, and then select **Local Groups**.

Assigning roles to externally managed users and groups

A user or member of a local group provisioned from an identity management service such as Entra ID cannot access Application Security unless the group has been assigned one or more roles, or the user is assigned a role individually from the **Local Users** page.

> **Important**
>
> From Application Security, the only changes you can make to externally-managed user and group accounts are role and application version assignments. You must perform all other configuration (and deletion) from Entra ID.

Assign roles to externally managed users and groups just as you would for local users created through the **Administration** view.

See also

Implementation of SCIM 2.0 protocol

Enabling SCIM for provisioning of externally managed users and groups

Using SCIM 2.0 and SAML 2.0 to configure a connection to Microsoft Entra ID for user provisioning

Configuring Application Security to work with SAML 2.0-compliant single sign-on

11. Applications and application versions

To obtain consistent measurement results, you define an application for a single codebase. Application Security organizes the iterative development and remediation of codebases into *applications* and *application versions*.

- An application is a codebase that serves as a container for one or more application versions. If you are working with a new codebase, you create a new Application Security application. Application Security automatically creates the first version of that application.
- An application version is an instance of the application or codebase that is to eventually be deployed. It contains the data, auditing, and attributes for a particular version of the application codebase. If you are working with an existing codebase, 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 analysis results	= Trending results
Results of any previous security analysis from OpenText Fortify SAST (Fortify Static Code Analyzer), OpenText Fortify DAST (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 are fixed and issues that remain

Analysis processing rules verify that the new scan is comparable to the older scan.

This section contains the following topics:

- About tracking development teams
- About creating application versions
- Viewing application versions
- Saving application view
- Searching applications and application versions from the Applications view
- Recalculating application metrics
- Editing application version details
- Exporting selected data for an application version
- Using bug tracking systems to help manage security vulnerabilities
- Changing the template associated with an application version
- Setting analysis result processing rules for application versions
- Configuring Fortify Audit Assistant options for an application version
- Enabling auto-apply and auto-predict for an application version
- About custom tags
- About deleting application versions

11.1. 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. Application Security 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.

This section contains the following topics:

- About the application creation process
- Strategies for creating application versions
- About annotating application versions for reporting

11.1.1. About the application creation process

After you sign in to Application Security and start to add a new application, a wizard displays a sequence of steps, each of which presents the team members responsible for creating the application version with strategy choices. After the team agrees and makes their selections, the Security Lead can complete the creation process.

Typically, the security team evaluates and decides on all the options before they actually start to create the application version. The following sections describe the options displayed on the wizard pages.

See also

Application version attributes

Template selection

Creating the first version of a new application

Adding a new version to an application

11.1.2. Strategies for creating application versions

As a Security Lead, you might choose to create an application version that enables you to track vulnerabilities within deployed applications. Security vulnerabilities often occur in areas of code where different components come together. Although teams might work on different components, it is good practice to track the entire software component as one piece. For 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 the file access library is not necessarily safe, because one might not know the origin of the text being processed.

11.1.2.1. 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 Manager can deactivate past application versions to archive results and remove them from view. For information about how to deactivate an application version, see Deactivating application versions.

  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 codebase, 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 evolved code (versus a complete rewrite).

11.1.2.2. Strategies for continuous deployment

For applications that use continual deployment, running scans with the `-build-label xxxx` option 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.

11.1.3. About annotating application versions for reporting

Application Security 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. Sample customizations can help organizations track onboarding progress by application ID, line of business, business unit, or regulatory compliance obligations.

11.2. About creating application versions

You can create a new Application Security application version for an entirely new application or create one for an existing application version. The following topics provide instructions for each method:

About the application creation process

Creating the first version of a new application

Adding a new version to an application

11.2.1. Application version attributes

Application versions have business attributes, technical attributes, and organization attributes. These attributes are metadata that Application Security uses to perform cross-application comparisons and reporting.

When you create a new application version, the **CREATE NEW APPLICATION VERSION** wizard guides you through the selection of required and optional technical, organization, business, and OpenText Fortify ScanCentral DAST application attributes. You cannot create an application version 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 Application Security 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.

The following tables list the default set of attributes for Application Security applications. Note that this list does not include custom attributes that an Administrator might have added to the system.

Technical attribute	Description
Development Phase	(Required) Current phase of development the application version is in
Development Strategy	(Required) Staffing strategy used for application development
Accessibility	(Required) Level of access required to use the application
Application Type	Nature of the codebase (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 the application

Organization attribute	Description
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 attribute	Description
Business Risk	Relative risk (high, medium, or low) the application poses to the business goals of the organization
Known Compliance Obligations	All known compliance obligations that the application must meet
Data Classification	Types data to be stored by this application
Application Classification	Direct consumers of the application

OpenText Fortify ScanCentral DAST attribute	Description
Base URL	URL prefix that all pages in your application start with, which is useful in establishing relative pathways

11.2.1.1. Creating custom attributes

Application Security 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.

<p autonum="Note: ">You can create custom attributes only if you have either an Administrator or Security Lead user account. <<repetitive to prior para>></p>

To create a custom attribute:

1. Sign in as an Administrator or a Security Lead.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Templates**, and then select **Attributes**.
4. Click **NEW**.

5. In the **CREATE NEW ATTRIBUTE** dialog box, provide the information described in the following table.

Field	Description
Name	Type a descriptive name for the attribute. **Important** If you delete an attribute that Application Security uses by default, and you then create a new attribute with the same name, database migration might fail.
Description	Type a brief description. The description is displayed under the attribute field in the **CREATE NEW APPLICATION VERSION** wizard.
Category	Select an attribute type. Depending on the category you select, the attribute is displayed on corresponding attribute tab of the **CREATE NEW APPLICATION VERSION** wizard.

Type	Select one of the following control types: ○ To create a text field into which a user can type a single line of text, select **Text - Single Line**. ○ To create a list from which a user can select only a single value for the attribute, select **List of Values - Single Selection**.  **Note** If you create a single-selection type attribute, users can select it from the **Group by** and **Aggregate by** lists on the **Dashboard** view to customize the displayed data. ○ To create a list from which a user can select multiple values for the attribute, select **List of Values - Multiple Selection**. ○ To create a text field into which a user can type multiple lines of text, select **Text - Multiple Lines**.  **Note** If you select one of the **List of Values** types, additional fields are displayed in which you add the values and their descriptions, and specify whether they are hidden. ○ To create a check box for the attribute, select **Boolean**. ○ To create a field that accepts an integer value, select **Integer**. ○ To create a calendar selection control for the attribute, select **Date**.  **Note** This type is not available for a dynamic scan request attribute. <<WIE>>
Required	Select this check box to require users to set this attribute when they create an application template.

Hidden	Select this check box to prevent this new attribute from being displayed in the **CREATE NEW APPLICATION VERSION** wizard. **Important** If you select **Hidden** to prevent the attribute from displaying in the **CREATE NEW APPLICATION VERSION** wizard, you must also clear the **Required** check box.

6. Click **SAVE**.

The new attribute is available the next time a user creates a new application version.

For instructions on how to specify custom attributes in existing application versions, see Applying new custom attributes to application versions.

Note

By default, a custom attribute you create through the user interface is deletable. You can use the Application Security API to define a non-deletable attribute. For information about how to access the API, see Accessing the API documentation.

See also

Deleting attributes and attribute values

Application version attributes

11.2.1.2. Deleting attributes and attribute values

If an attribute or attribute value is no longer of use, you can often delete it from the Application Security database, even if it is currently associated with one or more application versions. Doing so removes all traces of the attribute or attribute value from the system.

Deleting attributes

To delete an attribute from the Application Security database:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then select **Attributes**.
   If an attribute cannot be deleted, its check box appears dimmed, and you cannot select it for deletion.

   To see an explanation of why you cannot delete an attribute, point to the check box. The attribute is either system-defined, or it is user-defined and specified as non-deletable.
3. Select the check boxes for the attributes you want to delete, and then click **DELETE**.
   <meta class="data-nv" data-nv="SSC_Short" data-nv-value="Fortify Software Security Center" data-productid="2174" data-replace-parent="false" data-version="25.2"/> alerts you to the fact that the selected attributes will be permanently removed from the system and prompts you to confirm that you want to continue with the deletion.
4. To confirm that you want to permanently remove the attribute from the system, click **OK**.

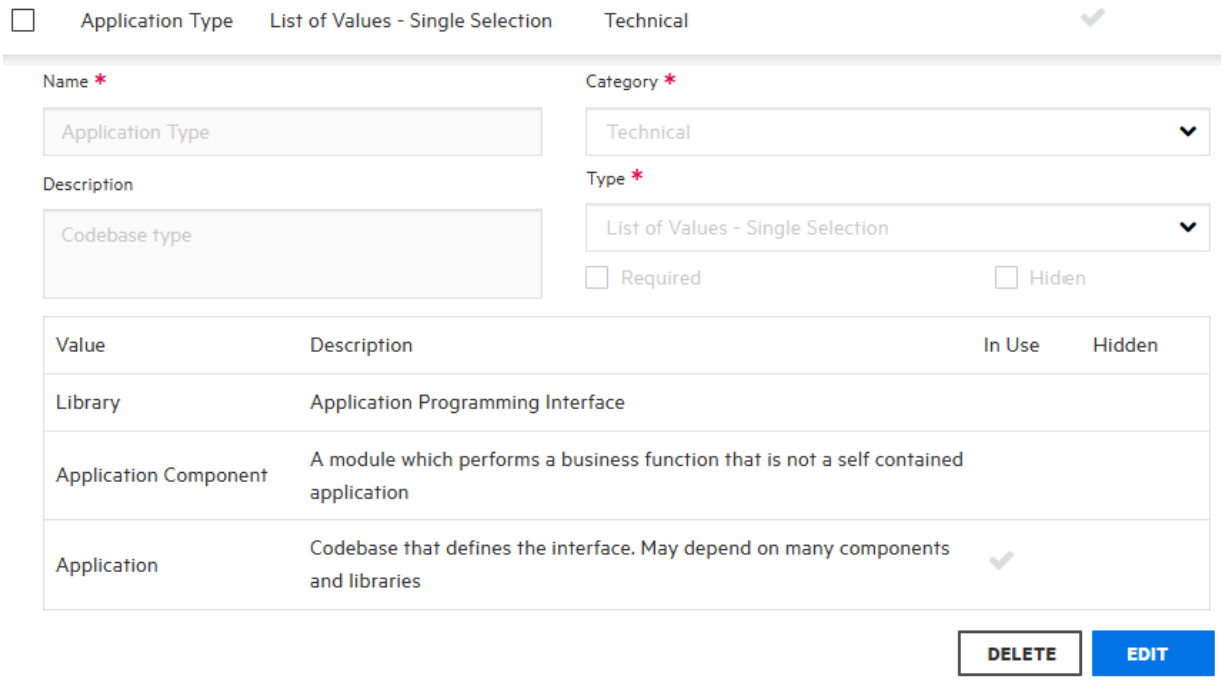
<p autonum="Note: ">By default, a custom attribute you create through the user interface is deletable. You can use the <meta class="data-nv" data-nv="SSC_Short" data-nv-value="Fortify Software Security Center" data-productid="2174" data-replace-parent="false" data-version="25.2"/> API to define a non-deletable attribute. For

information about how to access the API, see Accessing the API documentation .</p>

Deleting attribute values

To delete an attribute value:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then select **Attributes**.
3. Click to expand the row for the attribute that has one or more values that you want to delete.



   The **In Use** column indicates which values are currently used with one or more application versions.
4. Click **EDIT**.
5. To confirm you want to edit the attribute, click **OK**.
6. Click the **Delete** button for the value you want to delete.

> **Note**
> You can delete some attribute values, even if they are currently in use by one or more application versions. However, you cannot delete:
> - Values for system-defined list-type attributes that are in use
> - Values for system-defined attributes other than list type
> - Values that are both in use and that belong to a dynamic scan type attribute
> - Values for user-defined attributes designated as non-deletable that are in use

   Application Security removes the value without prompting you for confirmation. If you decide that you prefer not to delete the value, click **CANCEL** to restore it.

See also

Creating custom attributes

11.2.1.3. Applying new custom attributes to application versions

To apply a new custom attribute to an application version:

1. On the header, select **Applications**.
2. Select the application version for which you want to specify a new attribute.
   Application Security displays the **AUDIT** page for that version.

3. On the toolbar, click **PROFILE**.
4. In the **APPLICATION PROFILE** dialog box, click **APPLICATION SETTINGS**.
5. In the **Version Settings** area, click the **Edit** button .
6. Select **ATTRIBUTES**.
7. Select the attribute category, and then select the value or values for the new custom attribute.
8. Click **SAVE**.

See also

Creating custom attributes

Editing application version details

11.2.2. About issue templates

Applications are defined by *issue templates*, which determine how Application Security 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

Application Security comes with several 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 issue templates:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then select **Issue Templates**.

The **Issue** page lists the issue templates and their descriptions.

You can import a Application Security issue template into Fortify Audit Workbench, modify it, save it with a new name, and then import it into Application Security. You can also create a new issue template from scratch in Fortify Audit Workbench.



Note

When editing or creating filter sets and folders in Fortify Audit Workbench, be aware that the search modifiers used by Fortify Audit Workbench and Application Security might produce different results. Not all searches, filters, or folders based on search expressions will produce the same results. For example, if your search expression contains external metadata categories such as OWASP or CWE, your results might not match because the expressions might differ on Application Security and Fortify Audit Workbench. When there are multiple matched external categories, Application Security matches any of them, but Fortify Audit Workbench expects an exact match of all external categories. If you encounter this issue when editing or creating issue templates for use in Application Security, contact Customer Support for assistance.

For instructions on how to modify or create an issue template in Fortify Audit Workbench, see the *OpenText™ Fortify Audit Workbench User Guide*.

11.2.2.1. Adding issue templates to the system

To add an issue template from Fortify Audit Workbench to Application Security:

1. Sign in to Application Security as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Templates**, and then select **Issue Templates**.
   Application Security lists the system issue templates.
4. Click **NEW**.
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. Next to **Template**, click **BROWSE**, and then locate and select the new or modified template.
8. Click **SAVE**.

11.2.2.2. Template selection

Application Security issue templates provide 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.

11.2.3. Creating the first version of a new application

An application version consists of the data and attributes for a given variant of the application codebase.

To create the first version of a new application:

1. Sign in as an Administrator or a Security Lead.
2. In the **Dashboard** or **Applications** view, click **+ NEW APPLICATION VERSION**.
   The **CREATE NEW APPLICATION VERSION** wizard opens.
3. On the **GENERAL** tab, provide the information described in the following table.

Field	Description
Application Setup	
Application name	(Required) Type the application name. **Important** The application name must not start with the characters `=`, `-`, `+`, or `@`, and must not include control characters. For a complete list of Unicode characters included in these restricted ranges, see Control characters in ASCII and Unicode.
Application description	(Optional) Type a description of the new application.
Version Setup	
Version name	(Required) Type a name for the version. **Important** The version name must not start with the characters `=`, `-`, `+`, or `@`, and must not include control characters. For a complete list of Unicode characters included in these restricted ranges, see Control characters in ASCII and Unicode.
Version description	(Optional) Type information about this first version of the application.

Use existing application version	To use the settings of an existing application version, select this check box and do the following: 1. Click **BROWSE**. 2. Locate and select the application that has the settings you want to use for the new application. You can type a string into the search box, and then click **FIND** to refine the list of applications. The **VERSIONS** pane lists the active versions of the selected application. To display inactive versions, select the **Show inactive** check box. 3. From the **VERSIONS** list, select the check box for the version you want, and then click **DONE**. By default, Application Security includes all settings of the selected application version. 4. To exclude one or more settings, clear the corresponding check boxes for the settings. 5. To copy over all of the issues and audits associated with the selected application version, select the **Application state** check box. Only audits up to the latest application version metrics refresh are copied. To refresh the application metrics before you copy the application state, see Recalculating application metrics.

4. To proceed to the **ATTRIBUTES** settings, click **NEXT**.
5. On the **TECHNICAL ATTRIBUTES** tab, provide the information described in the following table.

Field	Description
Development Phase	Select **New**.
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.

This tab can also include technical attributes defined by your organization.

6. (Optional) Select the **ORGANIZATION ATTRIBUTES** tab, and then provide the information described in the following table.

Field	Description
Business Unit	Select the business unit with which to associate the new application.
Industry	Select the industry for which this application is being developed.
Region	Select the region to associate with the application.

This tab can also include organization attributes defined by your organization.

7. (Optional) Click the **BUSINESS RISK ATTRIBUTES** tab, and then provide the information described in the following table.

Field	Description
Business Risk	Select the value that best represents the relative risk that this new application poses to the business goals of your organization.
Known Compliance Obligations	Select the check boxes for all known compliance obligations that apply to the new application.
Data Classification	Select the check boxes for all data classifications that this application stores.
Application Classification	Select the check boxes for all consumer types for which this application is being developed.

This tab can also include business risk attributes defined by your organization.

8. If you are using OpenText Fortify ScanCentral DAST, click the **SCANCENTRAL DAST ATTRIBUTES** tab and then do the following:
    - Enter the **Base URL** to set the prefix for all of the pages in your application.
9. To proceed to the **POLICIES** settings, click **NEXT**.
   If the data retention policy is configured to allow application versions to opt-out of it, then you can opt-out of the policy for this application version. By default, all application versions are included in the default data retention policy. For more information about the data retention policy, see About data retention.
10. To opt-out of the data retention policy for this application version, from the **Data Retention Policy to Follow** list, select **None (Opt-out of Default)**.
11. To proceed to the **TEMPLATE** settings, click **NEXT**.
12. Under **Issue Template**, select the check box for a template that sets the minimum thresholds for issue detection. To see a description of a template displayed in the pane to the right, select its check box. The default template is Prioritized High Risk Issue Template.
13. To proceed to the **ACCESS** settings , click **NEXT**.
14. To add users to the team for this application version, do one of the following:
    - To assign a user from the Application Security database:
        1. Select **LOCAL**.
        2. Select the check boxes for the team member or members you want to assign.
           To find a specific user, type a user name into the **Search by user name** box, and then click **FIND**.
    - To assign a user from the LDAP directory:
        1. Click **LDAP**, and then, from the **View By** list, select the attribute to use to display LDAP entities.
        2. Select the check boxes for the team member or members to assign.
           To find a specific user, type a user name into the **Search by user name** box, and then click **FIND**.

15. Click **SAVE**.
    The new application version is now displayed in the **Applications** view. After data is uploaded for the application version, it is also displayed in the **Dashboard** view.
16. Click **CLOSE**.

See also

Uploading scan artifacts

Adding a new version to an application

11.2.4. Adding a new version to an application

> **Important**
>
> Before creating a new application version by copying or using an existing version, you must wait for Application Security to complete the current state recalculation.

To create a new version of an existing application:

1. Sign in as an Administrator or a Security Lead.
2. From the **Applications** view, select an application version, and then click **+ NEW VERSION**.
   The **Application name** and **Application description** boxes are populated with the name and description of the selected application.
3. On the **GENERAL** tab, under **Version Setup**, provide the information described in the following table.

Field	Description
Version name	Type a name for the version. **Important** The version name must not start with the characters `=`, `-`, `+`, or `@`, and must not include control characters. For a complete list of Unicode characters included in these restricted ranges, see Control characters in ASCII and Unicode.
Version description	(Optional) Type a description of this version of the application.
Use existing application version	To use the settings of an existing application version, select this check box and do the following: 1. Click **BROWSE**. 2. Locate and select the application that has the settings you want to use for the new application. You can type a string into the search box, and then click **FIND** to refine the list of applications. The **VERSIONS** pane lists the active versions of the selected application. To display inactive versions, select the **Show inactive** check box. 3. From the **VERSIONS** list, select the check box for the version you want, and then click **DONE**. By default, Application Security includes all settings of the selected application version. 4. To exclude one or more settings, clear the corresponding check boxes for the settings. 5. To copy over all of the issues and audits associated with the selected application version, select the **Application state** check box. Only audits up to the latest application version metrics refresh are copied. To refresh the application metrics before you copy the application state, see Recalculating application metrics.

4. To proceed to the **ATTRIBUTES** settings, click **NEXT**.
5. On the **TECHNICAL ATTRIBUTES** tab, provide the information described in the following table.

Field	Description
Development Phase	From this list, select the current development phase of the new version.
Development Strategy	Select the strategy used to develop the new application version.
Accessibility	Select the value that specifies how the application is to be accessed.
Application Type	Select the application type.
Target Deployment Platform	Select the target deployment platform.
Interfaces	Select the check boxes for the interfaces available to access the application.
Development Languages	Select the check boxes for the languages used to develop the application version.
Authentication System	Select the check boxes for the authentication systems used to access the application.

This tab can also include technical attributes defined by your organization.

6. (Optional) Select the **ORGANIZATION ATTRIBUTES** tab, and then provide the information described in the following table.

Field	Description
Business Unit	Select the business unit for which the application version is being developed.
Industry	Select the industry sector to which the application version applies.
Region	Select the region for which the application version is being developed.

This tab can also include organization attributes defined by your organization.

7. (Optional) Select the **BUSINESS RISK ATTRIBUTES** tab, and then provide the information described in the following table.

Field	Description
Business Risk	Select the value that best represents the risk this application version poses to your organization.
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.

This tab can also include business risk attributes defined by your organization.

8. If you are using OpenText Fortify ScanCentral DAST, click the **SCANCENTRAL DAST ATTRIBUTES** tab and then do the following:
   - Enter the **Base URL** to set the prefix for all of the pages in your application.

   This tab can also include OpenText Fortify ScanCentral DAST attributes defined by your organization.
9. To proceed to the **POLICIES** settings, click **NEXT**.
   If the data retention policy is configured to allow application versions to opt-out of it, then you can opt-out of the policy for this application version. By default, all application versions are included in the default data retention policy. For more information about the data retention policy, see About data retention.
10. To opt-out of the data retention policy for this application version, from the **Data Retention Policy to Follow** list, select **None (Opt-out of Default)**.
11. To proceed to the **TEMPLATE** settings, click **NEXT**.
12. Under **Issue Template**, select the check box for a template to set the minimum thresholds for issue detection.
    To see a description of a template displayed in the pane to the right, select its check box. The default template is Prioritized High Risk Issue Template.
13. To proceed to the **ACCESS** settings, click **NEXT**.
14. To add users to the team for this application version, do one of the following:

    Note
    A user in the Administrator role already has full access to all applications. You cannot assign an Administrator user to a team unless the user has also been assigned another role. This is true whether the Administrator is a local user or an LDAP user.

    - To assign a user from the Application Security database:
      1. Select **LOCAL**.
      2. Select the check boxes for the team member or members you want to assign.
         To find a specific user, type a user name into the **Search by user name** box, and then click **FIND**.
    - To assign a user from the LDAP directory:
      1. Click **LDAP**, and then, from the **View By** list, select the attribute to use to display LDAP entities.
      2. Select the check boxes for the team member or members you want to assign.
         To find a specific user, type a user name into the **Search by user name** box, and then click **FIND**.
15. Click **SAVE**.
    The new application version is now displayed in the application versions list.
16. Click **CLOSE**.

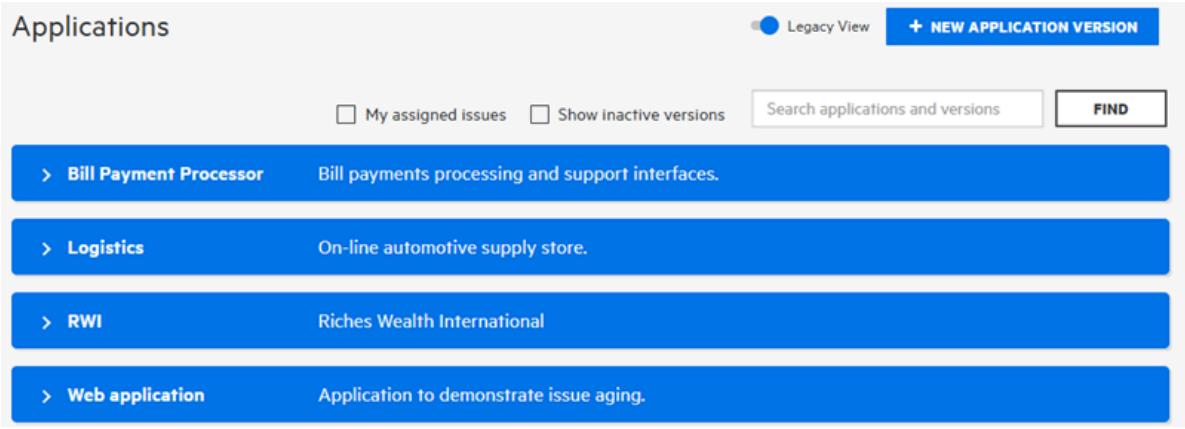
See also

Creating the first version of a new application

11.3. Viewing application versions

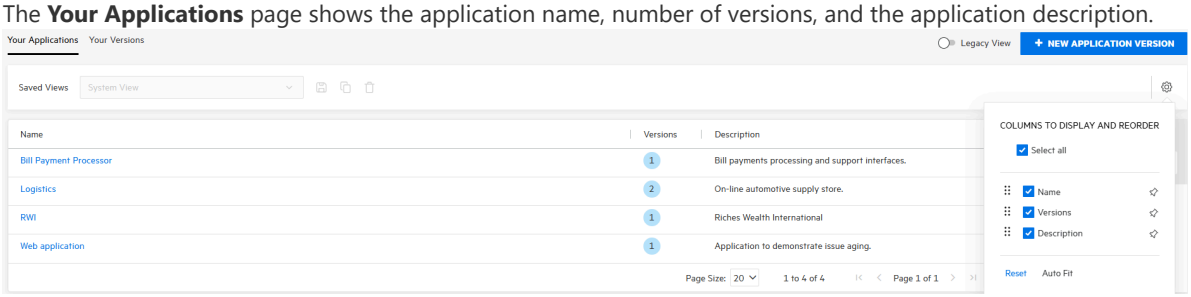
To view the application versions:

1. On the header, select **Applications**.
   The first time you access the **Applications** view, the applications are displayed in the **Legacy View**.



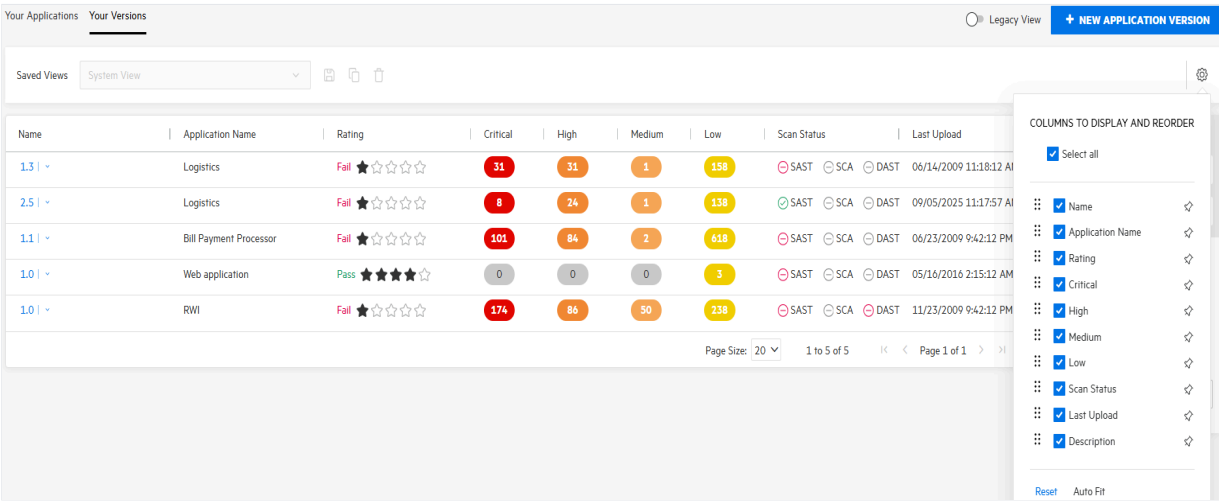
To view the versions for an application in the **Legacy View**, click an application row.

2. To view the applications in the modern **Applications** view, turn off the **Legacy View** switch.
   The **Your Applications** page shows the application name, number of versions, and the application description.



To view the versions for an application, click the application name.

The **Your Versions** page shows the application version name, version description, application name, rating (visual of the Fortify Security Rating performance indicator), scan type and status, and the date and time of the most recent scan.



Note

When you select **Scan Status** in the **Columns to Display and Reorder**:
If the scan type is STATIC/SAST (SCA):

- Displays **SAST**.
- Exists and has been in the last 30 days, it displays a green check.
- Exists and has been more than 30 days in the past, it displays a red hyphen.
- Does not exist, it displays a grey hyphen.

If the scan type is DYNAMIC/DAST (WebInspect):

- Displays **DAST**.
- Exists and has been in the last 30 days, it displays a green check.
- Exists and has been more than 30 days in the past, it displays a red hyphen.
- Does not exist, it displays a grey hyphen.

If the scan type is OPEN SOURCE (Sonatype, Debricked):

- Displays **SCA**.
- Exists and has been in the last 30 days, it displays a green check.
- Exists and has been more than 30 days in the past, it displays a red hyphen.
- Does not exist, it displays a grey hyphen.

You can hover over the icon to check the date of the last scan.

To view all the columns displayed in **Your Applications** or **Your versions** page, click **Columns to Display and Reorder**. By default, the **Select all** check box is selected.

You can either clear the **Select all** check box and select the required columns or clear the check box next to the column name that you do not require. To remove the column from **Your Applications** or **Your versions** page, you can drag the column out of the table.
If you drag all the columns out, click **Columns to Display and Reorder** and select the required columns to view.
To adjust the column width, click **Reset** or **Auto Fit**.
You can drag and drop the column names to arrange the columns based on your requirement.

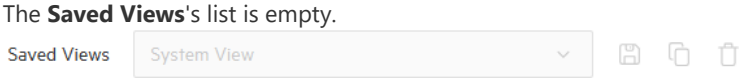
See also

Searching applications and application versions from the Applications view

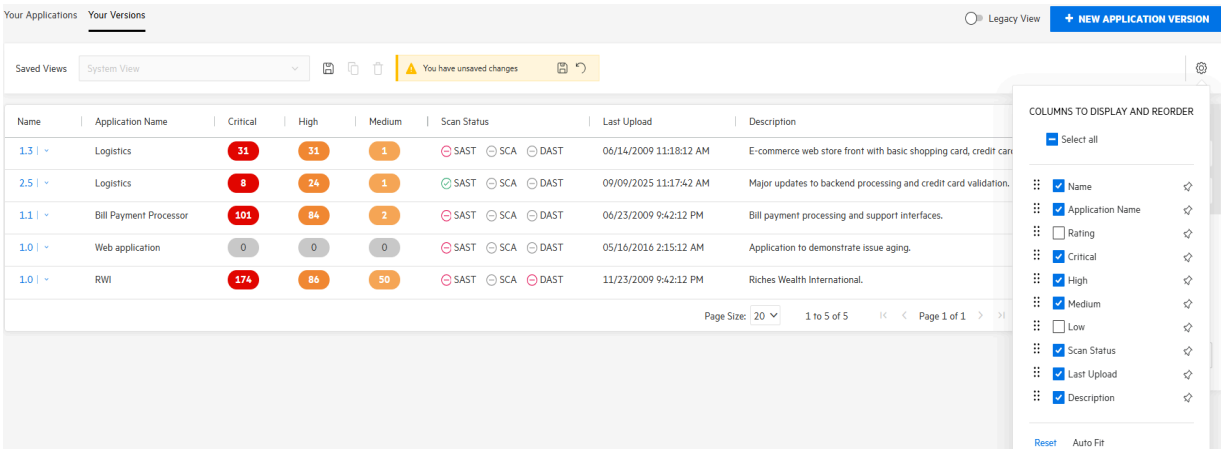
11.4. Saving application view

To save the application view:

1. The default view of **Your Applications** or **Your versions** page is displayed when you access the **Applications** view. The **Saved Views**'s list is empty.



2. When you modify the page, using the options **Columns to Display or Reorder**, **Filters**, **General** or **Attributes**, the **Save/Update view** icon is enable.



3. To save the modifications, click **Save/Update view**.
   Click **Undo** to discard the modifications.
4. Type the name of the view. Select **Mark as default view** if required.
5. Click **SAVE**. The name of the saved view appears in the list.

You can create and save the new views. You can also modify the already saved views and click **Rename fiter/view** to save them as needed.

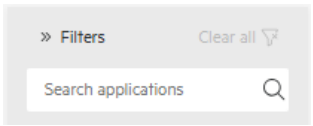
To delete the saved views, select the view and then click **Delete**.

11.5. Searching applications and application versions from the Applications view

Searching specific application

To search for a specific application:

1. Select the **Your Applications** page.
2. Under **Filters**, in the **Search applications** box, type at least part of the application name you want to find.



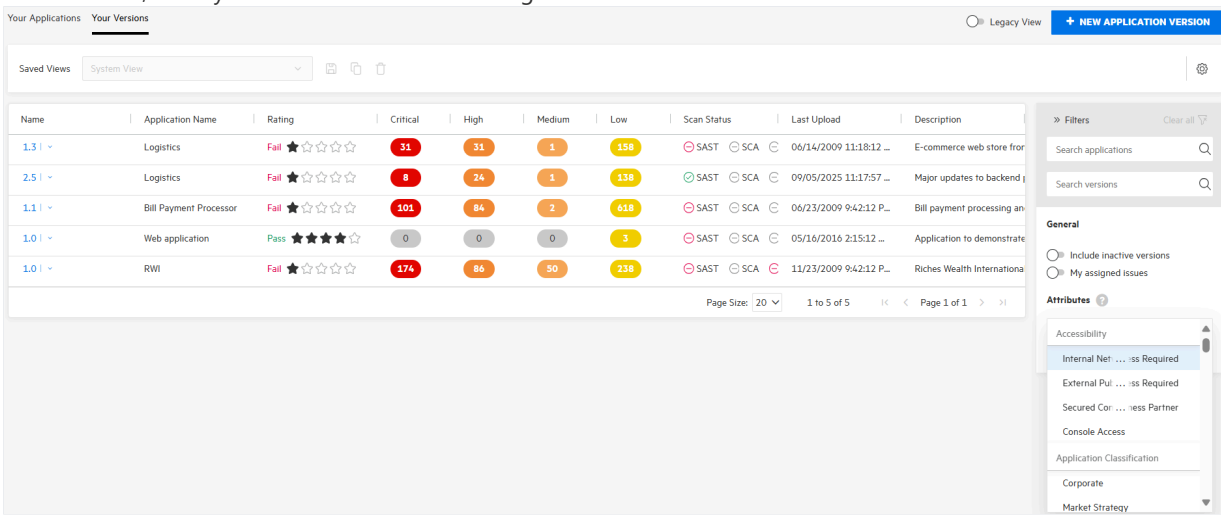
3. To return to the complete **Your Applications** page, clear the text in the search box.

Searching application version

To search for an application version:

1. Select the **Your Versions** page.

2. Under **Filters**, do any combination of the following:



   - In the **Search applications** box, type at least part of the application name you want to find.
   - In the **Search versions** box, type at least part of the application version name you want to find.

     Note
     The wildcards asterisk (*) and question mark (?) are not supported in either search box.

   - In the **Attributes** list, select one option per attribute you want to find. You can select up to three options. To remove a selected attribute, click the **x** next to its name. To remove all selected attributes, click **Clear attributes**.

   The **Your Versions** page lists all the application versions that match your search criteria.
3. To return to the complete **Your Versions** page, click **Clear all**.

(**Legacy View**) To search for a specific application or application version:

1. In the **Search applications and versions** box, type at least part of the application name or version name for the application or version you want to find.
   The wildcards asterisk (*) and question mark (?) are not supported.
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

11.6. Recalculating application metrics

If an application version has pending audit information, its **OVERVIEW** page displays a Pending Changes button .

To recalculate the metrics for the application:

- Click the **Pending Changes** button , and then, in the **REFRESH APPLICATION METRICS** dialog box, click **REFRESH NOW**.

Refreshing the application metrics also updates the application state (merged analysis results). The metrics refresh might take time, depending on current system activity. After the refresh is complete, the **OVERVIEW** page displays the latest data for the application.

See also

Downloading scan artifacts

11.7. Editing application version details

To edit the details of an application version:

1. On the header, select **Applications**.
2. Select the application version to edit.
3. On the **AUDIT** page, click the **Edit** button .



4. In the **EDIT VERSION** dialog box, click a tab to edit values in any of the fields described in Adding a new version to an application.
5. Click **SAVE**.

See also

Changing the template associated with an application version

11.8. Exporting selected data for an application version

You can export selected data for an application version to a comma-separated values (CSV) file. To determine how long the system retains your CSV files, see Configuring job scheduler settings.

To export data for an application version:

1. On the header, select **Dashboard** or **Applications**.
2. Select an application version.
3. (Optional) On the **AUDIT** page, you can select attributes to filter by.
4. Click **EXPORT**.

> **Note**
> A missing **EXPORT** button indicates that your Administrator has disabled this functionality.

5. In the **File Name** box, type a name for the file.
6. (Optional) In the **Notes** box, type information about the data you are exporting.
7. Click **SAVE**.
8. To view the exported result:
    1. On the header, select **Reports**.
    2. Click **DATA EXPORTS**.

    3. In the **Audit** table, point to the row for the exported file, and then click the **Download** button .

See also

Exporting the Dashboard summary table

11.9. 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 Application Security, 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, Application Security 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 Application Security for complete issue details

This section contains the following topics:

- Bug tracker configuration
- Velocity templates for bug filing
- Assigning a bug tracking system to an application version
- Submitting a bug for a single issue
- Submitting a bug for multiple issues
- Bug state management

11.9.1. Bug tracker configuration

To enable a team to access and use a bug tracking system from Application Security, a security lead or development manager must configure Application Security 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 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

Adding bug tracker plugins

Authoring bug tracker plugins

11.9.2. Velocity templates for bug filing

Text-based fields for filing bugs in Application Security 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.

Application Security provides pre-defined templates for the summary and description fields of the supported bug tracker plugins that ship with Application Security. 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

Customizing Velocity Templates for Bug Tracker Plugins

Deleting Velocity Templates

11.9.2.1. Adding Velocity Templates to Bug Tracker Plugins

Application Security provides pre-defined templates for the summary and description fields of the supported bug tracker plugins that ship with Application Security. 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, ensure 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, OpenText 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 header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then select **Bug Filing Templates**.
   The **Bug Filing** page lists the template groups for supported bug trackers.
3. In the table, click the row that shows the template group for your bug tracker plugin.
   The row expands to display details for the pre-defined templates mapped to the description and summary fields for the plugin.
4. Click **EDIT**.
5. Click **+ ADD FIELD**.
6. In the **Mapped Field** box, 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 formatting 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**.
   <div class="Admonition_Note"> <p autonum="Note: ">Not all variables are available for all issues. In particular, verbose content such as “ATTRIBUTE_COMMENTS,” “ISSUE_DETAIL,” and “ISSUE_RECOMMENDATION” is available only if you are filing a bug for a single issue. <<repeat of what's in the UI>></p> </div>
8. Click **APPLY**.
9. To add another template, repeat steps 5 through 8.
10. Click **SAVE**.

On the **Bug Filing** page, the details for the bug tracking plugin now include your new template.

See also

Velocity templates for bug filing

Customizing Velocity Templates for Bug Tracker Plugins

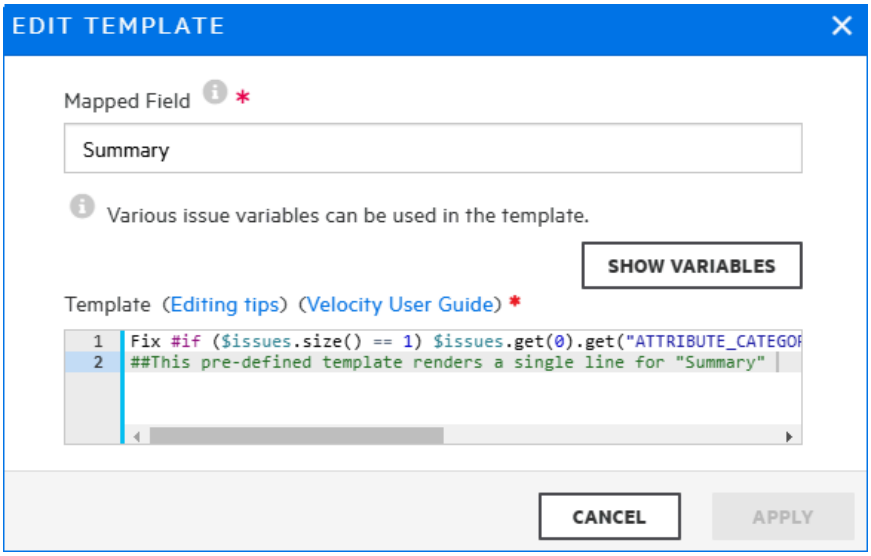
Bug tracker configuration

Deleting Velocity Templates

11.9.2.2. Customizing Velocity templates for bug tracker plugins

To customize the Velocity template for a bug tracker plugin:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then select **Bug Filing Templates**.
3. In the table, 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. Click the **Edit field** button  for the mapped field you want to modify.



6. To see useful tips on how to edit the template, click the **Editing tips** link.
   To access detailed instructions on how to modify the template, click the **Velocity User Guide** link. This takes you to the Apache Velocity Project website. To see a list of all available variables, click **SHOW VARIABLES**.
7. Make any necessary changes to the content in the **Mapped Field** and **Template** boxes.
8. Click **APPLY**.
9. Click **SAVE**.

The details displayed for the bug tracker plugin now include your changes.

See also

Deleting Velocity Templates

Velocity templates for bug filing

Adding Velocity Templates to Bug Tracker Plugins

11.9.2.3. 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 header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then select **Bug Filing Templates**.
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**.

> **Caution**
> OpenText 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

Adding Velocity Templates to Bug Tracker Plugins

Customizing Velocity templates for bug tracker plugins

11.9.3. 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.

To integrate with a bug tracking system:

1. On the header, select **Applications**.
2. Select the application version to which you want to assign a bug tracker.
   The **AUDIT** page for the selected application version lists the issues in the version.
3. On the toolbar, click **PROFILE**.
4. In the **APPLICATION PROFILE** dialog box, click the **BUG TRACKER** tab.

5. From the **Bug Tracker Integration** list, select the application to use for tracking bugs for this application version.
6. Complete the required fields, and then click **VALIDATE CONNECTION**.
7. In the **TEST BUG TRACKER PLUGIN CONFIGURATION** dialog box, type your bug tracker authentication credentials, and then click **TEST**.
   After Application Security verifies your connection to your bug tracker, it displays a message to indicate that the test was successful.
8. Click **OK**.
   You can enable bug state management for the application version. With bug state management enabled, Application Security can update bugs as the states of the issues within those bugs change.
9. (Optional) To enable bug state management, select the **Bug state management** check box.
10. In the **Username** and **Password** boxes, provide the credentials for your bug tracker, and then click **APPLY**.
11. Click **OK**.
12. Click **CLOSE**.

See also

About bug tracking system integration

Adding bug tracker plugins

Submitting a bug for multiple issues

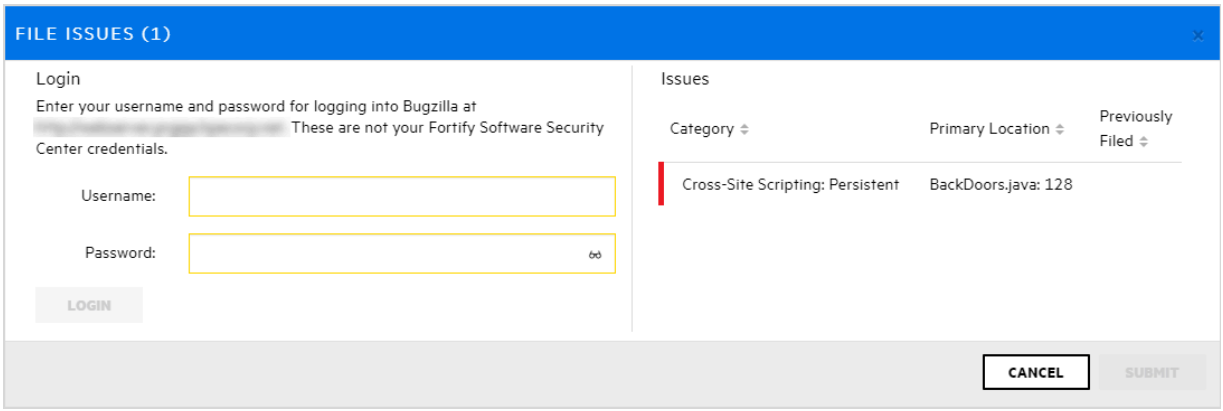
Authoring bug tracker plugins

11.9.4. Submitting a bug for a single issue

If a bug tracking plugin is specified for an application version (see Assigning a bug tracking system to an application version), you can use that bug tracker to submit bugs that cover one or multiple issues.

To submit a bug for a single issue:

1. From the **AUDIT** page for an application version, expand the row for an issue for which you want to submit a bug.
2. Click **FILE BUG**.
   If **FILE BUG** is not available, a bug tracker is not assigned to the application version. To address this, see Adding bug tracker plugins and Assigning a bug tracking system to an application version. Also, if a bug is already submitted for the issue, you cannot submit a new bug against it.



3. In the **Login** area, provide the username and password for the bug tracker associated with this application version, and then click **LOGIN**.
   Application Security retains your credentials for the duration of your work session so you do not have to provide them to file additional bugs during that session.
   The **Login** area displays the fields for the bug tracker specified for the application version.
4. Provide input for all fields required for the bug tracker, and then click **SUBMIT**.

After a successful submission, a bug icon is displayed for the issue in the **Bug submitted** column of the issues table.

See also

Submitting a bug for multiple issues

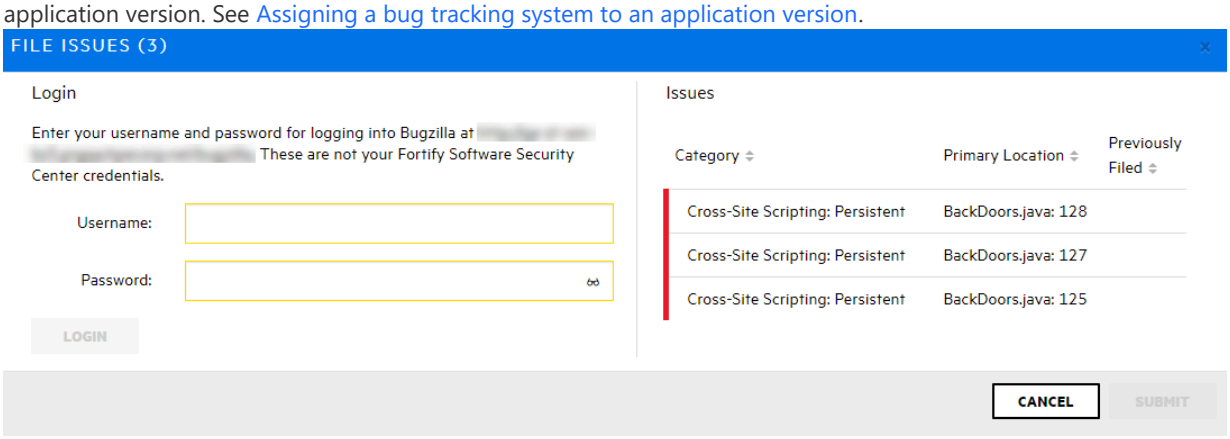
Viewing bugs submitted for issues

11.9.5. Submitting a bug for multiple issues

If a bug tracking plugin has been specified for an application version (see Assigning a bug tracking system to an application version), you can submit bugs that cover one or multiple issues. For information about how to file a bug for just one issue, see Submitting a bug for a single issue.

To submit a single bug that covers multiple issues:

1. From the **AUDIT** page for an application version, select the check boxes for all issues that you want to include in a bug, and then, above the issues table, click the **File Bug** button .
   If, after you select check boxes, the **File Bug** icon is not visible, you first need to set up a bug tracker for the application version. See Assigning a bug tracking system to an application version.



Note

If a bug was previously submitted for a selected issue, you cannot submit a new bug against that issue. The **FILE ISSUES** dialog box displays the message, "Some selected issues have already been filed and will be ignored," and displays a bug icon for the issue in the **Previously Filed** column.

2. In the **Login** area, provide the username and password for the bug tracker associated with this application version, and then click **LOGIN**.
   Application Security retains your credentials for the duration of your work session so you do not have to provide them to file additional bugs during that session.
   The **Login** section displays the fields for the bug tracker specified for the application version.
3. Provide input for all required fields, and then click **SUBMIT**.

After a successful submission, a bug icon is displayed for the selected issues in the **Bug submitted** column of the issues table.

See also

Submitting a bug for a single issue

Viewing bugs submitted for issues

11.9.6. Bug state management

Bug state management enables Application Security to make specific updates to bugs as the states of the issues within those bugs change. Application Security checks new security scans to determine whether filed bugs are to remain open, or can be closed.

If analysis results indicate that one of more security issues associated with a previously submitted bug persist (and match the selection criteria), Application Security 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), Application Security updates the bug to indicate that stakeholders can resolve or close this ticket. To enable auditing and traceability, Application Security 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.

11.10. Changing the template associated with an application version

You can modify many settings for an existing application version, including its issue template. However, keep in mind that assigning a different issue template to an application version or updating an issue template on the server results in loss of synchronization between the database cache and existing audit sessions.



Caution

OpenText recommends that you change the template associated with an application version only if no results have yet been processed for that application version. If you change the issue template for an application version for which results have already been processed, Application Security does not recalculate the issue metrics and metrics generated based on the previously assigned template are unavailable and cannot be deleted.

To change the template associated with an application version:

1. Sign in as either an Administrator or Security Lead.
2. On the header, select **Applications**.
3. Select the application version you want to modify.
4. On the toolbar, click **PROFILE**.
5. In the **APPLICATION PROFILE** dialog box, click **APPLICATION SETTINGS**.
6. In the **Version Settings** area, click the edit button .



Caution

Changing the template can alter the metrics calculated for the application version. Existing metrics are not recalculated.

7. In the **EDIT VERSION** dialog box, click the **TEMPLATE** tab.
   In the list of templates, the currently assigned template is marked as selected.
8. Select the check box for the template you prefer to use for the application version.
9. Click **SAVE**.

After you change the template, Application Security invalidates any auditing session of the affected application version (for example, by a different user) and displays a message to advise you that the application version audit session must be restarted.



Note

Anyone using Fortify Audit Workbench to audit the affected application version does not see this information.

11.11. Setting analysis result processing rules for application versions

The analysis result processing rules enable management approval and oversight of code scans. You can specify the rules that are followed when analysis results for an application version are processed during scan artifact uploads.

Administrators can configure the global file-count and line-count thresholds. The default percentage is 10%. For information about changing the global values, see Configuring global processing rule defaults.

To configure the analysis result processing rules for an application version:

1. Sign in as an Administrator
2. On the header, select **Dashboard** or **Applications**.
3. Select the application version for which you want to configure the processing rules for analysis results.
4. On the toolbar, click **PROFILE**.
5. In the **APPLICATION PROFILE** dialog box, select the **PROCESSING RULES** tab, and then review the listed processing rules.
6. Select or clear the check boxes for the processing rules you want to apply to the application version.
   These processing rules are described in the following table.

Processing rule	Description
Require approval if the Build Project is different between scans	Application Security 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, Application Security compares the external metadata version for the file with the external metadata version on the Application Security server. If the external metadata version for the FPR file is later than the external metadata file version on the server, Application Security requires approval for the file upload. If the external metadata version for the FPR file is earlier than, or the same as, the external metadata file version on the server, then Application Security allows the FPR file upload.
Require approval if file count decreases by more than 10%.	Application Security compares the file count for the scan and the scan that preceded it. If the file count decreased by more than ten percent, management approval is required before the scan can be uploaded.
Require approval if file count increases by more than 10%.	Application Security compares the file count for the scan and the scan that preceded it. If the file count increased by more than ten percent, management approval is required before the scan can be uploaded.
Require approval if result has Fortify Java Annotations	Application Security checks if the scan results include Fortify Java annotations. If any of the annotations is detected, management approval is required before the scan can be uploaded.
Require approval if line count decreases by more than 10%.	Application Security compares the line count for the scan and the scan that preceded it. If the line count decreased by more than ten percent, management approval is required before the scan can be uploaded.
Require approval if line count increases by more than 10%.	Application Security compares the line count for the scan and the scan that preceded it. If the line count increased by more than ten percent, management approval is required before the scan can be uploaded.

Require approval if the engine version of a scan is newer than the engine version of the previous scan	Application Security checks if any scan engine (<meta class="data-nv" data-nv="SCA_Short" data-nv-value="OpenText SAST" data-productid="2174" data-replace-parent="false" data-version="25.2"/>, <meta class="data-nv" data-nv="WebInspect_Short" data-nv-value="OpenText DAST" data-productid="2174" data-replace-parent="false" data-version="25.2"/>, <meta class="data-nv" data-nv="WebInspectAgent" data-nv-value="OpenText DAST Agent" data-productid="2405" data-replace-parent="false" data-version="25.2"/>) version is newer than the one already used in the application. If it detects a newer version, management approval is required before the scan can be uploaded.
Ignore SCA quick scan results and SCA speed dial results performed with a setting of less than four.	Blocks the processing of OpenText Fortify SAST (Fortify Static Code Analyzer) scans done in quick scan mode, which searches for high-confidence, high-severity issues. This rule also prevents the upload of speed dial analysis results performed at a level of less than four. To enable uploading speed dial and quick scan analysis results, clear this check box. **Caution** After you choose between uploading a full scan or uploading speed dial analysis results, OpenText recommends that future analysis results uploaded for the application version be of the same type.
Require approval if the Rulepacks used in the scan do not match the Rulepacks used in the previous scan	Application Security checks if 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, management approval is required before the scan can be uploaded.
Require approval if SCA or WebInspect Agent scan does not have valid certification	Application Security checks if an OpenText Fortify SAST or OpenText DAST Agent scan has valid certification. If the certification is not valid, then someone might 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 scan upload requires management approval.

Require approval if result has analysis warnings	Application Security checks if an OpenText Fortify SAST or OpenText DAST Agent scan contains analysis warnings. If it detects analysis warnings, the scan upload requires management approval. **Note** This processing rule applies only to the first upload of a given analysis results file, and does not apply to subsequent uploads of the artifact. For example, if audit information is added to a previously-uploaded FPR file that contains analysis warnings, Application Security does not require management approval when the changed artifact is again uploaded.
Perform Force Instance ID migration on upload	A newer version of OpenText Fortify SAST (Fortify Static Code Analyzer) or of a Rulepack can change an instance ID from one created in a previous scan by an earlier version of OpenText Fortify SAST or a Rulepack. Both instance IDs identify the same issue. When enabled, this processing rule forces migration of old instance IDs to the corresponding new instance IDs, even if the OpenText Fortify SAST version (or Rulepack) versions are the same. For detailed information about how this rule works, see About processing rules that affect instance ID migration.
Automatically perform Instance ID migration on upload	A newer version of OpenText Fortify SAST (Fortify Static Code Analyzer) or of a Rulepack can change an instance ID from one created in a previous scan by an earlier version of OpenText Fortify SAST or a Rulepack. Both instance IDs identify the same issue. When enabled, this processing 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. For detailed information about how this rule works, see About processing rules that affect instance ID migration.
Warn if audit information includes unknown custom tag	If the audit information includes an unknown custom tag, the processing 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 processing rule blocks the upload.

Disallow upload of analysis results that change values of hidden tags	If the analysis results contain any changes to values of hidden tags, Application Security blocks upload of the analysis results.
Disallow upload of analysis results if there is one pending approval	If an analysis result still requires approval, Application Security blocks the upload of the analysis results.
Disallow approval for processing if an earlier artifact requires approval	If an earlier scan artifact requires approval, and was not approved, this rule blocks the user from approving the current scan artifact. If this processing rule is *not* selected, then when a user approves the current artifact, all previous artifacts are automatically approved.

7. Click **APPLY**.
8. To confirm that you want to save the settings for analysis result processing rules, click **OK**.

About processing rules that affect instance ID migration

Two processing rules affect instance ID migration; Perform Force Instance ID migration on upload, and Automatically perform Instance ID migration on upload. It is useful to understand how these are used.An issue instance ID can mutate for any one of the following reasons:

- The IID-generation algorithm changes with a new OpenText Fortify SAST version
- Use of a new Rulepack version
- Changes to scan settings
  For example, using extra rules are specified for a scan.
- Vulnerable code is duplicated
  For example, the same vulnerable code is copied and pasted multiple times in an application version. In this case, OpenText Fortify SAST generates a unique instance ID for the first duplicate fragment, and then increments this generated instance ID for all remaining duplicated fragments. So, two separate scans can produce different instance IDs for the same code fragments, depending on the order in which the two scans uncover them.

The **Automatically perform Instance ID migration on upload** rule addresses issue instance ID mutation that results either from an IID-generation algorithm change with a new OpenText Fortify SAST version, or from a change in Rulepack version. For example, Application Security detects that the OpenText Fortify SAST version used in the latest scan is newer than the version used for previous scans. With **Automatically perform Instance ID migration on upload** selected, Application Security runs the migration. If Application Security detects no changes in the OpenText Fortify SAST version used, it does not run the migration (even if **Automatically perform Instance ID migration on upload** is selected).

The **Perform Force Instance ID migration on upload** rule addresses instance ID mutation that results from changes in scan settings or from vulnerable code duplication. Application Security can easily determine whether the OpenText Fortify SAST version or Rulepack version has changed. If Application Security detects such a change, it performs the migration automatically. However, in other cases (duplicate code, scan settings), Application Security cannot make this determination. You can use this processing rule to force Application Security to perform migration in such cases.

If you suspect that the issue instance ID changed as a result of either changes in scan settings or vulnerable code duplication, OpenText recommends that you select the **Perform Force Instance ID migration on upload** processing rule.



Note

Instance ID migration takes a noticeable amount of time, which is why these two rules exist. Because you might not want to run IID migration every time, these rules let you determine whether to run instance ID migration after each scan upload.

See also

Uploading scan artifacts

Approving analysis results for an application version

11.12. Configuring Fortify Audit Assistant options for an application version

You can override the default Fortify Audit Assistant options for an application version if you set this ability when you configured Fortify Audit Assistant (see Configuring Fortify Audit Assistant). Otherwise, the default settings are used for all application versions.

To configure Fortify Audit Assistant options for an application version:

1. Ensure that Application Security is configured to use Fortify Audit Assistant with your applications.
2. On the header, select **Dashboard** or **Applications**.
3. Select the application version for which you want to configure Fortify Audit Assistant options.
4. On the toolbar, click **PROFILE**.
5. In the **APPLICATION PROFILE** dialog box, select the **AUDIT ASSISTANT OPTIONS** tab.
6. From the **Application version prediction policy** list, select the prediction policy that you want Fortify 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. Otherwise, Fortify Audit Assistant uses the default prediction policy.

7. To have unaudited issues for this application version sent to the Fortify Audit Assistant server for assessment, select the **Enable auto-predict** check box.

   Note
   The **Enable auto-prediction** and **Enable auto-apply** check boxes are available only if those audit settings are enabled system-wide.

8. To have Fortify Audit Assistant automatically apply predicted values to the mapped custom tag values, select the **Enable auto-apply** check box.
9. Click **APPLY**.
10. To confirm your changes, click **OK**.
11. Click **CLOSE**.

See also

Configuring Fortify Audit Assistant

11.13. Enabling auto-apply and auto-predict for an application version

If your Administrator has configured Fortify Audit Assistant, enabled auto-apply system-wide, and mapped the appropriate primary custom tags fields in the Custom Tags section of the Administration view, you can enable auto-apply for a specific application version.

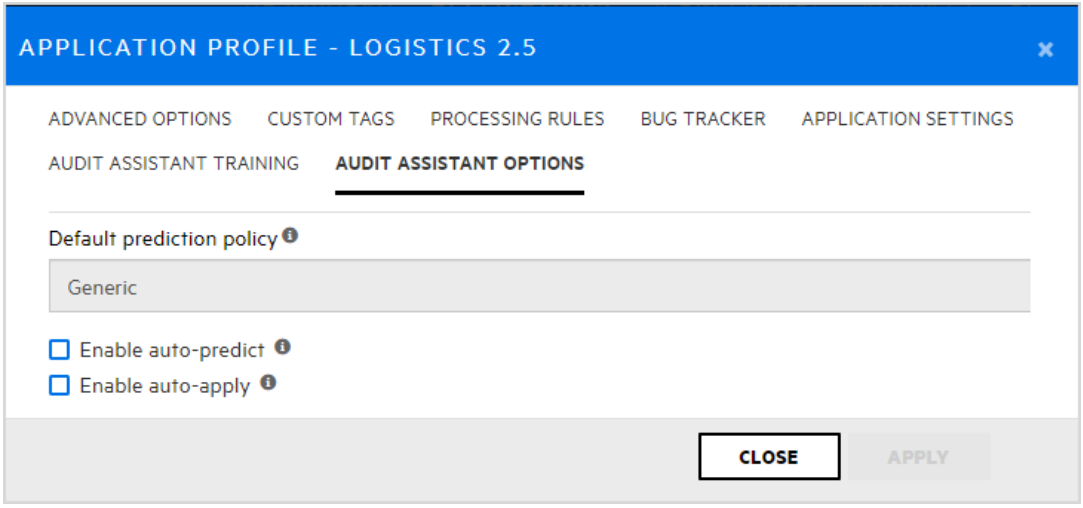
If you enable auto-apply for an application version, then whenever you use Fortify Audit Assistant to request a prediction on your static analysis issues, Application Security applies those predictions to your custom tag values.

When Fortify Audit Assistant automatically applies custom tag values to issues, the metadata saved for the issue shows that it was audited by Fortify Audit Assistant. A gray gavel displayed next to the custom tag name informs users that Fortify Audit Assistant predicted the issue.

To enable auto-apply for an application version:

1. From the **Dashboard** or **Applications** view, select the application version for which you want to enable auto-apply.
2. On the toolbar, click **PROFILE**.

3. Select **AUDIT ASSISTANT OPTIONS**.



4. To have Fortify Audit Assistant automatically assess unaudited issues, select the **Enable auto-predict** check box. For information on auto-prediction, see About Audit Assistant auto-prediction.
5. Select the **Enable auto-apply** check box.
   If your primary tag values are not mapped to Audit Assistant, Application Security displays a warning to that effect and advises you to contact your Administrator.
6. Click **APPLY**.
7. To save your settings, click **OK**.
8. Click **CLOSE**.

See also

Configuring Fortify Audit Assistant

11.14. About custom tags

To audit code in Application Security, the security team examines analysis results and assigns values to "tags" that are associated with application issues. The development team can then use these tag values to determine which issues to address and in what order.

By default, Application Security provides a single default tag named **Analysis** to use for issue assessment. Valid values for the **Analysis** tag are **Exploitable**, **Not an Issue**, **Suspicious**, **Reliability Issue**, and **Bad Practic**e. You can modify the **Analysis** tag attributes, revise the tag values, or add new tag values to support your auditing needs.

To refine your auditing process, you can define your own custom tags. Like the **Analysis** tag, your custom tag definitions are stored in an issue template that you can associate with an application version. For example, you might create a custom tag used to track the sign-off process for an issue. After a developer audits the issues assigned to them, a security expert can review those issues and mark each as "approved" or "not approved."

Note

Fortify Audit Workbench users can add custom tags to their projects as they audit them. However, if these custom tags are not defined in Application Security for the issue template associated with the corresponding application version, then the new custom tags are lost after the Fortify Audit Workbench user uploads an FPR file to Application Security.

This section contains the following topics:

- Adding custom tags to the system
- Modifying custom tag attributes
- Globally hiding custom tags
- Deleting custom tags

- Adding custom tag values
- Editing custom tags
- Deleting custom tag values
- Associating custom tags with issue templates
- Removing custom tags from issue templates
- Assigning custom tags to application versions
- Disassociating a custom tag from an application version
- Managing custom tags through issue templates
- Managing custom tags through an issue template in an FPR file

11.14.1. Adding custom tags to the system

As an Administrator, you can add custom tags to the system.

> **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.

To add a custom tag:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then select **Custom Tags**.
3. On the **Custom Tags** page, click **NEW**.
4. Type a name for the new tag in the **Name** box.

   > **Important**
   >
   > Ensure that the name you specify for a custom tag *is not* a database reserved word.

5. (Optional) In the **Description** box, type content that describes how to use the custom tag.
6. From the **Type** list, select one of the tag types listed in the following table.

Type	Values accepted
Date	Calendar date in the format specified in system-wide preferences (see Setting preferences system-wide and across application versions).
Decimal	Number with a precision of up to 18 (up to 9 decimal places)
List	Selection from the list of values that you specify for the tag
Text	String with up to 500 characters (HTML/XML tags and newlines are not allowed)

7. (Optional) Select any or all of the following optional tag features:
   - **Restricted**—To allow only users with specific permission (managers, security leads, administrators) to modify the tag, select this check box.
   - **Extensible**—(List-type only) Make a custom tag *extensible*, which means that auditors can add values to it as they audit issues. To enable users to add new values to the list tag during audits, select this check box.
   - **Hidden**—To prevent the display of the tag in the **ASSIGN** dialog box or in Fortify Audit Workbench, select this check box.

- **Requires comment**—To require users to leave a comment whenever the value of this custom tag changes, select this check box. If a custom tag that requires a comment is changed, the system automatically adds a comment to indicate the changes made to the tag.

  > **Note**
  > If the new custom tag that requires a comment is a date-type tag, the date users select for the tag while auditing is always in the format specified in the **PREFERENCES** dialog box.

8. If your new custom tag is a date-, decimal-, or text-type tag, click **SAVE**. If your new custom tag is a list-type tag, you need to add values. For information on creating values for your list-type custom tag, see Adding custom tag values.

See also

Mapping Fortify Audit Assistant analysis tag values to Application Security custom tag values

Globally hiding custom tags

Deleting custom tags

Custom tags

Editing custom tags

Associating custom tags with issue templates

Managing custom tags through issue templates

Managing custom tags through an issue template in an FPR file

11.14.2. Modifying custom tag attributes

To modify the attributes of a custom tag:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then click **Custom Tags**.
3. On the **Custom Tags** page, click the row that displays the tag you want to modify.
   The row expands to reveal the details.
4. Click **EDIT**.
5. Modify the tag attributes, and then save your changes.

> **Caution**
> Ensure that the name you specify for a custom tag *is not* a database reserved word.

See also

Adding custom tag values

Adding custom tags to the system

11.14.3. Globally hiding custom tags

To globally hide a custom tag:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then click **Custom Tags**.
3. Click the row for the tag you want to hide.
   The row expands to display the details for the tag.
4. Click **EDIT**.
5. Select the **Hidden** check box.
6. Click **SAVE**.

The custom tag no longer appears on the **AUDIT** page or in Fortify Audit Workbench.

11.14.4. Deleting custom tags

If you are an Administrator or a Security Lead, you can delete custom tags.

> **Note**
>
> You cannot delete a custom tag if:
>
> - It is set as the primary tag.
> - It has been used in auditing issues.
> - It is currently associated with an application version or issue template. For information on how to remove a custom tag from an application version, see Disassociating a custom tag from an application version. For information on how to remove a custom tag from an issue template, see Removing custom tags from issue templates.
>
> You can never delete the **Analysis** tag.

To delete custom tags:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then click **Custom Tags**.
3. Select the check boxes for the custom tags you want to delete.
4. In the **Custom Tags** toolbar, click **DELETE**.
5. To confirm deletion of the selected tags, click **OK**.

See also

Custom tags

11.14.5. Adding custom tag values

As an Administrator, you can add values to list-type custom tags.

> **Note**
>
> If a custom tag is assigned the extensible attribute, then you can add values to it as you audit issues.

If Fortify Audit Assistant is configured, see Add a custom tag value ([%=FortifyProducts_Vars.AuditAssistant%] configured).

To add a value to a list-type custom tag:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then click **Custom Tags**.
3. Click the row for the custom tag to which you want to add a value.
4. Click **EDIT**.
5. Click **+ ADD**.
   The **ADD VALUE** dialog box opens.
6. Type a name and, optionally, a description for the new value.
7. (Optional) To prevent the tag from being displayed in the Assign dialog box or in Fortify Audit Workbench, select the **Hidden** check box.
8. Click **APPLY**, and then click **SAVE**.
9. (Optional) Setting the Issue State.
10. To add additional values, repeat steps 5 through 9.

See also

Add a custom tag value ([%=FortifyProducts_Vars.AuditAssistant%] configured)

Assigning custom tags to application versions

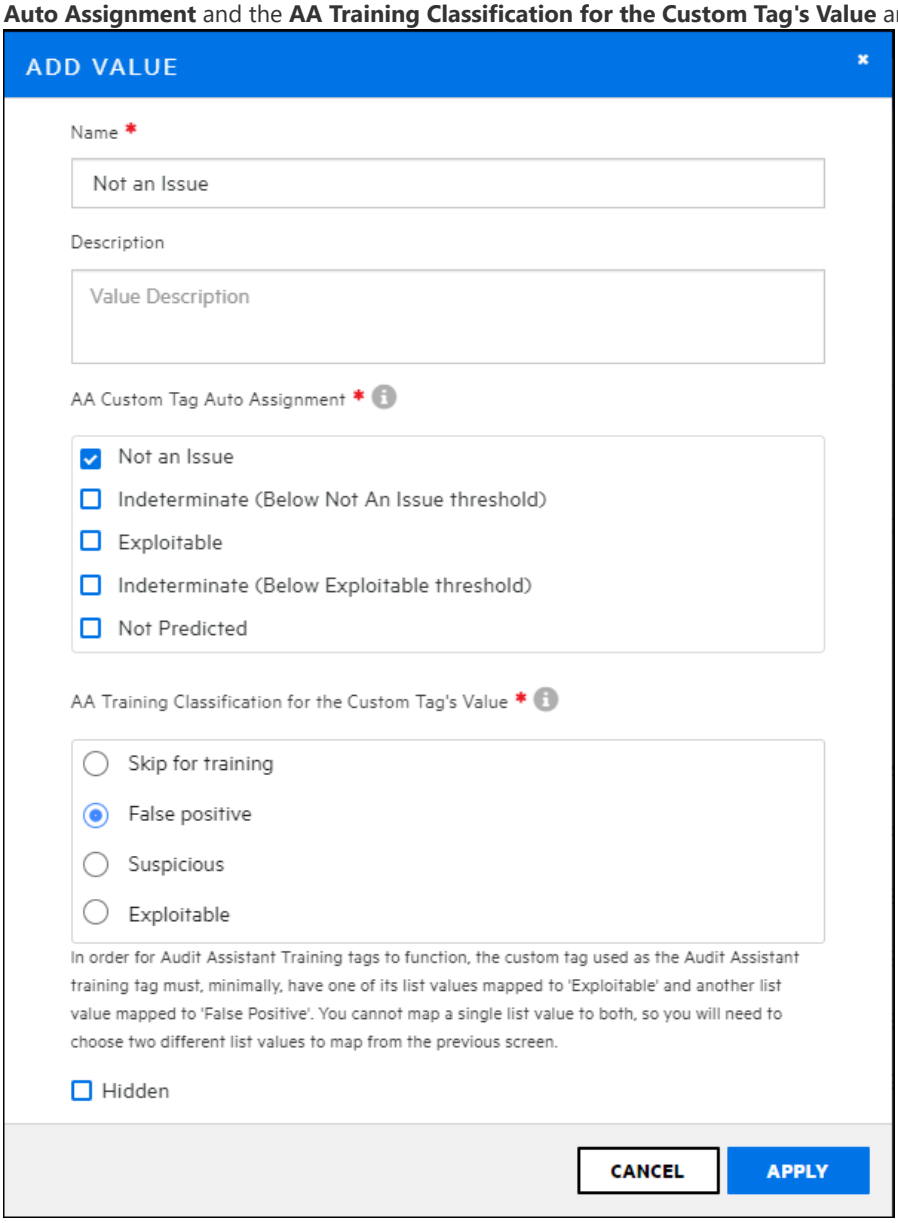
11.14.5.1. Add a custom tag value (Fortify Audit Assistant configured)

When adding or editing a custom tag value, you will:

- Specify a name for the new value
- (Optional) Provide a description for the new value
- Map your custom values to Fortify Audit Assistant values and decide whether the value is used in training the Fortify Audit Assistant model
- Assign the value to an Issue State

To add a value to a list-type custom tag when Fortify Audit Assistant has been configured:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then click **Custom Tags**.
3. Click the row for the custom tag to which you want to add a value.
4. Click **EDIT**.
5. Click **+ ADD**.
   If Fortify Audit Assistant auto-apply feature is enabled, the **ADD VALUE** dialog box includes the **AA Custom Tag Auto Assignment** and the **AA Training Classification for the Custom Tag's Value** areas.



6. If the new value aligns with Fortify Audit Assistant prediction value in the **AA Custom Tag Auto Assignment** area, select its check box to automatically map the list value to the selected prediction value.

This enables automatic mapping of values for all application versions where you have enabled the auto-apply feature.

7. To train Fortify Audit Assistant, select what this custom tag value means to Fortify Audit Assistant. Repeat this step for each list value you want to use to train Fortify Audit Assistant.
   By setting this tag value for your issue, Fortify Audit Assistant learns how you view the issue based on how you classify it. Although you do not have to use all of the list values in training, you must assign at least two for training to occur. You must assign one value to **Exploitable** and one to **False Positive**.
8. (Optional) To prevent the tag from being displayed during an issue audit or in Fortify Audit Workbench, select the **Hidden** check box.
9. (Optional) Set the issue state (see Setting the Issue State).
10. Click **APPLY** and then 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.

11.14.5.2. Setting the Issue State

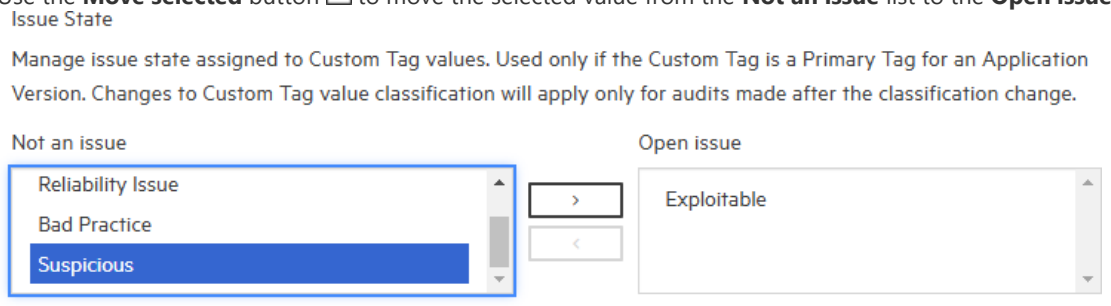
When adding values to your custom tag, you can set their Issue State if Fortify Audit Assistant is enabled. Using the Issue State, you can assign issues to one of two categories: Not an Issue or Open Issue. When auditing your results, you can select **Issue State** from the **Group By** menu to quickly assess which and how many issues are still open and need to be addressed. As you audit your issues and assign values to the **Analysis** custom tag value, the Issue State folders are updated based on the value you selected.

Custom Groups define audited issues by whether the issue is an Open Issue or Not an Issue based on the level of analysis set for the primary tag. Values equivalent to Suspicious and Exploitable are considered open issue states in the Analysis tag.

Initially, all added list-type custom tag values are listed in the **Not an issue** list of the **Issue State** area.

To set the Issue State for your custom tag values:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then click **Custom Tags**.
3. Click the row for the custom tag to which you want to edit a value.
4. Click **EDIT**.
5. In the **Issue State** area, select a value to be considered an open issue.
6. Use the **Move selected** button ▸ to move the selected value from the **Not an issue** list to the **Open issue** list.



7. Repeat steps 5 and 6 until all values are in the appropriate Issue State list.
8. Click **SAVE**.

See also

Editing custom tags

Deleting custom tag values

Adding custom tags to the system

Assigning custom tags to application versions

11.14.6. Editing custom tags

If you are an Administrator-level user, you can modify custom tags in the system.

To edit a custom tag:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then select **Custom Tags**.
3. Click the row for the tag you want to edit to expand it and display the details.
4. Click **EDIT**.
5. Edit the values for any of the displayed fields, and then click **SAVE**.

See also

Adding custom tags to the system

Deleting custom tag values

Assigning custom tags to application versions

11.14.7. Deleting custom tag values

Administrators and Security Leads can delete custom tag values.

> **Note**
>
> You cannot delete a custom tag value that is currently associated with an application version, issue template, or if an issue was audited using the value.

To delete a value for a custom tag:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then select **Custom Tags**.
3. Click the row for the tag from which you want to delete a value.
   The row expands to display the details for the tag.
4. Click **EDIT**.
5. In the table of values, click the **Remove value** button in the row for the value you want to delete.
6. Click **SAVE**.

See also

Editing custom tags

Adding custom tags to the system

Adding custom tag values

11.14.8. 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 header, select **Administration**.

2. On the navigation pane, select **Templates**, and then select **Issue Templates**.
3. Click the row that displays the issue template that you want to associate with the custom tag.
   The row expands to reveal the template details.
4. Click **EDIT**.
5. In the **CUSTOM TAGS** area, click **+ ADD CUSTOM TAG**.
6. In the **ADD CUSTOM TAG** dialog box, select the check box for the custom tag to associate with the issue template, and then click **+ADD**.
7. Click **SAVE**.

See also

Disassociating a custom tag from an application version

11.14.9. Removing custom tags from issue templates

To remove a custom tag from an issue template:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then select **Issue Templates**.
3. 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** area lists the custom tags currently associated with the template.

4. Click **EDIT**.

5. In the last column, click the **Remove custom tag** button for the custom tag that you want to remove from the template.

   > **Note**
   > You cannot remove the designated primary tag from an issue template.

6. Click **SAVE**.

See also

Custom tags

11.14.10. 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. On the header, select **Dashboard** or **Applications**.
2. Select the application version you want to edit. Or expand the row for the application, and then select the name of the version you plan to audit.
3. On the toolbar, click **PROFILE**.
4. In the **APPLICATION PROFILE** dialog box, select the **CUSTOM TAGS** tab.
5. Click **ASSIGN/ REMOVE**.
   The **CUSTOM TAGS** tab lists all of the tags available for auditing issues.
6. Select the check box for the custom tag you want to assign to the application version (you can select multiple tags), and then click **DONE**.
   The selected tag is now listed as an assigned tag.
   To successfully complete the audit of an issue in Application Security, you must specify a value for the custom tag that is designated as the *primary tag*. By default, the **Analysis** tag is the primary tag.

During an audit, the primary tag is listed first. If list-type custom tags other than **Analysis** exist in your Application Security instance and are assigned to the application version, you can select one of these (instead of **Analysis**) as the primary tag.

7. (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.

   1. Click **SELECT PRIMARY**.
   2. From the **Select Primary Tag** list in the SELECT PRIMARY TAG dialog box, select the tag to set as the primary custom tag.

      Note
      If you use Fortify Audit Assistant, and you have not provided Fortify Audit Assistant guidance information, ensure that you edit the tag to include that information. For information about how to provide Fortify Audit Assistant guidance, see Adding custom tags to the system. For information about how to edit a custom tag, see Editing custom tags.

   3. Click **DONE**.
8. Click **CLOSE**.

The assigned custom tag will be available the next time a team member audits issues for the application version.

See also

Disassociating a custom tag from an application version

11.14.11. 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 header, select **Dashboard** or **Applications**.
2. Select the application version to which the custom tag is assigned.
3. On the toolbar, click **PROFILE**.
4. In the **APPLICATION PROFILE** dialog box, select the **CUSTOM TAGS** tab.
5. Click **ASSIGN/REMOVE**.
   The **CUSTOM TAGS** tab lists all custom tags in the system. The check boxes for tags associated with the application version are selected.
6. Clear the check box for the custom tag that you want to remove, and then click **DONE**.
7. Click **CLOSE**.

The **AUDIT** tab in the issue details on the **AUDIT** page for this application version no longer lists the custom tag.

After you remove the custom tag from all application versions and issue templates to which it has been assigned, you can delete the tag.

See also

Removing custom tags from issue templates

Adding custom tags to the system

Assigning custom tags to application versions

11.14.12. 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 Application Security 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 Application Security, as follows:

1. On the header, select **Administration**.
2. On the navigation pane, expand **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.

11.14.13. Managing custom tags through an issue template in an FPR file

FPR files typically contain an issue template. If an FPR file uploaded to Application Security contains an issue template with a custom tag that has been set as editable, you can add a value to the tag.

11.15. About deleting application versions

You cannot directly delete an application in Application Security. Application Security removes an application automatically after all of its versions are deleted.

If you are assigned the Administrator role in Application Security, 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** views, you can *deactivate* it.

This section contains the following topics:

- Deactivating application versions
- Reactivating application versions
- Deleting an application version

11.15.1. Deactivating application versions

Deactivating an application version hides that version in the **Applications** view.

To deactivate an application version:

1. On the header, select **Dashboard** or **Applications**.
2. Select the application version you want to deactivate.
3. On the toolbar, click **PROFILE**.
4. In the **APPLICATION PROFILE** dialog box, click the **APPLICATION SETTINGS** tab.
5. In the **Version Settings** pane, click **DEACTIVATE**.
6. Click **OK** to confirm deactivation of the application version.
   If you need to, you can re-activate the version later.
7. Click **CLOSE**.

See also

Reactivating application versions

Deleting an application version

11.15.2. Reactivating application versions

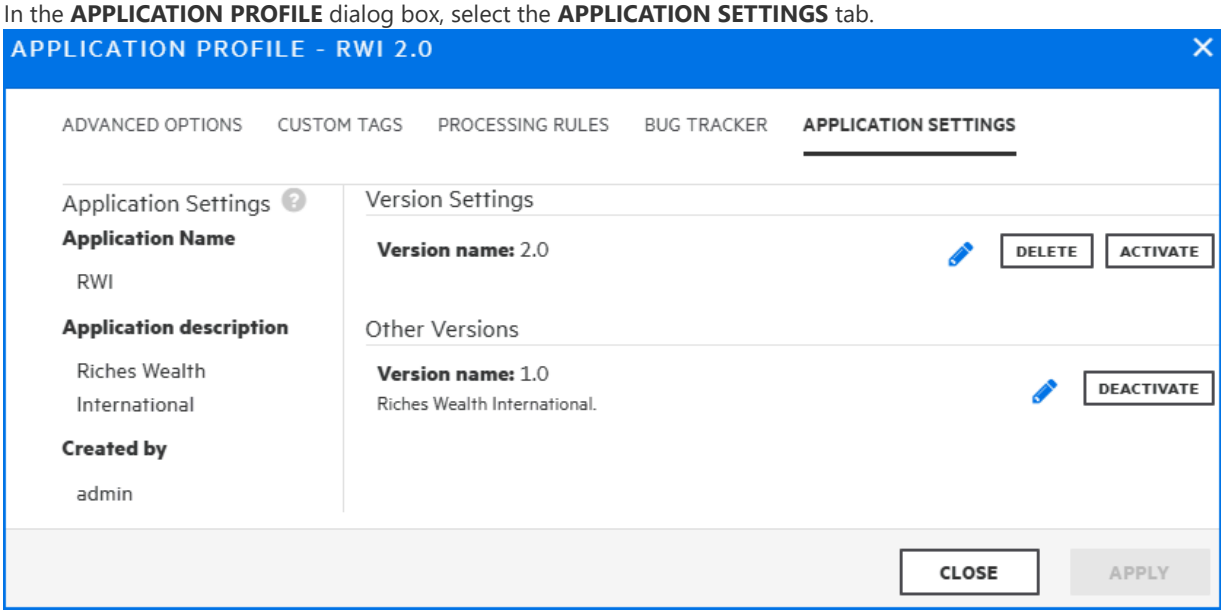
If a specific application version has been deactivated and is not listed on the **Dashboard** or the **Applications** view, you can reactivate it to make it visible again.

If the deactivated application version is the only version of the application that exists, you must first create a new version of the deactivated application, and then use the following procedure to reactivate it.

To reactivate an application version when another version of the application exists:

1. On the header, select **Applications**.
2. Under Filters, turn on the **Include inactive versions** switch (or in **Legacy View**, select the **Show inactive versions** check box).

3. Select the inactive application version.
4. On the toolbar, click **PROFILE**.
5. In the **APPLICATION PROFILE** dialog box, select the **APPLICATION SETTINGS** tab.



6. Click **ACTIVATE**.
7. To confirm the activation, click **OK**.
8. Click **CLOSE**.

The application version is again displayed on the **Dashboard** and **Applications** views.

11.15.3. Deleting an application version

If you would rather not delete an application version, but prefer instead to remove it from display on the Application Security **Dashboard** and in the **Applications** view, see Deactivating application versions

> **Important**
>
> If you delete all versions of an application, Application Security automatically deletes the application.

To delete a Application Security application version:

1. From the **Applications** view, select the application version you want to delete.
2. On the toolbar, click **PROFILE**.
3. In the **APPLICATION PROFILE** dialog box, select the **APPLICATION SETTINGS** tab.
4. In the **Version Settings** pane, click **DELETE**.
   Application Security prompts you to confirm that you want to delete the version.
5. Click **OK**.

Application Security removes the version from the database.

12. About webhooks

null

You can create webhooks to update external systems about events that occur in Application Security.

This section contains the following topics:

- Webhooks permissions
- Creating webhooks
- Editing webhooks

- Viewing webhook payloads
- Redelivering webhook payloads
- Deleting webhooks

12.1. Webhooks permissions

The following table shows which Application Security roles have permission to perform which webhook-related tasks.

Roles	Permissions
Administrator	User can create, view, and manage webhooks to monitor events.
Security Lead	• User can view webhooks. Application versions that webhooks monitor will be filtered to include only those for which the user has explicit view permission. • User can create and manage webhooks monitoring events only on entities for which the user has explicit view permission. A Security Lead cannot create or manage the following: • Webhooks with the **Send me everything!** option selected • Webhooks with the **Monitor All Application Versions** option selected • Webhooks set to monitor any events that require universal access

See also

Viewing permissions for Application Security roles

12.2. Creating webhooks

null

As an Administrator, you can create webhooks to monitor events that are either global or application version-specific. As a Security Lead, you can create webhooks that monitor events on the entities that you have permission to view.

<p autonum="Note: ">For information on which roles have which permissions to work with webhooks, see Webhooks permissions.</p>

To create a new webhook:

1. Sign in to Application Security as an Administrator or a Security Lead.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Configuration**, and then select **Webhooks**.
4. On the **Webhooks** page, click **NEW**.

5. In the **CREATE NEW WEBHOOK** dialog box, provide the information described in the following table.

Field	Description
Payload URL	Specify the URL to which you want the requested payload sent.
Description	(Optional) Provide a description of the webhook and its payload.
SSL Verification	Specify whether SSL certificate verification is required to invoke the webhook based on the specified URL.
Use SSC proxy	(Optional) If you set up a proxy for Application Security integrations, you can select this check box to use it for webhooks. For information about how to configure a proxy for Application Security integrations, see Configuring a proxy for Application Security integrations.
Content Type	Specifies the format used for the delivered payload. **Note** JSON is the only content type currently supported.
Secret	(Optional) Enter a webhook secret used to verify the data integrity and authenticity of POST requests. The secret is used to calculate a hash-based message authentication code (HMAC), which is communicated to the payload destination by way of the "X-SSC-Signature" header. The code is calculated using the HMAC-SHA256 algorithm. The secret is used as a key and the payload body (with HTTP "Date" header value appended) is used as a message. The HMAC value is then encoded as a hexadecimal number with the prefix `sha256=`.

Which events would you like to trigger this webhook?	Do one of the following: ○ To have the following events included in the payload, select **Send me everything!**. This applies to all current and future events. ○ To include a focused subset of events in the payload, select **Let me select individual events**, and then, in the **Global events** and **Application version events** lists, (described below) select the check boxes for the events to include in the payload.
	Global events (system-wide): **USER_CREATED**: A new local user, local group, or LDAP entity was added to Application Security. **USER_DELETED**: A local user, local group, or LDAP entity was deleted from Application Security. **USER_UPDATED**: A local user, local group, or LDAP entity was updated. **LOCAL_USER_ACCOUNT_LOCKED**: A local user was locked out of Application Security as a result of too many sign-in attempts with invalid credentials. **APP_VERSION_CREATED**: A new application version was created in Application Security. **APP_VERSION_DELETED**: An application version was deleted from Application Security. **REPORT_GENERATION_COMPLETE**: A new requested report is available for viewing and download. **REPORT_GENERATION_REQUESTED**: A new report was requested.
	Application version events (application version-specific): **ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS**: An uploaded artifact was successfully processed, and its data is available. **ANALYSIS_RESULT_UPLOAD_FAILURE**: An uploaded artifact was not successfully processed. **ANALYSIS_RESULT_UPLOAD_REQUIRES_APPROVAL**: An uploaded scan artifact requires approval before it can be processed. **ANALYSIS_RESULT_INDEXING_COMPLETED**: Indexing of data for global searches after Application Security finished processing an uploaded artifact was completed. **ANALYSIS_RESULT_UPLOAD_APPROVE**: An artifact was approved for uploading. **APP_VERSION_UPDATED**: An application version was updated.

Which application versions would you like to monitor?	Do one of the following: ○ To monitor all application versions (existing application versions and application versions to be created in the future), select the **Monitor all application versions** option. ○ To monitor just a subset of application versions, select the **Select individual application versions** option and then do the following: 1. Click **ADD**. 2. From the **APPLICATION** list, select an application to monitor. 3. To select all versions, select the **Select all** check box. Otherwise select the check boxes for the versions. 4. To add more application versions, repeat steps ii through iii. 5. Click **DONE**.
Active	Select this check box to make the webhook active. To leave the webhook inactive for now, leave the check box cleared.

6. Click **SAVE**.

See also

Deleting webhooks

12.3. Editing webhooks

To edit a webhook:

1. Sign in to Application Security as an Administrator or Security Lead.
2. On the header, select **Administration**.

> **Note**
> A Security Lead can only edit webhooks that monitor the entities for which you have explicit view permission.

3. On the navigation pane, expand **Configuration**, and then select **Webhooks**.
   The **Webhooks** page lists all existing webhooks.
4. Select the row to see the details for the webhook you want to edit.
5. Click **EDIT**.
6. Change any values for the fields described in Creating webhooks.
7. (Optional) To request redelivery of a payload after you finish making changes, under **Recent deliveries**, select the row for the payload you want redelivered, and then click **REDELIVER**.
8. Click **SAVE**.

See also

Viewing webhook payloads

Creating webhooks

12.4. Viewing webhook payloads

As an Administrator, you can view all webhook payloads. If you are a Security Lead, you can view only webhook payloads for application versions that you have explicit permission to view.

To view webhook payloads:

1. Sign in to Application Security as an Administrator or Security Lead.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Configuration**, and then select **Webhooks**.
   The **Webhooks** page lists all existing webhooks and their current status.
   ✓ A green check mark indicates that the last payload request was successful.
   ✗ A red x indicates that the webhook is active but could not deliver the last payload requested.

   Note
   If the **Status** column for a listed webhook displays no icon in the Webhooks table, expand its row and ensure that the **Active** check box is selected.

4. In the Webhooks table, select a webhook to expand its details and examine its recently-delivered payloads (up to ten).

   Recent deliveries

22	10/14/2020 11:29:20 AM
21	10/14/2020 11:23:47 AM
20	10/14/2020 11:23:00 AM
19	10/14/2020 11:10:29 AM
17	10/14/2020 11:09:59 AM
15	10/14/2020 11:08:40 AM
14	10/14/2020 11:08:20 AM
13	10/14/2020 10:43:17 AM
12	10/14/2020 10:18:14 AM
8	10/14/2020 10:00:39 AM

   The Recent deliveries area lists the payloads (up to ten) most recently delivered.
5. Click the row for the payload you want to examine.

6. To see header or body details for the response, select the **RESPONSE** tab.

See also

Webhook payloads

Deleting webhooks

Creating webhooks

Editing webhooks

12.5. Redelivering webhook payloads

If changes are made that affect the payload delivered to the payload URL for a webhook, you can request redelivery of the payload.

To request redelivery of a webhook payload:

1. Sign in as an Administrator or Security Lead.
2. On the header, select **Administration**.

> **Note**
> A Security Lead can only edit webhooks that monitor the entities for which you have explicit view permission.

3. On the navigation pane, expand **Configuration**, and then select **Webhooks**.
4. Select the row for the webhook for which you want a payload redelivered.
5. Under **Recent deliveries**, select the row for the payload you want redelivered, and then click **REDELIVER**.

See also

Creating webhooks

Editing webhooks

Viewing webhook payloads

12.6. Deleting webhooks

To delete a webhook:

1. Sign in as an Administrator or Security Lead.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Configuration**, and then select **Webhooks**.
4. Select the check box for the webhook you want to delete, and then click **DELETE**.

See also

Creating webhooks

Editing webhooks

13. Variables, performance indicators, and alerts

Application Security lets you store measured values and event conditions for application versions as variables. A 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. Variables and performance indicators provide the building blocks for you to create customized metrics, which you can then incorporate into customized alert definitions.

You can use the values of variables to trigger alerts, which are displayed on the dashboards of users specified as recipients in alert definitions. Application Security can also email alert notifications to members of an application version team.

This section contains the following topics:

- Creating variables
- Creating performance indicators
- Creating alerts

- Viewing and marking alerts

13.1. Creating variables

As an Administrator or a Security Lead, you can define variables for your applications.

To create a Application Security variable:

1. Sign in as an Administrator or a Security Lead, and then select **Administration**.

   > **Note**
   > Developer accounts cannot create variables.

2. On the navigation pane, under **Metrics & Tracking**, select **Variables**.
3. On the **Variables** toolbar, click **NEW**.
4. In the **CREATE NEW VARIABLE** dialog box, provide the information described in the following table.

Field	Description
Name	Type a variable name that begins with a letter (a-z, A-Z), and 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 Application Security variable search string. For information about how to construct search strings, select the **Syntax Guide** link or see Variable syntax.
Folder	From this list, select a folder from the default filter set to associate it with the variable. The **Folder** list displays 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 **SAVE**.

The **Variables** table now lists your new variable.

13.1.1. Variable syntax

The Application Security variable format is `<modifier>:<search_string>`. For example:

```
[Fortify Priority Order]:critical audited:false
```

To search for an exact match of the string, enclose the string in quotes. To search for a string without qualifications, type the string without quotes.

The following table lists the relational operators.

Relational operator	Description	Example
number range	A comma-separated pair of numbers used to specify the beginning and end of a range of numbers. Use a bracket to specify that the range includes the adjoining number. Use a parenthesis to specify that the range excludes (is greater than or less than) the adjoining number.	`(2,4]` Indicates a range of greater than two and less than or equal to four
`!` (not equal)	Negate a search string with an exclamation character (`!`).	`file:!Main.java` Returns all issues that are not in `Main.java`.

13.2. Creating performance indicators

Application Security 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 topic provides information about performance indicator syntax and instructions on how to create performance indicators.

To create a Application Security performance indicator:

1. Sign in to Application Security as a Security Lead or Administrator, and then click the **Administration** tab.

   Note
   Users who are assigned the Manager or Developer role cannot create Application Security performance indicators.

2. On the navigation pane, expand **Metrics & Tracking**, select **Performance Indicators**.
   The table to the right lists existing performance indicators.
3. Click **NEW**.
4. In the **CREATE NEW PERFORMANCE INDICATOR** dialog box, provide the information described in the following table.

Field	Description
Name	Type a performance indicator name.
Description	(Optional) Type a description of this performance indicator.
Equation	Type a valid performance indicator equation. The format for a performance indicator is as follows: `<variable><operator><variable>` where <*operator*> is a standard mathematical operator (`+`, `-`, `*`, `/`), a comparator (`==`, `>`, `<`), or the ternary operator (`?`) and <*variable*> is an existing Application Security variable.
Return Type	Select the value type to return.

5. After you configure and validate the new performance indicator, click **SAVE**.

The **Performance Indicators** table lists your new indicator.

13.3. Creating alerts

null

Alert definitions can include variables or performance indicators to determine when Application Security is to generate an alert notification in the **Todo List** pane of the Dashboard.

> **Note**
> This functionality is available only if a Application Security 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.

You can define alerts for any application versions to which you have been granted access.

To create a Application Security alert:

1. Sign in to Application Security as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Templates**, and then select **Alerts**.
   The **Alerts** page displays any defined alerts.
4. In the **Alerts** toolbar, click **NEW**.
5. In the **Name** box, type a name for the alert.
6. (Optional) In the **Description** box, type a description of the alert.
7. To create the alert without enabling it, clear the **Enable alert** check box.
8. Next to **Type**, select the type of alert you want to create.

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

9. Next to **Recipients**, do one of the following:
   - To have the alert sent only to you, leave the **Me only** option selected.
   - To have the alert sent to users assigned to application version assignees, select the **Version assignees** option.
   - (For scheduled alerts only) To have the alert sent to all Application Security users, select **All system users**.

   Regardless of the option you select, you will receive the notification.
10. Provide the information for the alert type you selected, as described in the following table.

Alert type	Instructions
Performance indicator	1. From the **Alert when** list, select a performance indicator. 2. From the list of operators, select an operator. 3. Type a numeric value. The selected performance indicator type determines whether the value represents an integer or a percentage. By default, performance indicator alerts are triggered just once, when the performance indicator value meets the criterion set for **Alert when**. For example, an alert with the trigger criterion set to Critical Exposure Issues < 50 is triggered only once, even if new critical issues are uncovered in subsequent scans. 4. To have your alert reset after each new artifact upload, select the **Reset after triggering** check box.
Variable	1. From the **Alert when** list, select a variable. 2. From the list of operators, select an operator. 3. Type a numeric value. The selected variable type determines whether the value represents an integer or a percentage. By default, variable alerts are triggered just once, when the variable value meets the criterion set for **Alert when**. For example, an alert with the trigger criterion set to `NEWIssues = 0` is triggered only once, even if new issues are uncovered in subsequent scans. 4. To have your alert reset after each new artifact upload, select the **Reset after triggering** check box.
System event	○ From the **Alert when** list, select the system event to trigger the alert.
Scheduled alert (Administrators only)	1. From the **Alert when** date box, click to open a calendar and specify the date on which Application Security is to send the alert. 2. Type the hour and minute (hh:mm) at which to send the alert. 3. Click to toggle between **AM** and **PM** to set whether the alert is sent in the morning or afternoon. 4. From the list of countries and regions, select the country or region to which your date and time settings apply. 5. From the time zone list, select the time zone to which your time and date settings apply.

11. For a performance indicator or variable alert, do the following to specify the application versions to use for the alert:
    1. Click **ADD**.
    2. In the **SELECT APPLICATION VERSION** dialog box, from the **APPLICATION** list, select an application to use for the alert.
       The **VERSIONS** pane lists the active versions of the selected application.
    3. To include inactive versions of the application in the **VERSIONS** list, select the **Show inactive** check box.
    4. To use the alert for all application versions, select the **Select all** check box. Otherwise, in the **VERSIONS** list, select the check boxes for the versions to use for the alert.
    5. To select versions of another application, repeat steps b through d.
    6. Click **DONE**.
12. In the **Message** box, type a message to inform recipients why they have received the alert.
    If you are creating a scheduled alert, message text is required.
13. Click **SAVE**.

See also

Deleting alerts

Configuring email alert notification settings

Enabling and disabling receipt of email alerts

13.3.1. Editing alerts

To edit a Application Security alert:

1. Sign in to Application Security as an Administrator.
2. On the header, select **Administration**.
3. In the pane on the left, click **Templates**, and then select **Alerts**.
   The **Alerts** page displays all alerts you have defined.
4. In the **Alerts** table, locate and select the row for the alert you want to edit.
   The row expands to reveal the alert settings.
5. Click **EDIT**.
6. Make the necessary changes and then click **SAVE**.

13.3.2. Deleting alerts

To delete a Application Security alert:

1. Sign in to Application Security as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Templates**, and then select **Alerts**.
   The **Alerts** page displays all alerts you have defined.
4. In the **Alerts** table, select the check box for the alerts you want to delete.
5. In the **Alerts** toolbar, click **DELETE**.
6. To confirm the deletion, click **OK**.

13.4. Viewing and marking alerts

Application Security flags any unread alerts that either you or another user has set up for you to receive. These alert notifications are visible on the **Todo List** in the **Dashboard** view, and on the header in every view.

To view your unread alerts, do one of the following:

- On the header, click the red circle that shows the number of unread alerts.
- On the **Dashboard** view, in the **Todo List** area, 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 for the alert name, and then click **MARK AS READ**.

To mark an alert as unread:

- In the ALERTS window, select the check box for 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 marked all of your alerts as read, the red alert notification is no longer displayed. To see these alerts, go to the **Dashboard** view and, in the **Todo List** area, click the **Show all alert notifications** link.

14. Working with scan artifacts

The following sections describe the aspects of working with scan artifacts.

- Uploading scan artifacts
- Viewing scan artifact details
- Downloading analysis results
- Approving analysis results for an application version
- Viewing issue metadata
- Mapping analysis results to external lists
- Purging scan artifacts
- Deleting artifacts

14.1. Uploading scan artifacts

The following procedure describes how to upload your scan artifacts to the Application Security database. For information about how to submit training metadata to Fortify Audit Assistant, see Submitting training data to Fortify Audit Assistant.



Note

As it adds data to the database, Application Security truncates HTTP responses that contain more than 100,000 characters. Such responses are either cut off at the end, or contain `\n\n...\n\n` elsewhere in the response. This does not affect downloaded scans. It affects only the data displayed on the Application Security **AUDIT** page.



Important

The files you upload to Application Security must not exceed 2 GB.



Important

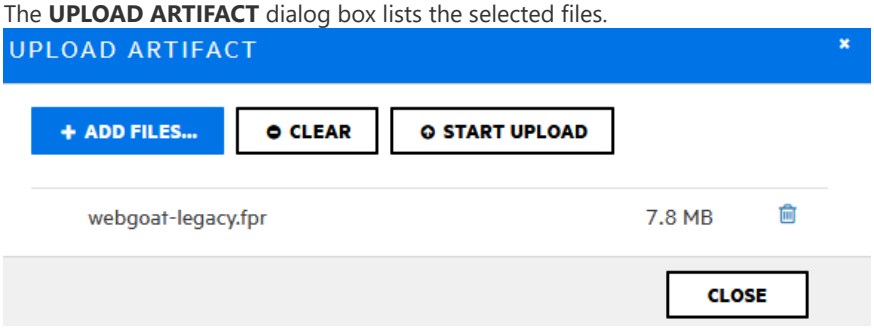
To upload third-party artifacts, you must have the correct parser configured. For information, see Adding and managing parser plugins.

To upload a scan artifact to the Application Security database:

1. On the header, select **Dashboard** or **Applications**.
2. Select the application version for which you want to upload an artifact, and then select the **Artifacts** page.

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

3. Click **ARTIFACT**.
4. In the **UPLOAD ARTIFACT** dialog box, click **+ ADD FILES**.
5. Select one or more (up to five) artifact files to upload.
   If the OpenText Fortify SCA or Sonatype third-party parser is enabled, you can select the artifact type from a list.
   The **UPLOAD ARTIFACT** dialog box lists the selected files.



6. To remove a file from the list, click the **Delete** button for that file.
   To remove all of the listed files, click **CLEAR**.
7. Click **START UPLOAD**.
   The dialog box displays a progress bar as each file is uploaded.
8. After your files are successfully uploaded, click **CLOSE**.

> **Note**
> If a scan artifact requires approval based on analysis result processing rules, it must be approved before processing. For information, see Approving analysis results for an application version.

Viewing file processing errors

If there was an error in processing an uploaded artifact, the **Status** column of the **ARTIFACT HISTORY** table displays **Error Processing**, along with a circled number that indicates the number of processing rules violated.

To view information about the processing rules violated:

- Click the circled number.

The **Artifact Processing Messages** box opens to display details about problems encountered during the upload.

See also

Downloading scan artifacts

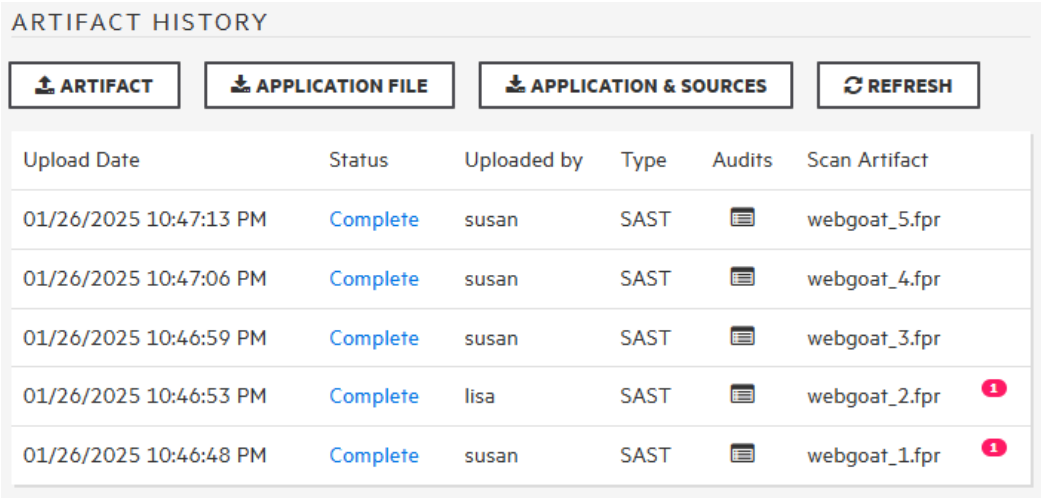
Setting analysis results processing rules for application versions

Uploading FPR files

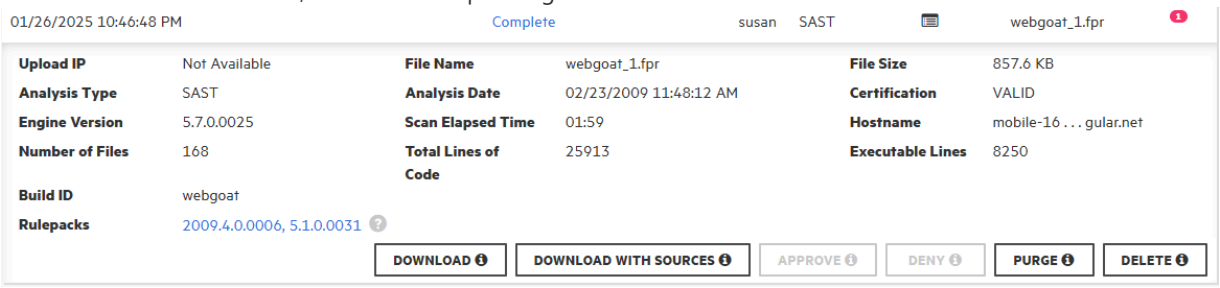
14.2. Viewing scan artifact details

To view the details available for uploaded scan artifacts:

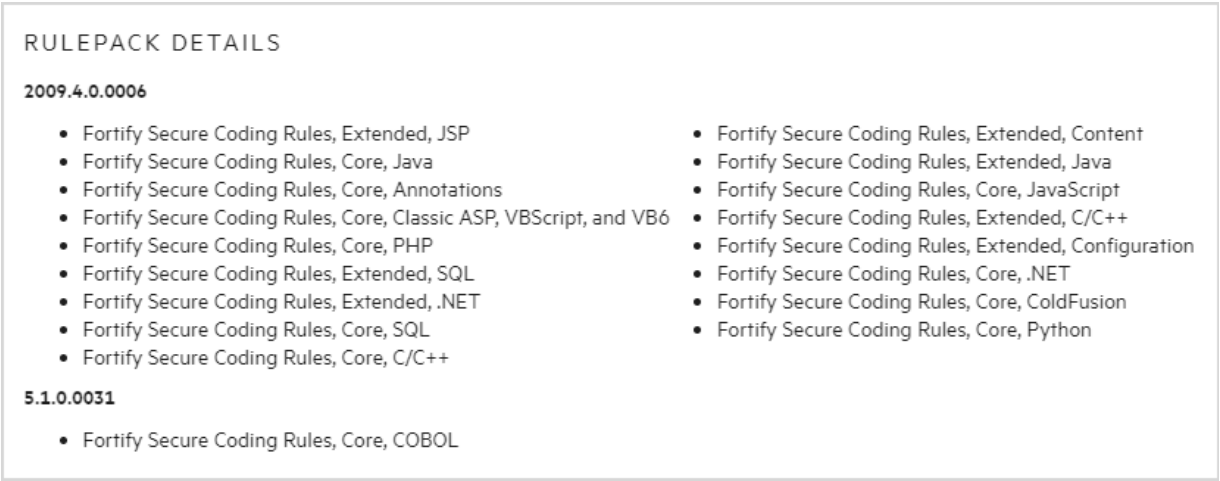
1. On the header, select **Dashboard** or **Application**.
2. Select the application version for which you want to view artifact details, and then select the **Artifacts** page.
   The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the application version.



3. To view details for an artifact, click the corresponding row.



   The details shown include the analysis engine version, number of files and lines of code scanned, the analysis date, and more.
   If an error occurred in processing the uploaded artifact, the **Status** column of the **ARTIFACT HISTORY** table displays **Error Processing**. A number on the right indicates the number of processing rules violated.
4. To view the lines of code associated with any processing errors for the scan, click the circled number (1).
   The **SCAN WARNINGS** box displays the line of code where processing rules were violated, along with a description of the violation.
5. To view a list of the coding rules applied during the scan, grouped by the Rulepack version, click the **Rulepacks** version link.



If a scan artifact requires approval based on analysis result processing rules, it must be approved before processing. For information, see Approving analysis results for an application version.

See also

Uploading scan artifacts

Downloading scan artifacts

Purging scan artifacts

Setting analysis results processing rules for application versions

Uploading FPR files

14.3. Downloading analysis results

You can download the latest merged FPR file for an application version, or you can download FPR files that result from individual scans. Open the analysis results in Fortify Audit Workbench by double-clicking the downloaded FPR file.

Downloading the merged FPR file for an application version

To download the latest merged analysis results for an application version in FPR format:

1. On the header, select **Dashboard** or **Applications**.
2. Select an application version or click to expand the row for the application and then select a version.
3. Select **ARTIFACTS**.
   The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the application version.
4. Do one of the following:
   - To download the latest merged analysis results for an application version, at the top of the **ARTIFACT HISTORY** table, click **APPLICATION FILE**.
   - To download the current merged analysis results for an application with sources, at the top of the **ARTIFACT HISTORY** table, click **APPLICATION & SOURCES**.

Downloading individual analysis results

To download results for a given processed scan:

1. On the header, select **Dashboard** or **Applications**.
2. Select an application version or click to expand the row for the application and then select a version.
3. Select **ARTIFACTS**.
   The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the application version.
4. Click the row for the artifact you want to download to expand it and see the artifact details.
5. To download the artifact, click **DOWNLOAD**.

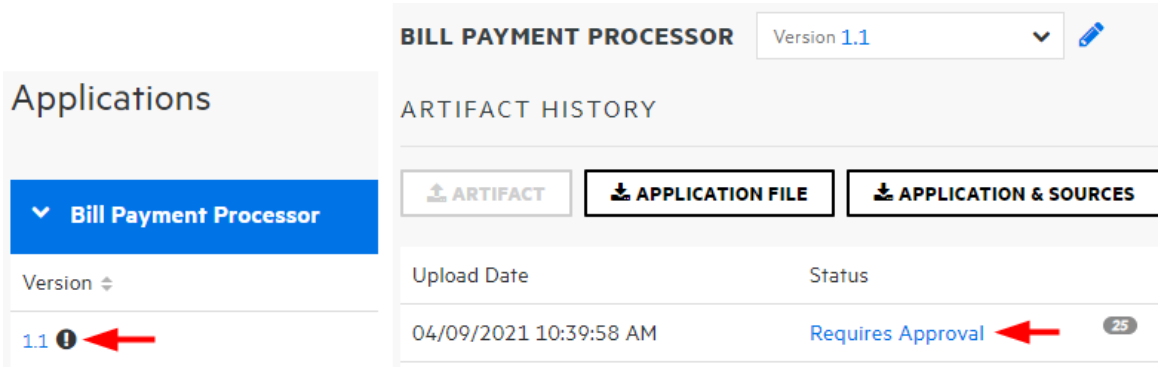
See also

Uploading scan artifacts

Deleting artifacts

14.4. Approving analysis results for an application version

Depending on the processing rules configured for an application version, and whether the Rulepack used to process a scan was outdated (older than the server Rulepacks), analysis results might require approval. (See Setting analysis results processing rules for application versions.) If analysis results require approval, this is indicated by an alert icon (!) next to the version name in the **Applications** view and by the **Requires Approval** value in the **Status** column of the **ARTIFACT HISTORY** table.



Note

If an artifact was uploaded by mistake or you do not want Application Security to process the artifact, see Denying processing approval.

To approve analysis results for an application version so that Application Security can process the artifact:

1. On the header, select **Dashboard** or **Applications**.
2. Select an application version, and then select **Artifacts**.
   The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the selected application version.
3. Click a row with the value **Requires Approval** in the **Status** column.
4. Click **APPROVE**.
   The **Processing Messages** section shows an explanation of what, specifically, triggered the approval requirement.
5. In the **Approval Comment** box, type a comment to indicate why you are approving these analysis results.
6. Click **APPROVE**.

Application Security proceeds to process the artifact.

Denying processing approval

If an artifact was uploaded by mistake or, for some other reason, you do not want Application Security to process the artifact, you can either delete it, or, if you want to retain a record of the artifact upload, you can deny approval.

To deny approval of an artifact:

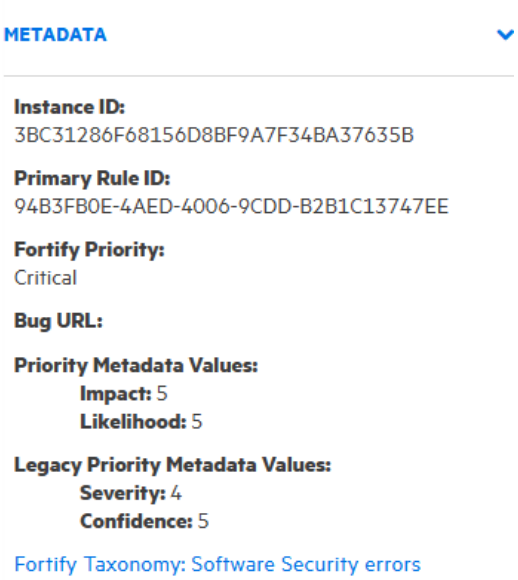
1. On the header, select **Dashboard** or **Applications**.
2. Select an application version, and then select **Artifacts**.
   The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the selected application version.
3. Expand the row for the artifact that requires approval, and which you do not want Application Security to process.
4. Click **DENY**.
   The **Processing Messages** area lists explanations of what, specifically, triggered the approval requirement.
5. In the **Comment** box, type a comment to indicate why you want to deny approval of these results.
6. Click **DENY**.

The **Status** value for the artifact changes to **Approval Denied**.

14.5. Viewing issue metadata

To view metadata for an issue:

1. Open 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. Click the **INFO** tab, and then click to expand **METADATA**.



The metadata information includes the unique issue identifier (Instance ID), the unique identifier for the rule that generated the issue (Primary Rule ID), the bug URL (if applicable), priority metadata values, and legacy priority metadata values.

> **Note**
> The instance ID displayed is unique to the specific application version and is not associated with any other application versions.

5. To go to the website that provides detailed information about software security errors, click the **Fortify Taxonomy: Software Security errors** link.

14.6. Mapping analysis results to external lists

OpenText distributes an external metadata document with Rulepacks. This document includes mappings from the Fortify categories to alternative categories (such as OWASP Top Ten 2010, PCI, or CWE). Security leads can create their own files to map issues to different taxonomies, such as internal application security standards or additional compliance obligations. For detailed information about how to create custom mappings, see the *OpenText™ Static Application Security Testing Custom Rules Guide*.

To apply the modified or new external metadata document across all applications, you must first import it into Application Security.

To import a new or modified external metadata document into Application Security:

1. Sign in as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, under **Metrics &Tracking**, select **Rulepacks**.
4. On the **Rulepacks** page, click **IMPORT**.
5. In the **IMPORT RULEPACK** dialog box, click **+ ADD FILES**.
6. Find and select your document, and then click **START UPLOAD**.

If you are conducting a collaborative audit between Application Security and Fortify Audit Workbench, you can import the changed mapping document to Application Security, and then open the FPR file in Fortify Audit Workbench to see how the mapping works with the analysis results.

14.7. Purging scan artifacts

Purging an artifact recovers space from the Application Security 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 Customer Support first to determine whether an artifact purge will affect them.
- Purging removes *all* artifacts that have the same or earlier analysis date.

You can purge an artifact if it meets *all* of the following conditions:

- It has not already been purged.
- It does not contain just one scan generated from a given analysis engine type. For example, if only one OpenText Fortify SAST-generated artifact exists for an application version, you cannot purge it. If two artifacts from the same analysis engine were uploaded for the application version, you can purge only the older of the two artifacts.
- Its status is one of the following:
  - PROCESS_COMPLETE
  - ERROR_PURGING
  - ERROR_DELETING

You cannot purge an artifact if:

- It is being processed.
- An error occurred during processing.
- It contains the latest scan for the analysis engine type.

To purge a scan artifact from the Application Security database:

1. On the header, select **Dashboard** or **Applications**.
2. Select the application version with artifacts that you want to purge, and then select **Artifacts**.
   The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the application version.
3. Click the row that displays the artifact you want to purge from the database.
   The table expands to show the details of the selected artifact.
    <<Old Analysis Type and missing DENY button>>
4. Click **PURGE**.
5. To confirm purging the artifact, click **OK**.

See also

Deleting artifacts

14.8. Deleting artifacts

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

> **Note**
>
> You cannot delete an artifact that is being processed or one that has already been purged.

To delete a scan artifact from the Application Security database:

1. On the header, select **Dashboard** or **Applications**.
2. Select the application version with artifacts that you want to delete, and then select **Artifacts**.
   The **ARTIFACT HISTORY** table lists all scan artifacts uploaded for the application version.
3. Click the row that displays the scan artifact you want to delete.
   The table expands to show the details of the selected artifact.

4. Click **DELETE**.
5. To confirm deletion of the artifact, click **OK**.

See also

Purging scan artifacts

15. Working with Aviator auto-remediation results

You can use OpenText™ Application Security Aviator for Vulnerability Remediation to automatically remediate your code using AI-assisted code fixes for vulnerabilities detected during a static scan.

OpenText™ Application Security Aviator for Vulnerability Remediation leverages Large Language Model (LLM) to audit static scan results, identify vulnerabilities, and provide auto-remediation suggestions. The results from OpenText™ Application Security Aviator for Vulnerability Remediation are stored as audit information in Application Security.

This section describes how Application Security receives, stores, and provides the OpenText™ Application Security Aviator for Vulnerability Remediation auto-remediation results that are included in uploaded FPR files. The AI-assisted auto-remediation results can be viewed in Application Security audits and retrieved by IDE plugins such as VS Code, Visual Studio, IntelliJ, and Eclipse. This enables users to use the auto-remediation results and fix their source code quickly and accurately with minimal manual intervention.

Applying or pushing code fixes to repositories directly from Application Security is not supported.

Receiving auto-remediation data

Auto-remediation data is produced after OpenText™ Application Security Aviator for Vulnerability Remediation analyzes vulnerabilities in uploaded FPR files. The auto-remediation data, `remediations.xml`, is included in the FPR file.

`remediations.xml` file is included when:

- OpenText™ Application Security Aviator for Vulnerability Remediation runs against a scan already known to Application Security
- An FPR with auto-remediation results is uploaded directly to Application Security (through FCLI, IDE, or manual upload)

This release version supports uploading FPR with auto-remediation results to Application Security. For uploading FPRs, see Uploading scan artifacts.

Application Security automatically detects and processes the `remediations.xml` during FPR consumption.

Viewing auto-remediation data in Application Security

Auto-remediation data is visible when reviewing an issue in Application Security. Depending on the configuration, the data appear as:

- A dedicated auto-remediation field
- A comment or recommendation section within the issue details

This allows users to review AI-assisted recommendations without leaving Application Security.

Retrieving auto-remediation data using the REST API

IDE plugins can retrieve auto-remediation data for a specific issue using the following REST API endpoint.

- `/projectVersions/{parentId}/remediations`
- `/projectVersions/{parentId}/remediations/{id}`

This endpoint returns the remediation details stored by Application Security. The returned data is the same remediation information that Application Security received from the FPR file.

See also

Configuring Aviator

Uploading scan artifacts

Downloading analysis results

16. Collaborative auditing

When an analysis engine (analyzer such as OpenText Fortify SAST) 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 is considered a vulnerability without direct developer confirmation.

Issue audits, whether performed in Application Security, Fortify Audit Workbench, or by Fortify 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

Application Security uses issue templates to categorize and display issues.
This section provides an overview of the auditing process and instructions on how to display and use the auditing interface. This information assumes that you know how to create and configure application versions. For information about applications and application versions, see Applications and application versions.

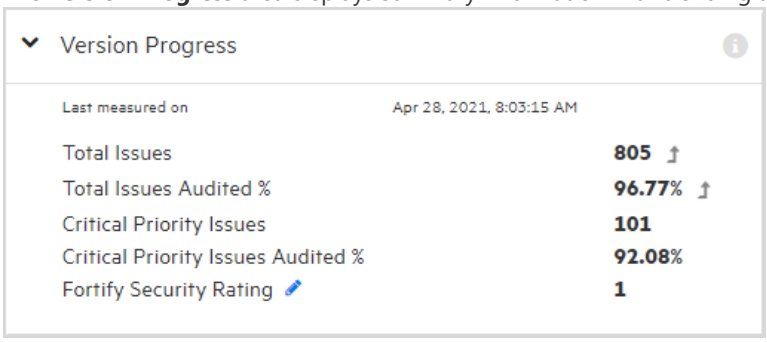
This section contains the following topics:

- Viewing high-level summary metrics for an application version
- About current issues state
- Viewing information about issues to audit
- Filtering issues for display
- Searching issues
- Searching globally
- Auditing analysis results
- Using Fortify Audit Assistant with Application Security
- Exporting open source data
- Integrating Application Security with Fortify WebInspect Enterprise
- Viewing open source data
- Downloading an OpenText Core SCA (Debricked) software bill of materials

16.1. Viewing high-level summary metrics for an application version

To view high-level summary results for an application version:

1. On the header, select **Dashboard** or **Applications**.
2. Select the application version you are interested in, and then select **Overview**.
3. On the **OVERVIEW** page, if the pane on the right is collapsed, expand it.
   The **Version Progress** area displays summary information with trending arrows.



4. To display a metric other than **Fortify Security Rating**, click the **Edit** button, and then select a different metric to display from the list.

<img data-zoom="true"
src="file/images/general/fssc/SSC_Project/ssc_project_resources_imagesVer_progress_1.png" style="width: 518px;height: 411px; border: none !important;"/>

See also

Viewing summary metrics for application versions

16.2. About current issues state

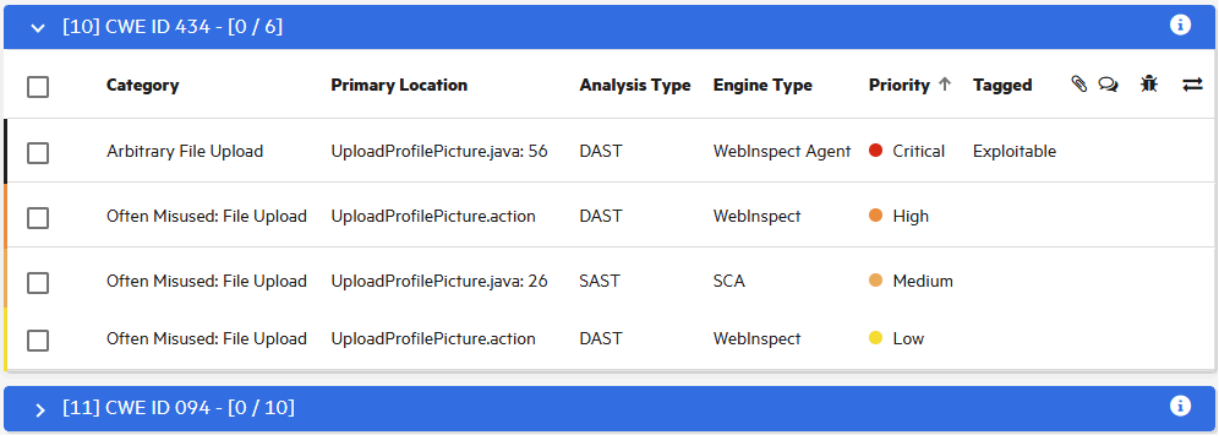
Application Security keeps track of the analysis engine that uncovers each issue in an application version and merges any new information into the existing body of results for the application version. After new audit information is uploaded to the server or entered on the **AUDIT** page, Application Security merges that information into any existing audit information for a given issue. Application Security also marks an issue as *removed* after the analysis engine no longer finds the issue.

Whenever new analysis results are uploaded, Application Security checks every issue to determine if it was uncovered in a previous scan.

16.3. Viewing information about issues to audit

To display the issues you want to audit:

1. Upload analysis results for the application version you want to audit (see Uploading scan artifacts).
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.
   For more information, see Filtering issues for display and Viewing issues based on folders.
   <img data-zoom="true"
   src="file/images/general/fssc/SSC_Project/ssc_project_resources_imagesPetWeb_Grouping.png" style="width: 548px;height: 202px; border: none !important;"/>
4. In the issues table, if you have selected a grouping, expand a group to view the issues it contains.



The following table describes the columns in the issues table. To sort listed issues, click a column heading (note that you cannot sort the **Contains attachment** (), **Contains comments** (), or **Bug submitted** () columns).

Column	Description
Category	Displays the category of issue uncovered (sort is alphanumeric)
Primary Location	Shows the file scanned and line of code on which the issue was detected (sort is alphanumeric)
Analysis Type	Displays the type of analysis performed on the code
Engine Type	Displays the analysis engine used to perform the scan
Priority	Shows the relative threat the issue represents (sort is from high to low or low to high priority)
Tagged	Displays the primary custom tag value applied to the issue if any
 Contains attachment	Indicates whether any attachments are associated with the issue
 Contains comments	Indicates whether any comments were added to the issue
 Bug submitted	Indicates whether any defects were submitted against the issue
 Has correlated issues	Indicates that static and dynamic results for the issue are correlated. If they are, the issue is listed twice in the table, once for each analysis type. If either a subsequent static scan or dynamic scan shows an issue was fixed, the correlation icon is removed. (Sort displays correlated issues first or last.)

See also

Auditing analysis results

16.3.1. Viewing issues based on folders

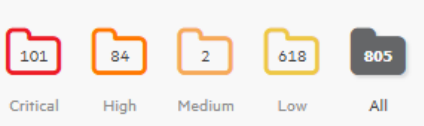
The **OVERVIEW** and **AUDIT** pages include **Critical**, **High**, **Medium**, **Low**, and **All** links, which you can use to view issues based on their assignment to a Fortify folder. By default, the folders correspond to Fortify priority values (and the potential risk they pose to the enterprise), However, the folders displayed can include any custom folders created in and added to a filter set (and then an issue template) from Fortify Audit Workbench (see the *OpenText™ Fortify Audit Workbench User Guide*).

Note

When you edit or create filter sets and folders in Fortify Audit Workbench, be aware that the search modifiers used by Fortify Audit Workbench and Application Security might not match. Not all searches, filters, or folders based on search expressions produce the same results. In addition, if your search expression contains external metadata categories such as OWASP or CWE, your results might not match because the expressions might differ on Application Security and Fortify Audit Workbench. When there are multiple matched external categories, Application Security matches any of them, but Fortify Audit Workbench expects an exact match of all external categories. If you encounter this issue when editing or creating issue templates for use in Application Security, contact Customer Support for assistance.

To view issues from the **OVERVIEW** page based on Fortify folder assignment:

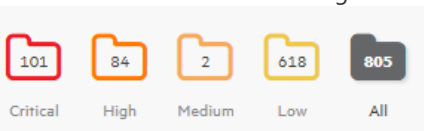
1. From the **Dashboard** or **Applications** view, select the application version of interest, and then select **Overview**. The **OVERVIEW** page for the application version opens. To the left of the **Group by** and **Filter by** lists, the total number of issues in their respective folders is displayed. By default, all issues are shown. If you select attributes to filter by, the numbers displayed for the folders change accordingly.
2. To see the number of issues in a folder that have been reviewed, point to the folder.

   The number of reviewed issues is shown first, followed by the total number of issues. For example, **High - [79 / 84]** indicates that 79 of 84 total high priority issues were reviewed.
3. To view issue charts on the **OVERVIEW** page based on an assigned folder, select the folder.

To view issues from the **AUDIT** page based on the Fortify folder assignment:

1. On the **Dashboard**, point to the version of the application of interest, and then select **Audit**.
   The **AUDIT** page for the application version opens. Below the search box, the total number of issues in their respective folders is displayed. By default, all issues are shown. If you select attributes to filter by, the numbers displayed for the folders change accordingly.
2. To see the number of issues assigned to a given folder that have been reviewed, point to the folder.

   The number of reviewed issues is on the left, and the total number of issues is on the right. For example, **High - [79 / 84]** indicates 79 of 84 total high priority issues were reviewed.
3. To list issues on the **AUDIT** page based on folder assignment, select the folder.

See also

Filtering issues for display on the OVRVIEW and AUDIT pages

16.3.2. Viewing issues assigned to you

To view all issues assigned to you:

1. On the header, select **Applications**.
2. Under **Filters**, turn on the **My assigned issues** switch (or in **Legacy View**,select the **My assigned issues** check box). The **Applications** view lists the application versions that have issues assigned to you.

See also

Setting issue viewing preferences

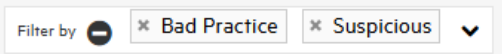
16.4. Filtering issues for display

The following instructions describe how to filter issues for display for an application version from either the **OVERVIEW** page or from the **AUDIT** page.

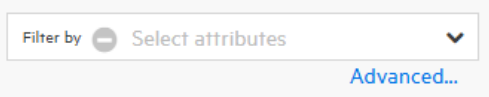
> **Note**
>
> You can also select a filter set to change the issues displayed on the **OVERVIEW** and **AUDIT** pages. For information and instructions, see Changing displayed issues using filter sets.

To filter issues for display on the **OVERVIEW** or **AUDIT** page:

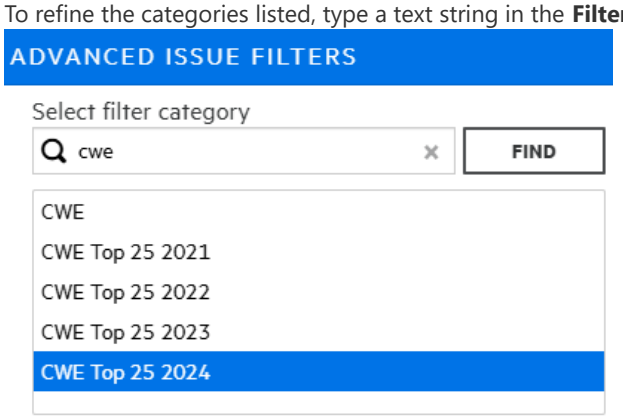
1. From the **Group by** list, select an attribute to use to group the issues in the issues table.
   To remove the selected attribute, click the **Clear all** button .
2. From the **Filter by** list, select the attributes to use to filter the issues for display in the issues table.
   You can select multiple attributes from this list. You must select attributes one at a time.

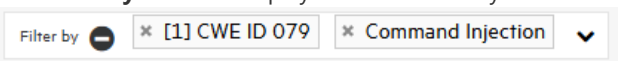
   To remove a selected attribute, click the **x** next to its name. To remove all selected attributes, click the **Clear all** button .
3. To filter issues based on values for a custom tag other than **Analysis**, or based on risks related to OWASP, CWE, or other security threat classifications:
   1. Click the **Advanced** link.

   2. In the **ADVANCED ISSUE FILTERS** dialog box, from the **Select filter category** list, select a category.
      To refine the categories listed, type a text string in the **Filter categories** box, and then click **FIND**.

      The **Select filters** list is populated with the filters available for the selected category.
   3. To refine the **Select filters** list further, type a text string in the **Filter options** box, and then click **FIND**.
      The **Select filters** list displays the filters that contain the matching text.
      To see the complete list of filters again, click the **x** in the **Filter options** box.
   4. In the **Select filters** list, click each of the filters you want to filter by.
      Each filter you select is added to the **Selected filters** list.
   5. To add filters for another filter category, repeat steps b through d.
   6. Click **APPLY**.
      The **Filter by** box now displays all of the filters you have selected.

4. To remove a filter, click the **x** for the filter.
5. To clear all **Group by**, **Filter by**, and advanced filter selections, click the **Clear all** button .

See also

Auditing correlated issues

Searching issues

Viewing issues based on folders

Searching globally

16.5. 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. From the **Dashboard** or **Applications** view, select the application version of interest.
   The **Audit** page is displayed for the selected application version.
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	Searches for a range of numbers using the standard mathematical interval notation of parentheses and/or brackets to indicate whether the endpoints are excluded or included, respectively Example: `(2,4]` indicates greater than two and less than or equal to four
not equal	Excludes issues specified by the string when you precede the string with the 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. The syntax for using a modifier is `<modifier>:<search_term>` .
A search string can contain multiple modifiers and search terms. If you specify more than one modifier, Application Security 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**.
4. To return to the complete issues list, clear the text in the search box.

See also

Search modifiers

Filtering issues for display on the OVERVIEW and AUDIT pages

Search query examples

Searching globally

16.5.1. Search modifiers

You can use a search modifier to specify to which issue attribute the search term applies. To use a modifier that contains a space in the name, such as the name of the custom tag, you must enclose the modifier in brackets. For example, to search for issues that are new, enter `[issue age]:new`.

A search that is not qualified by a modifier matches the search query 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.

The following examples describe using the search with and without applying a search modifier:

- To apply the search to all modifiers, enter a string such as `control flow`. This searches all modifiers and returns any result that any results that contain the "control flow" 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 detected by the Control Flow Analyzer.

The following table describes the search modifiers. A few modifiers have a shortened name indicated in parentheses. You can use either modifier string.

Modifier	Description
analysis	Searches for issues that have the specified audit analysis value such as exploitable, not an issue, and so on.
[analysis type]	Searches for issues based on the analyzer product.
analyzer	Searches the issues for the specified analyzer such as control flow, data flow, structural, and so on.
audience	Searches for issues by intended audience. Valid values are targeted, medium, and broad. **Note** This metadata is legacy information that is no longer used and will be removed in a future release. OpenText recommends that you do not use this search modifier.
audited	Searches the issues to find true if the primary custom tag is set and false if the primary custom tag is not set. The default primary tag is the Analysis tag.
category (cat)	Searches for the given category or category substring.
comments (comment, com)	Searches for issues that contain the search term in the comments added to the issue.
commentuser	Searches for issues with comments from the specified user.
confidence (con)	Searches for issues that have the specified confidence value. OpenText Fortify SAST calculates the confidence value based on the number of assumptions made in code analysis. The more assumptions made, the lower the confidence value.

`<custom_tagname>`	Searches for issues based on the value of the specified custom tag. To search for a specific date in a date-type custom tag, specify the date in the format: yyyy-mm-dd. To search for issues that have no value set for a custom tag, use `<none>` for the search term. For example, to search for all issues that have no value set in the custom date-type tag labeled Target Date, type: `[Target Date]:<none>`
`[engine priority]`	Searches for issues based on the original priority value determined by the engine that identified the issue.
`file`	Searches for issues where the primary location or sink node function call occurs in the specified file.
`[fortify priority order]`	Searches for issues that have a priority level that matches the specified priority. Valid values are `critical`, `high`, `medium`, and `low`.
`historyuser`	Searches for issues that have audit data modified by the specified user.
`[issue age]`	Searches for the issue age, which is `new`, `updated`, `reintroduced`, or `removed`.
`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 ten <year>]`, `[CWE top 25 <version>]`, `[stig <version>]`, and `[pci ssf <version>]`, and others.
`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 sink and [source context].
primaryrule (rule)	Searches for all issues related to the specified sink rule.
sink	Searches for issues that have the specified sink function name. Also see [primary context].
source	Searches for dataflow issues that have the specified source function name. Also see [source context].
[source context]	Searches for dataflow issues that have the source function call contained in the specified code context Also see source and [primary context].
sourcefile	Searches for dataflow issues with the source function call that the specified file contains. Also see file.
status	Searches issues that have the status reviewed, not reviewed, or under review.
suppressed	Searches for suppressed issues.
taint	Searches for issues that have the specified taint flag.

For examples of search queries that use modifiers, see Search query examples.

See also

Searching issues

16.5.2. Search query examples

The following table contains search query examples.

Search query exaomples

Search target	Query
All privacy violations in file names that contain `jsp` with `getSSN()` as a source	`category:"privacy violation" source:getssn file:jsp`
All file names that contain `com/test/123`	`file:com/test/123`
All issues that contain `cleanse` as part of any modifier	`cleanse`
All audited issues that have the `[my tag]` assigned and set to `P1`	`[my tag]:P1`
All suppressed vulnerabilities with `asdf` in the comments	`suppressed:true comments:asdf`
All categories except for SQL Injection	`category:!SQL Injection`
All issues in file names that contain either `java` or `jsp`	`file:java OR file:jsp`
All issues in file names that contain `java` and that occur on line number 12	`file:java AND line:12`
All issues that have a value specified for a custom tag labeled `version`	`version:!<none>`

See also

Searching issues

Search modifiers

16.6. Searching globally

Regardless of the view you have open, you have access to the global **Search** box on the header. Any search string you type here is applied across all application versions, issues, reports, comments, and users.



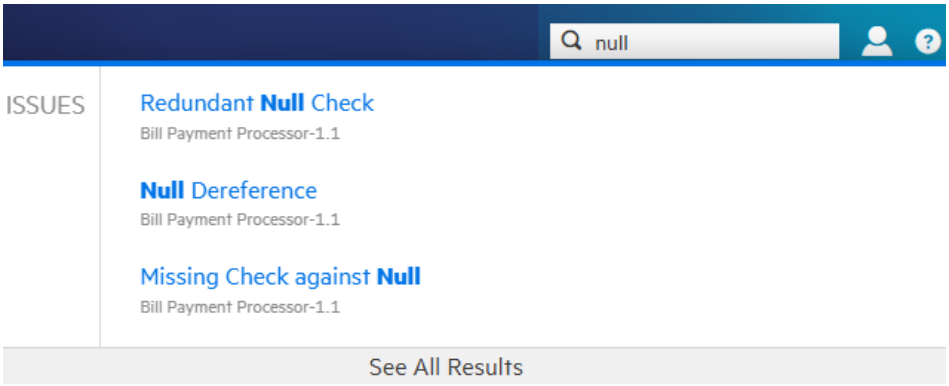
Note

The search box is visible only if **Enable global search** was selected during Application Security setup. For more information, see Configuring Application Security for the first time.

To use the global **Search** box:

1. From any view, type a search string into the **Search** box.
   Application Security displays the first several items that match your search string, grouped by category. The application version is also displayed.
2. To go to a specific item listed, click the item.
3. To see a list of all search results, below the listed items, click **See All Results**.

Example: Finding issues



After you select an issue from the listed results, Application Security takes you to the corresponding version page with the issue expanded to full view.

If you select **See All Results**, Application Security 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 results.

Note

The search results for issues might include removed, hidden or suppressed issues. If the **AUDIT** page does not display an item you selected, check the viewing preferences set for the application version to ensure that you have the appropriate settings enabled to display removed, hidden, and suppressed issues. For instructions, see Setting issue viewing preferences.

Example: Finding users After you select a single user from the listed results, assuming you have the required permission, <meta class="data-nv" data-nv="SSC_Short" data-nv-value="Fortify Software Security Center" data-productid="2174" data-replace-parent="false" data-version="25.2"/> takes you to the details for the user account in the Administration view.

See also

Searching applications and application versions from the Applications view

16.7. Auditing analysis results

The following procedure describes how to audit analysis results from the **AUDIT** tab. If you are working with open source results, you can audit the analysis results from either the **AUDIT** or the **OPEN SOURCE** page.

To display the issues you want to audit:

1. Upload analysis results for the application version you want to audit.
   For instructions, see Uploading scan artifacts.
2. Open the **AUDIT** page for the application version.

   The table in the **AUDIT** page lists issues based on their assigned folders (by default, critical to low).
3. To selectively display the issues you want to audit, apply filters to the issues list.
   For more information, see Filtering issues for display and Viewing issues based on folders.
4. In the issues table, if you have selected an attribute to group by, expand a group to view the issues it contains.

To audit an issue:

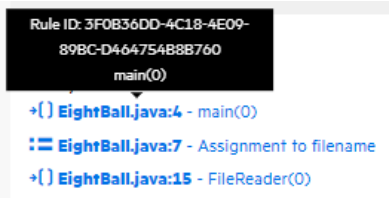
1. To expand an issue and view its details, click its row in the table.

For information about viewing OpenText Fortify DAST results, see Viewing OpenText Fortify DAST scan results in Application Security.

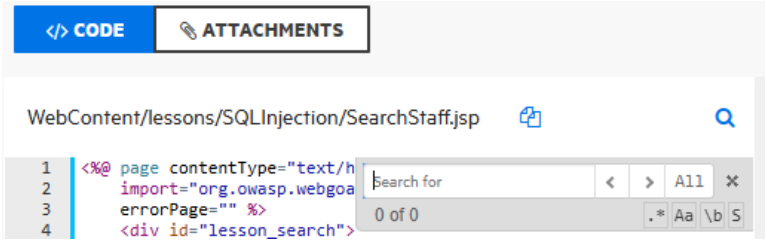
> **Tip**
> To view the details for the issue in a new browser window, click the **Open in a new tab** button. To copy the issue link so that you can easily access it later, click the **Copy issue link to clipboard** button.

The **CODE** tab displays the path the tainted data has taken in the source code associated with the issue.

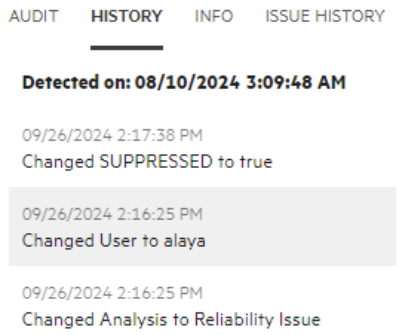
2. To view summary details about a step along the course that tainted data has taken, under **Analysis Trace**, point to that step.



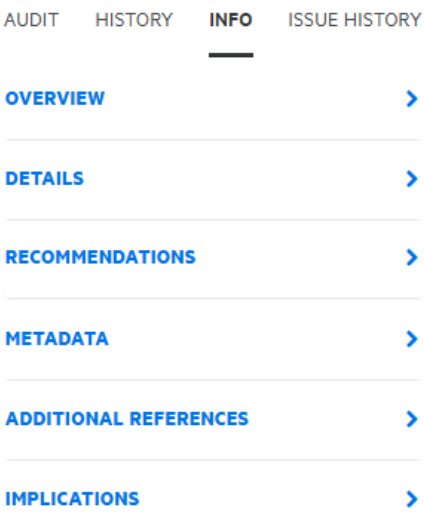
3. To view code associated with a step, click the step under **Analysis Trace**.
   The corresponding line of code is highlighted on the **CODE** tab.
4. To search for a specific string in the code associated with the issue:
   1. On the **CODE** tab, click the search button.
   2. In the **Search for** box, type a search string.



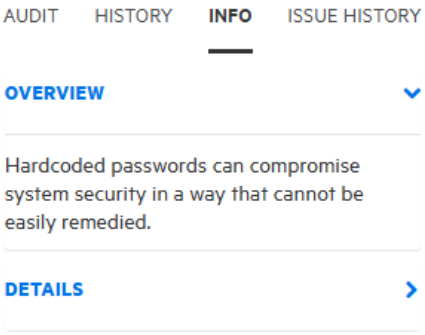
   Use the **Next** and **Previous** buttons to move through the search results.
5. To view any audit history available for the issue, in the right pane, select the **HISTORY** tab.



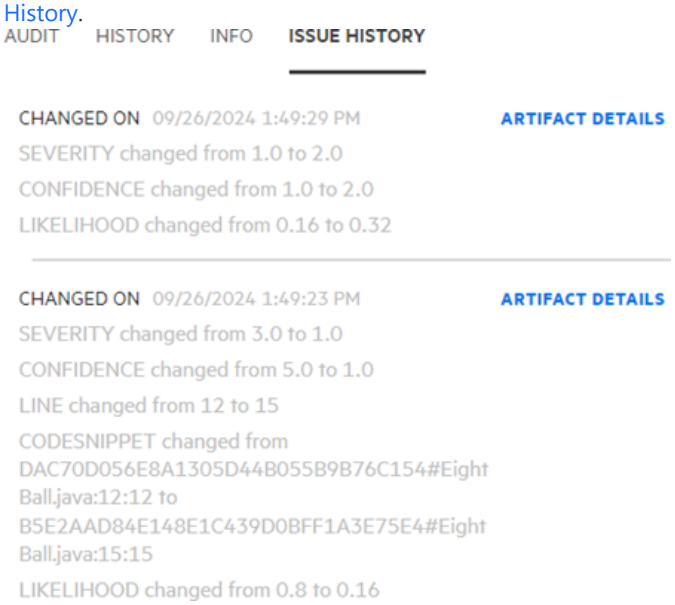
6. To view an overview of the issue, details about the finding, recommendations for remediation, issue metadata, references to additional resources, and implications for your application version, in the right pane, select the **INFO** tab.



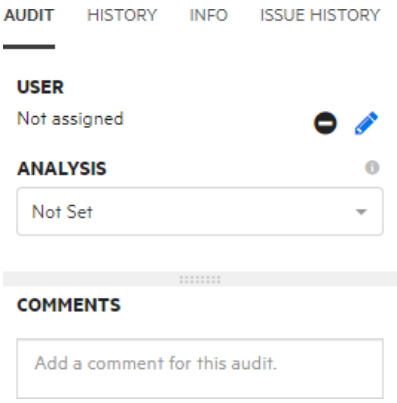
7. To expand a row and view a category of information, click the corresponding arrow (›).



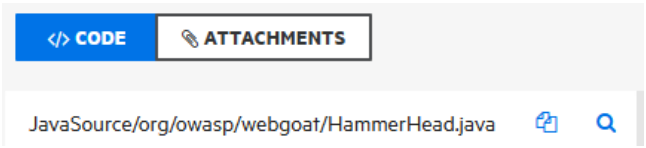
8. To view attribute changes for an issue as you upload new scans for an audit, select the **ISSUE HISTORY** tab. Click **ARTIFACT DETAILS** to view the list of artifacts from the scan history. For more information, see Audit Issue History.



9. When you have enough information to start your audit, select the **AUDIT** tab.



10. (Optional) To exclude an issue from display because you know it is fixed or it is not of immediate concern, click **SUPPRESS**.
11. (Optional) If your Administrator has configured application security training, 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 <meta class="data-nv" data-nv="SSC_Short" data-nv-value="Fortify Software Security Center" data-productid="2174" data-replace-parent="false" data-version="25.2"/>. Click OK.
    The application security training website opens in a new browser tab that displays training content based on the category, subcategory, and language of the selected issue.
12. To attach a file to the issue:
    1. Click **ATTACHMENTS**.

    2. Click **CLICK HERE TO ADD**.
    3. In the **UPLOAD ATTACHMENT** dialog box, click **BROWSE**, and then select the file you want to upload.
       Supported file formats are TXT, LOG, DOC, DOCX, PDF, PPT, PPTX, JPG, JPEG, BMP, PNG, TIFF, GIF, ZIP, GZIP, TAR, and 7ZIP. (Documents in XML format are not supported.) <<this is in the UI and the doc is out of date anyway>>

       Note
       The file size must not exceed 3 MB.

    4. (Optional) In the **Description** box, type a description of the file.
    5. Click **SAVE**.
       If you attached an image file, Application Security displays a preview of the image on the right, under **Image Preview**.

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

13. Click **CODE**, and then select the **AUDIT** tab.
14. To assign a user to the issue:
    1. Under **USER**, click the **Edit assigned user** button .

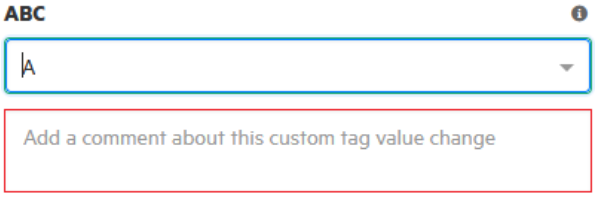
    2. To locate a user to assign to the issue from the **SELECT USER** dialog box, in the **Find user** box, type part or all of a user's name, and then click **FIND**.

3. In the list of returned names, click the name of the user to assign to the issue.
4. Click **DONE**.
    << Style: need acceptable user names>>

> **Note**
> To remove the assigned user, click the **Unassign User** button. Alternatively, to change the assigned user to a different user, select the **Edit assigned user** button and select the preferred user.

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

15. From the **Analysis** list (or other defined primary custom tag), select a value that reflects your assessment of this issue.
    If you do not provide a value, Application Security treats the issue as unaudited.
16. If additional custom tags are associated with the application version, specify the values for those tags.
    If your Administrator specified that a comment is required for a custom tag you assign, then you must type a comment in the box outlined in red, which appears under the custom tag box.



> **Note**
> If Fortify Audit Assistant assessed the issues, the additional tags **AA_Prediction**, **AA_Confidence**, and **AA_Training** are displayed. For information about how to use these fields, see Reviewing Fortify Audit Assistant results.

17. In the **COMMENTS** box, type a comment about this issue audit.
18. Click **SAVE**.

See also

Auditing correlated issues

Auditing a batch of issues

About Fortify Audit Assistant

Audit Issue History

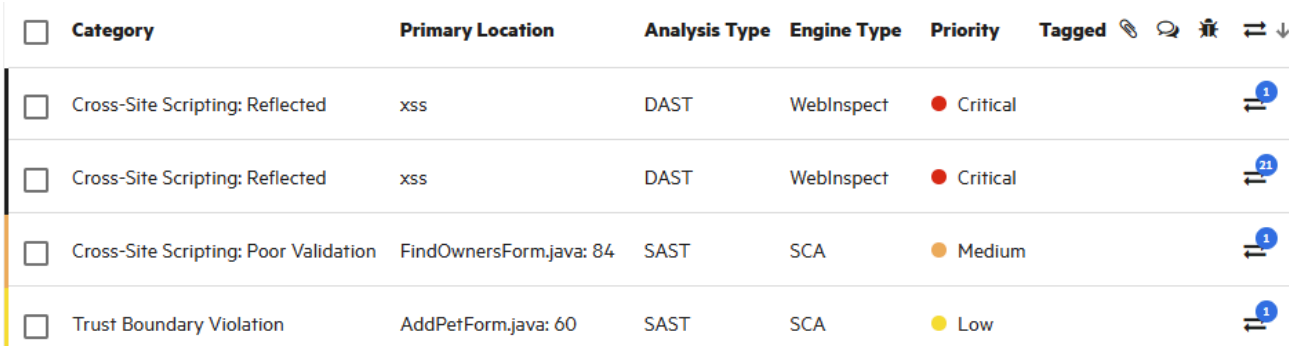
Configuring application security training.

16.7.1. Auditing correlated issues

If the artifacts uploaded for the application version include results from both static (OpenText Fortify SAST) and dynamic (OpenText Fortify DAST) analysis, some issues might be correlated with one another.

If an issue is correlated with one or more other issues uncovered using a different analysis type, the **Has correlated issues** button is displayed, along with the number of correlated issues that either target or originate from the selected issue.

To list issues that are correlated with other issues, click the **Has correlated issues** column header .

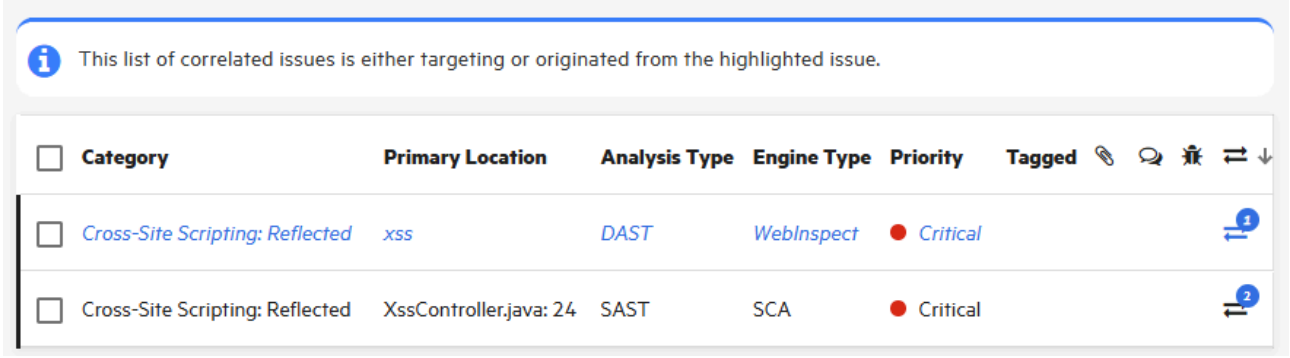


Category	Primary Location	Analysis Type	Engine Type	Priority	Tagged
Cross-Site Scripting: Reflected	xss	DAST	WebInspect	Critical	
Cross-Site Scripting: Reflected	xss	DAST	WebInspect	Critical	
Cross-Site Scripting: Poor Validation	FindOwnersForm.java: 84	SAST	SCA	Medium	
Trust Boundary Violation	AddPetForm.java: 60	SAST	SCA	Low	

The number shown in the blue circle indicates how many issues are correlated with an issue.

To list the correlated issue or issues:

- Click the circle or the **Has correlated issues** ⇄ button.



You can audit the listed issues as described in Auditing scan results.

Note

If, following an audit, a developer fixes the root problem uncovered in one issue, the remaining correlated issues might also be fixed.

To return to the complete issues table, to the right of the **Filter by** list, click **CLEAR ALL**.

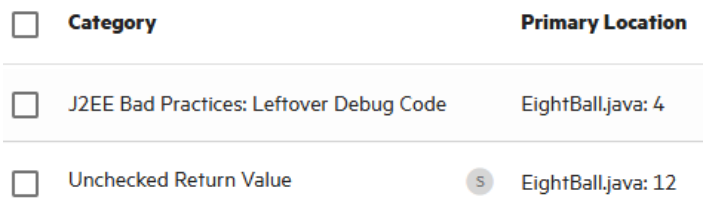
16.7.2. About suppressed, removed, and hidden issues

You can control whether the issues pane lists suppressed, removed, and hidden issues.

Suppressed issues

As you assess successive scans of an application version, you might want to completely *suppress* some exposed issues. It is useful to mark an issue as suppressed if you are sure that the specific vulnerability is not, and will never be, an issue of concern. You might also want to suppress warnings for specific types of issues that might not be high priority or of immediate concern. For example, you can suppress issues that are fixed, or issues that you plan not to fix.

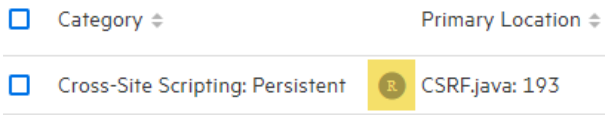
Suppressed issues are not included in the **Total Issues** value shown in the **Version Progress** section of the expandable pane of the **OVERVIEW** page. Suppressed issues are also not included in the calculation of application version metrics. For information about how to suppress an issue, see Auditing scan results.



Category	Primary Location
J2EE Bad Practices: Leftover Debug Code	EightBall.java: 4
Unchecked Return Value	EightBall.java: 12

Removed issues

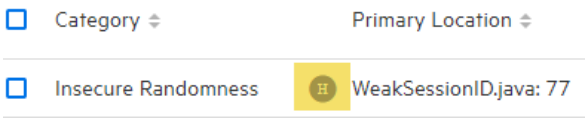
As multiple scans are run on an application over time, issues are often remediated or become obsolete. As Application Security merges analysis results, it marks issues that were uncovered in a previous scan, but are no longer evident in the most recent analysis results as *Removed*.



Removed issues are not included in the **Total Issues** value shown in the **Version Progress** section of the expandable pane on the OVERVIEW page.

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.



See also

Setting issue viewing preferences

16.7.2.1. Setting issue viewing preferences

You can set certain viewing preferences for individual application versions.

Viewing suppressed issues

To view the suppressed issues associated with an application version:

1. From the **Dashboard** or **Applications** view, select the version for the application you are interested in.
   Application Security opens the **AUDIT** page for the selected version.
2. On the toolbar, click **PROFILE**.
   The **APPLICATION PROFILE** dialog opens to the **ADVANCED OPTIONS** tab.
   Below the check boxes, the **Issue counts by state, based on current selections** shows the number of hidden, suppressed, and removed issues in the database associated with the selected application version.

   Note
   The filter set you select does not affect the number of suppressed issues shown. For example, if a suppressed issue is hidden in the selected filter set, it is still included in the count of suppressed issues.
3. Select the **Show suppressed issues** check box.
4. Click **APPLY**, and then click **CLOSE**.

   The **AUDIT** page displays all removed issues. Each removed issue is tagged with an **S** in the **Primary Location** column.

Viewing removed issues

When Application Security merges uploaded analysis results, it removes issues that were uncovered in the previous analysis but are no longer evident in the most recent results.

To view the issues that were removed for an application version:

1. From the **Dashboard** or **Applications** view, select the version name for the application version you are interested in.
   Application Security opens the **AUDIT** page for the selected version.
2. On the toolbar, click **PROFILE**.
   The **APPLICATION PROFILE** dialog box opens to the **ADVANCED OPTIONS** tab.

Below the check boxes, the **Issue counts by state, based on current selections** shows the number of hidden, suppressed, and removed issues in the database associated with the selected application version.

> **Note**
> The filter set you have selected does not affect the number of removed issues shown. For example, if a suppressed issue is hidden in the selected filter set, it is still included in the count of removed issues.

3. Select the **Show removed issues** check box.
4. Click **APPLY**, and then click **CLOSE**.

The **AUDIT** page displays all removed issues. Each removed issue is tagged with an **R** in the **Primary Location** column.

Viewing hidden issues

In Application Security, 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:

To reveal any hidden issues associated with an application version:

1. From the **Dashboard** or **Applications** view, select the version for the application version you are interested in. Application Security opens the **AUDIT** page for the selected version.
2. On the toolbar, click **PROFILE**.
   The **APPLICATION PROFILE** dialog box opens to the **ADVANCED OPTIONS** tab.
   Below the check boxes, the **Issue counts by state, based on current selections** shows the number of hidden, suppressed, and removed issues in the database associated with the selected application version.
3. Select the **Show hidden issues** check box.
4. Click **APPLY**, and then click **CLOSE**.

The **AUDIT** page displays all hidden issues. Each hidden issue is tagged with an **H** in the **Primary Location** column.

16.7.3. Changing displayed issues using filter sets

Filter sets enable you to change the display of application version issues on the **OVERVIEW**, **AUDIT**, and **OPEN SOURCE** pages. The filter sets that are listed depend on the issue template assigned to the application version. Three filter sets are included in the issue templates that OpenText provides. However, you can use other issue templates that have different filter set names and filter conditions.

Application Security provides the following filter sets:

- Quick View
  The Quick View filter set provides a view of issues in the Critical folder (these have a potentially high impact and a high likelihood of occurring) and the High folder (these have a potentially high impact and a low likelihood of occurring). This filter set provides a useful first look at results that enables you to quickly address the most pressing issues.
- Security Auditor View
  This view reveals a broad set of security issues to be audited. The Security Auditor View filter contains no visibility filters, so all issues are shown.
- PCI Auditor View
  This view is defined for individuals responsible for auditing an application with respect to its compliance with Payment Card Industry Security Standards.

16.7.4. Overriding assigned issue priority

When analysis results are parsed and loaded into Application Security, the scan parser for each supported engine type assigns a priority value to each issue. However, this priority value does not reflect the full context of the affected code or application. Other factors that concern the use of the affected code might justify assigning a different priority. For example, a vulnerability assigned the "critical" priority value might be better classified as "medium" or "low" priority if the section of code in question is never invoked in the application, or if the application is intended for use exclusively by a small department and has no connections to other applications and systems, so the identified vulnerability would have a low

likelihood of being exploited. To enable such a use case, Application Security provides the capability for trusted users to change the priority originally assigned to an issue. Such priority changes are reflected in generated reports.



Caution

Use of this feature must be considered as a long-term change in that it affects generated reports, computed metrics, and so on, depending on the data in the system. Ensure that, before you use it, you discuss the planned change with your security lead.

Enabling the priority override capability

You can enable priority overrides on your system either during a new deployment or on an existing Application Security instance.

To enable the priority override capability:

1. On the navigation pane of the **Administration** view, expand **Configuration**, and then select **Issue Audit**.
2. Select the **Enable Priority Override** check box.
3. Click **SAVE**.
4. Restart the server.

After server restart, the feature is enabled and is applied to all application versions. On the **AUDIT** page, the issue details (**AUDIT** tab) now includes the **PRIORITY OVERRIDE** list tag.

To enable your users to make use of this functionality, create a new user role for them that includes the "Edit restricted custom tag values" permission. Grant these roles only to trusted users who have the knowledge and diligence to accurately assess issue priority. For information about how to create a user role, see Creating custom roles.



Note

Any user roles with permission to edit restricted custom tag values can override issue priority. The system-defined Security Lead role can edit restricted custom tags.

To turn off the priority override capability:

1. On the navigation pane of the **Administration** view, expand **Configuration**, and then select **Issue Audit**.
2. Clear the **Enable priority override** check box.
3. Click **SAVE**.
4. Restart the server.

After server restart, the feature is disabled system-wide, and the **PRIORITY OVERRIDE** list tag is no longer visible in the issue details.

Overriding priority values during an audit

To override the priority value for an issue during an audit:

1. On the **AUDIT** page, expand the row that contains the issue.
2. On the **AUDIT** tab in the right pane, from the **PRIORITY OVERRIDE** list, select the preferred priority value.
3. (Required) In the box outlined in red below the list, type a comment to explain why you changed the value.

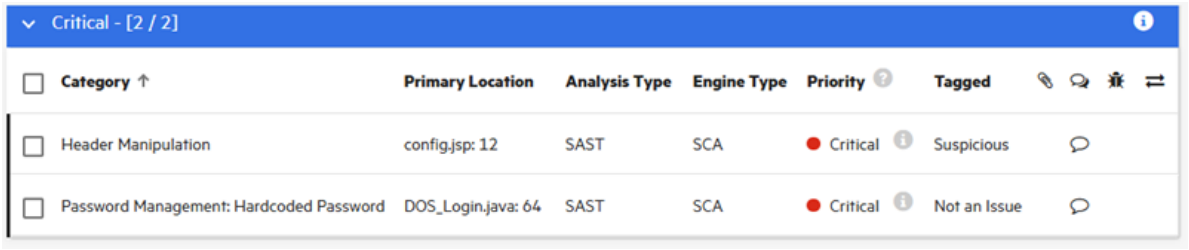
   Note

   If you want to undo the override *before* you save the audit, click **UNDO**.

4. To save the new priority value and associated comments, click **SAVE**.

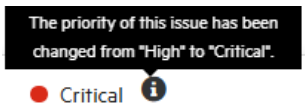
Viewing issues that have changed priority values

To view issues that have priority values that you and others have manually assigned, from the **Group by** list, select **Priority Override**.



The issues table lists issues with overridden priorities, grouped by the priority override tag value. Issues with unchanged priority values are grouped under **Not Set**.

To see how the **Priority** value was changed, point to the information icon.

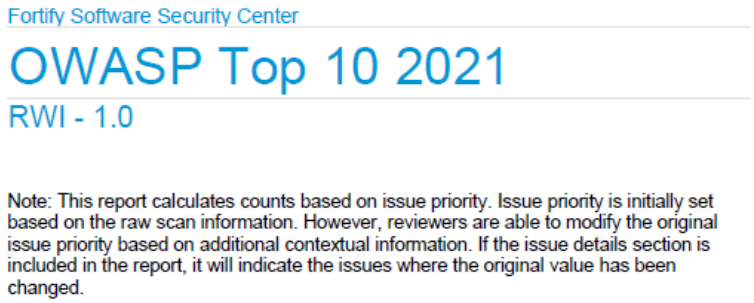


Viewing priority override information in issue reports

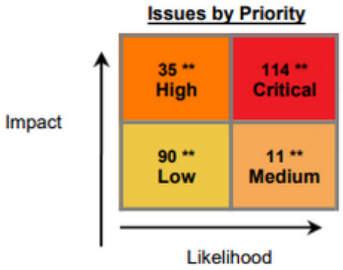
If the priority override tag was used in auditing an application version, you can include the information in the issue reports you generate.

To include priority override information in a new issue report, as you specify the parameters for the report, leave the **Detailed Report** and **Categories by Fortify Priority** check boxes selected.

If an issue report includes issues that have overridden priority values (and have **Detailed Report** and **Categories by Fortify Priority** options selected), a note to that effect is displayed on the cover page, as shown here:



If the priority override feature is used, and the **Detailed Report** and **Categories by Priority** parameters are selected (either manually or by default), the **Issues by Priority** cube in the **Executive Summary** displays a double asterisk where issues have changed priority values.



The **Issue Details** sections of these reports show the current priority values, along with the original priority values.

Path Manipulation *Remediation Effort(Hrs): 0.5*	Low Original: Critical

Package: com.order.splc		
Location	**Analysis Info**	**Analyzer**
WEB-INF/src/java/com/order/splc/ConnFactory.java:20 Priority Override: Low Analysis: Not an Issue	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** ConnFactory() **Source:** java.lang.System.getProperty() **from** com.order.splc.ConnFactory.ConnFactory() **In** WEB-INF/src/java/com/order/splc/ConnFactory.java:16	SCA
WEB-INF/src/java/com/order/splc/ConnectionFactory.java:30 Priority Override: Low Analysis: Not an Issue	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** ConnectionFactory() **Source:** java.lang.System.getProperty() **from** com.order.splc.ConnectionFactory.ConnectionFactory() **In** WEB-INF/src/java/com/order/splc/ConnectionFactory.java:26	SCA

Reverting to original priority values

If you overrode the original priority value for an issue, and saved it, but you now want to revert the priority value to its original value:

1. On the **AUDIT** page, expand the row that contains the issue.
2. To the right of the **PRIORITY OVERRIDE** list tag, click the revert button .
3. (Required) In the box outlined in red below the list, type a comment to explain why you changed the value.
4. To save the new priority value and associated comments, click **SAVE**.

Reports reflect the current effective priority value, whether that is the original priority set by the engine (if unmodified) or the overridden value. If a user changed the priority value, those reports show the changed value. If not, the reports show the original priority.

16.7.5. Viewing bugs submitted for issues

The issues table on the **AUDIT** page includes a **Bug submitted** column that shows whether a bug has been submitted against a listed issue.

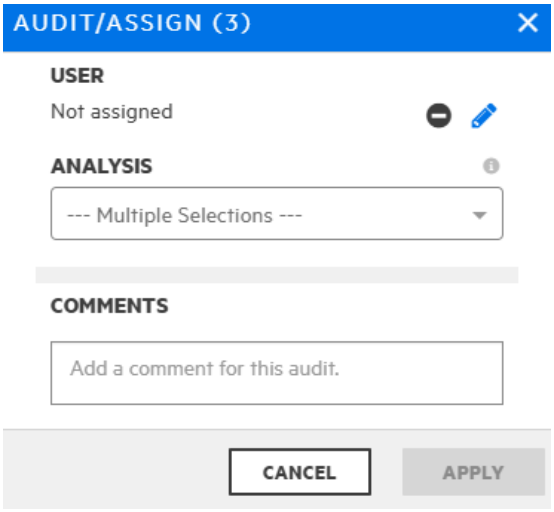
To view the bug, click the **VIEW BUG** icon , and log in to the assigned bug tracking application.

> **Tip**
>
> To view a bug, you must use a browser supported by the bug tracker application.

16.7.6. Auditing a batch of issues

To audit multiple issues at a time for an application version:

1. In the **Applications** view, open the **AUDIT** page for the application version.
2. In the issues list, select all of the check boxes for the issues you want to include in the batch audit.
3. Click **AUDIT**.



4. To assign a user to the selected issues:
    1. Select the **Edit assigned user** button .
    2. To find a user account, in the **Find user** box, type part or all of a user's name, and then click **FIND**.
    3. In the list of returned names, click the name of the user to assign.
    4. Click **DONE**.
       The **USER** section now displays the selected user name and avatar (if available).
5. From the **ANALYSIS** list (or other defined primary custom tag), select a value that reflects your assessment of this batch of issues.
6. If additional custom tags are associated with the application version, specify the values for those tags.

> **Note**
> If Fortify Audit Assistant assessed the issues, the additional tags **AA_Prediction**, **AA_Confidence**, and **AA_Training** are displayed. For information about how to use these fields, see Reviewing Fortify Audit Assistant results.

7. (Optional) In the **COMMENTS** box, type a comment about this issue audit.
8. Click **APPLY**.

See also

Auditing Scan Results

16.8. Using Fortify Audit Assistant with Application Security

With the launch of Fortify Audit Assistant version 23.2.0, OpenText introduced a new Fortify Audit Assistant engine. The second generation (G2) engine has a much-improved prediction engine and greater harmonization with training data provided by the decisions your team makes when assessing vulnerabilities. The results you receive are more accurate and relevant to the applications in your environment.

This section provides information on how you can best take advantage of the power and precision of the Fortify Audit Assistant G2 engine.

> **Note**
> If you have not updated Application Security to version 23.2.0 (or later), you can continue to use the previous Fortify Audit Assistant (G1). After you upgrade, the G1 version of Fortify Audit Assistant is no longer supported. Users who have installed the off-cloud version of Fortify Audit Assistant also must upgrade to the G2 version if they intend to use it with Application Security version 23.2.0 or later.

16.8.1. Consistent use of tags

Fortify Audit Assistant uses two tags when making its predictions: FALSE POSITIVE and EXPLOITABLE.

To make the best use of Fortify Audit Assistant:

- Map your tags to Fortify Audit Assistant tags
  Map the tag you use to identify vulnerabilities that can be exploited to the Fortify Audit Assistant EXPLOITABLE tag and the tag you use to label vulnerabilities that are not an issue to the Fortify Audit Assistant FALSE POSITIVE tag. Otherwise, Fortify Audit Assistant uses the global model which is based on decisions made by OpenText Fortify on Demand auditors. If your tags are mapped to the Fortify Audit Assistant tags, decisions your auditors make are used in conjunction with the global model, enabling you to enhance your results by taking into consideration decisions that align with your software environment and decision process.
- Consistently tag vulnerabilities
  To get the most out of Fortify Audit Assistant, your auditors must consistently use the tags you have mapped to Fortify Audit Assistant.

For more information, see Mapping Fortify Audit Assistant analysis tag values to Application Security custom tag values.

16.8.2. Mapping Fortify Audit Assistant analysis tag values to Application Security custom tag values

To use Fortify Audit Assistant with Application Security, you must map Fortify Audit Assistant analysis tag values to Application Security list-type custom tag values. You can map the Fortify Audit Assistant analysis tag values to the **Analysis** custom tag that is installed with Application Security and is required to identify a vulnerability as audited, or you can choose a different list-type custom tag for this purpose.

If you selected the **Enable auto-apply** check box when configuring Fortify Audit Assistant, you can also tell Fortify Audit Assistant which Fortify Audit Assistant analysis tag values to automatically apply to the list-type custom tag values.

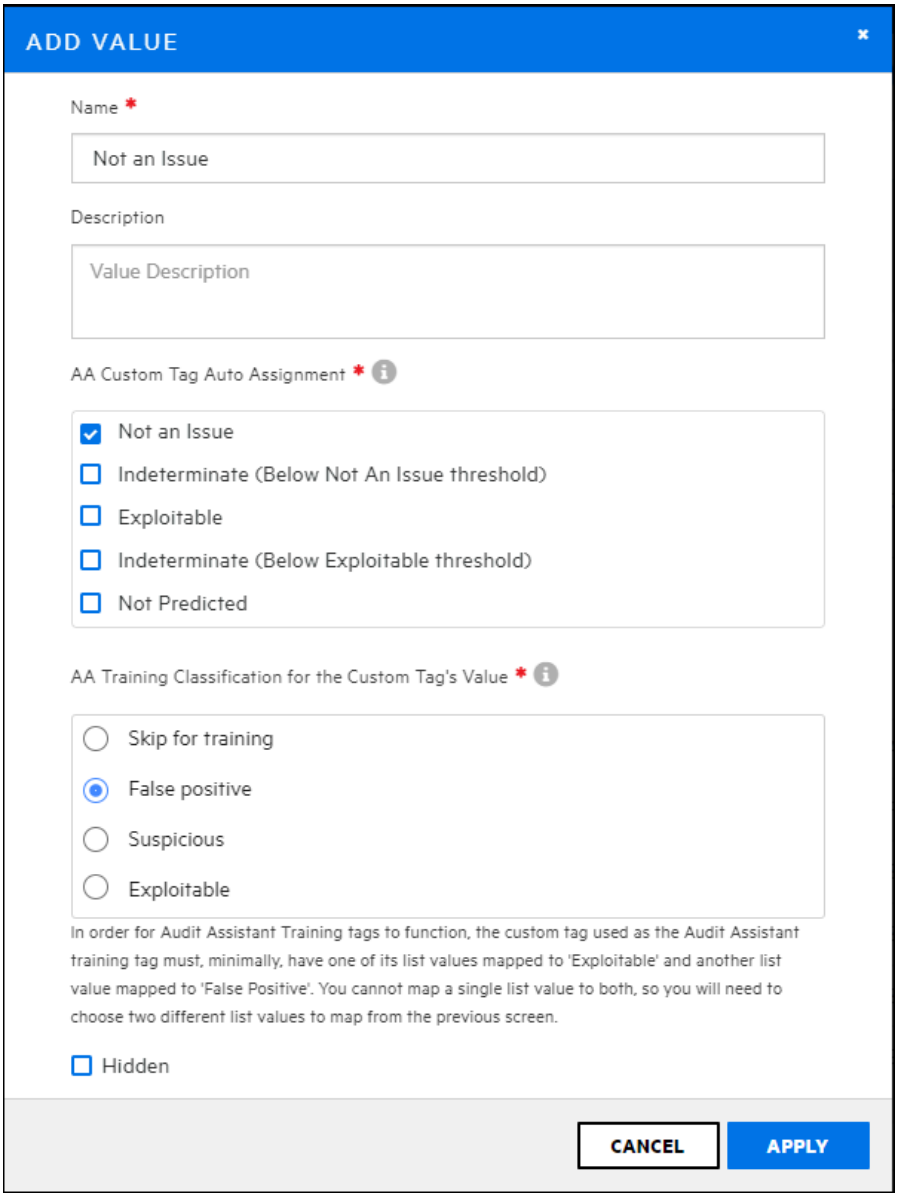


Note

If you have not created your custom tag values yet, see Adding custom tag values for instructions on how to create the values and map them to Fortify Audit Assistant. If you are using the default **Analysis** custom tag or a custom tag you have already created, continue with these instructions. Ensure to create tags or use **Analysis** custom tag first.

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

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then click **Custom Tags**.
3. Click the row for the custom tag you want to edit.
   The row expands to display the details for the tag.
4. Click **EDIT**.
5. In the **List Values** table, click the **EDIT value** button for a value.
   The **ADD VALUE** dialog box opens.



If Application Security is configured to use Fortify Audit Assistant and auto-apply is enabled, the ADD VALUE dialog has an **AA Custom Tag Auto Assignment** area and an **AA Training Classification for the Custom Tag's Value** area.

6. If the new value aligns with a Fortify Audit Assistant prediction value in the **AA Custom Tag Auto Assignment** area, select its check box to automatically map the list value to the selected prediction value.
   This enables automated auditing for all application versions where you have enabled it.
7. In the **AA Training Classification for the Custom Tag's Value** area, select the option to be used when training the Fortify Audit Assistant model.
   For Fortify Audit Assistant Training tags to function, you must map at least two list values to Audit Assistant Training tags. One must be mapped to the False positive Fortify Audit Assistant Training tag and another list value must be mapped to the Exploitable Fortify Audit Assistant Training tag.
8. Repeat steps 5 through 7 to map additional list values.
9. Click **APPLY** and then click **SAVE**.

See also

Adding custom tag values

16.8.3. About setting prediction policies

To use Fortify Audit Assistant to make predictions about your analysis results, you must first define at least one *prediction policy*. A prediction policy establishes confidence thresholds for its predictions. There are two confidence thresholds to set:

- False Positive
- Exploitable

The default confidence thresholds are set at 80%, but you can set them between 0 and 100%, in 10 percent increments. An increase in the confidence thresholds increases the confidence in your results and reduces the number of results to just those that meet or exceed the threshold set. By adjusting the thresholds, you can fine tune the prediction policy to your software environment.

Although you can adjust these values, OpenText suggests that you use the default settings for a while before adjusting them. As you use Fortify Audit Assistant, the training data you provide will positively impact your results and you might find that the results of your initial scans dramatically improve.

A prediction is not made if the minimum confidence threshold is not met. Confidence levels beneath the confidence thresholds are indeterminate—Fortify Audit Assistant cannot provide an assessment based on the set confidence level.



Note

During Fortify Audit Assistant configuration, an Administrator selects a default global prediction policy, which it uses for an application version if no prediction policy is specified for that application version. If a prediction policy is specified for an application version, then Fortify Audit Assistant uses that policy to assess issues.

After you assess the impact of training on your results, you can adjust the thresholds if you find you are receiving too much noise. The higher you set a threshold, the more confidence Fortify Audit Assistant has in its predictions. This results in fewer hits as only those vulnerabilities that meet or exceed the confidence threshold level are identified as False Positive or Exploitable.

For detailed instructions on how to define prediction policies in Fortify Audit Assistant, see the Fortify Audit Assistant Help in the Fortify Audit Assistant Documentation.

See also

Configuring Fortify Audit Assistant options for an application version

Configuring Fortify Audit Assistant

About Fortify Audit Assistant auto-prediction

16.8.4. Fortify Audit Assistant workflow

The workflow for using Fortify Audit Assistant is as follows:

1. Update the Fortify Audit Assistant configuration after upgrading to version 23.2.0 or later. For detailed information, see Configuring Fortify Audit Assistant.
2. Obtain a Fortify Audit Assistant account.
    1. Go to https://analytics.fortify.com.
    2. Click the **Need an Account?** link.
       The **Request a Fortify Audit Assistant Tenant** window opens.
    3. Provide your company information and click **Subscribe**.
       After your information is verified, you will receive a welcome email.
3. Log in to Fortify Audit Assistant and create one or more prediction policies.
   For detailed instructions on how to define prediction policies in Fortify Audit Assistant, see the Fortify Audit Assistant Help in the Fortify Audit Assistant Documentation.
4. Obtain a Fortify Audit Assistant token.
   For detailed information, see the Fortify Audit Assistant Help in the Fortify Audit Assistant Documentation.

5. From the **Audit Assistant** page in Application Security:
    - Configure and test the connection to Fortify Audit Assistant and then, click **REFRESH POLICIES** to populate the **Default prediction policy** list.
    - Specify a default prediction policy.
    - (Optional) Enable Application Security to automatically send unaudited issues to Fortify Audit Assistant for prediction.
    - (Optional) Enable Fortify Audit Assistant to automatically apply predicted values to custom tags.
      For detailed information, see Configuring Fortify Audit Assistant.
6. From Application Security, open an application version, and submit the latest completely audited scan to Fortify Audit Assistant.
   This step is referred to as training. For more information, see Submitting Training Data to Audit Assistant.
7. From Application Security, open an application version and submit its OpenText Fortify SAST analysis results to Fortify Audit Assistant.
8. After Fortify Audit Assistant completes its assessment, view the results and, if necessary, adjust them.
9. Submit corrected results to Fortify Audit Assistant.

See also

About prediction policies

Configuring Fortify Audit Assistant

Configuring Fortify Audit Assistant options for an application version

Enabling auto-apply and auto-predict for an application version

Submitting training data to Fortify Audit Assistant

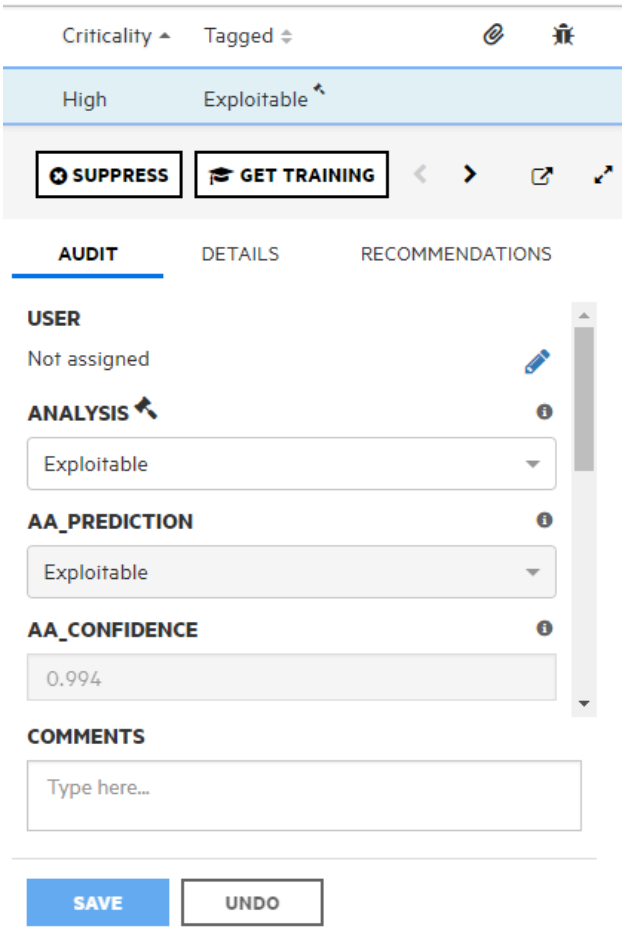
Reviewing Fortify Audit Assistant results

16.8.5. Reviewing Fortify Audit Assistant results

After you submit analysis results to Fortify Audit Assistant and the assessment of the issues is complete, you can examine the results.

To view Fortify Audit Assistant results:

1. Open the **AUDIT** page for the application version.
2. Use the Fortify Priority risk links, the **Group by** list, and **Filter by** lists to display the issues you want to audit.
   See Viewing issues based on folders and Filtering issues for display on the OVERVIEW and AUDIT pages.
3. In the issues table, if you have selected a grouping, expand a group to view the issues it contains.
4. To expand an issue and view its details, click its row in the table.



5. In addition to the **Analysis** tag and any other custom tags associated with the application version, the following tags are displayed in the **Audit** tab:
    - **AA_PREDICTION**—Exploitability level that Fortify Audit Assistant assigned to the issue.
    - **AA_CONFIDENCE**—Fortify 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 0.994 Indicates a confidence level of 99.4 percent.
6. If your exploitability assessment agrees with the **AA_Prediction** value displayed, you can select the value that corresponds to the Fortify Audit Assistant assessment from the list of custom tag values. Otherwise, select a different custom tag value.
7. Click **SAVE**.

See also

About Fortify Audit Assistant

Auditing scan results

16.8.6. About Fortify Audit Assistant training

You can train Fortify Audit Assistant using the decisions your own auditors have made when auditing your analysis results. The training data you provide enables Fortify Audit Assistant to make predictions that are more accurate and relevant to the applications running in your environment. The data you send is non-sensitive metadata derived from and calculated based on your audited analysis results.

By default, your primary custom tag is set as the Audit Assistant Training tag if no other custom tag has been chosen as your Audit Assistant Training Tag.

To configure Application Security to provide training data to Fortify Audit Assistant:

- Select a custom tag to use as your Audit Assistant Training tag. You can use the default **Analysis** custom tag or choose a different custom tag you created. If you do not select a custom tag, Fortify Audit Assistant uses your

primary tag.

- Map custom tag values to Fortify Audit Assistant Training tag values.
- Submit training data to Fortify Audit Assistant.

See also

Selecting a Fortify Audit Assistant training tag

Mapping Fortify Audit Assistant analysis tag values to Application Security custom tag values

Submitting training data to Fortify Audit Assistant

16.8.6.1. Train your model using decisions your auditors make

If you mapped your tags to Fortify Audit Assistant tags and submitted your audited analysis results, the decisions your auditors make are considered, aligning your Fortify Audit Assistant predictions more closely to those of your organization.

To reap the maximum benefits from your training data, it is important that your audits include both EXPLOITABLE and FALSE POSITIVE assessments. After you submit 1,500 or more issues per language, you will see a noticeable improvement in your Fortify Audit Assistant predictions.



Note

The 1,500 issues are per language and should include a comparable number of EXPLOTABLE and FALSE POSITIVE results. All languages might not reach this threshold at the same time.

For more information, see About Audit Assistant Training.

16.8.6.2. Selecting a Fortify Audit Assistant training tag

To set up Fortify Audit Assistant training, you must select a custom tag you want to use to train Fortify Audit Assistant. If you do not select a custom tag, the primary tag is used.

To select a Fortify Audit Assistant tag:

1. Sign in as an Administrator.
2. On the header, select **Dashboard** or **Applications**.
3. Select an application version, and then select **Audit**.
4. On the toolbar, click **PROFILE**.
5. In the **APPLICATION PROFILE** dialog box, select **CUSTOM TAGS**.
6. Select the custom tag you want to use as your Audit Assistant Training tag.
7. Click **SELECT AA TRAINING TAG**.
   The **SELECT AUDIT ASSITANT TRAINING TAG** dialog opens. If the custom tag selected has not been set up for training already, the **Select AA Training Tag** box is **Not Set**.
8. From the **Select AA Training Tag** list, select the custom tag you want to use as your Fortify Audit Assistant training tag.

16.8.6.3. Submitting training data to Fortify Audit Assistant

After an application version has been audited by your security auditors, you can send the training data to Fortify Audit Assistant. The data you send is non-sensitive metadata derived from and calculated based on your audited analysis results.

By default, the primary custom tag is used as the Fortify Audit Assistant Training tag.

To submit training data to Fortify Audit Assistant:

1. From the **Dashboard** or **Applications** view, select the application version of interest and select **Audit**.
2. On the toolbar, click **PROFILE**.
3. In the **APPLICATION PROFILE** dialog box, click the **AUDIT ASSISTANT TRAINING** tab.
   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**.
5. Click **CLOSE**.

6. Select **ARTIFACTS**, and then check to see whether the **Status** field for your upload is **Complete**.

After processing is completed, you can view the results on the **AUDIT** page.

See also

Reviewing Fortify Audit Assistant results

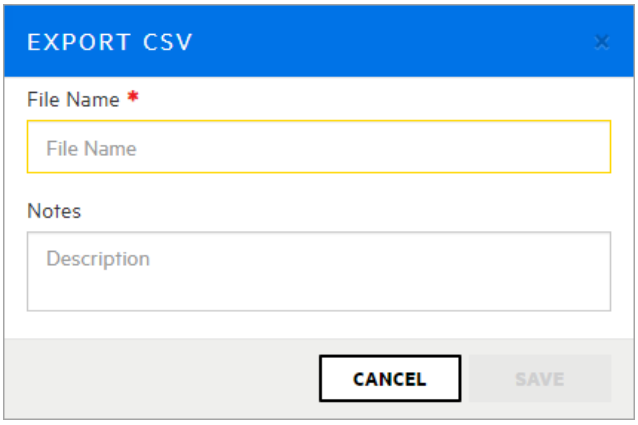
About Fortify Audit Assistant

Enabling auto-apply and auto-predict for an application version

16.9. Exporting open source data

To export open source data displayed on the **OPEN SOURCE COMPONENTS** page:

1. After you upload open source data for an application version, select the **OPEN SOURCE** page for that application version.
2. Click **EXPORT**.



3. In the **File Name** box, type the name for the CSV file to generate.
4. (Optional) In the **Notes** box, type any notes to associate with the generated file.
5. Click **SAVE**.
6. To view the exported result:
    1. On the header, select **Reports**.
    2. Click the **DATA EXPORTS** tab.
    3. In the resulting table, point to the row for the exported file, and then click the **Download** button .

In the resulting CSV file, open source fields are displayed as `<engine_type>.<field_name>`. For example, `SONATYPE.cweurl` corresponds to the Sonatype **CWE URL** field.

To determine how long the system retains your CSV files before deleting them, see Configuring job scheduler attributes. The default expiration period for these reports is two days.

16.10. Integrating Application Security with Fortify WebInspect Enterprise

Application Security and Fortify WebInspect Enterprise are closely integrated and can share analysis results. Administrators can also submit requests for dynamic scans from the user interface. This section describes how to view OpenText Fortify DAST results in Application Security and provides instructions for Application Security users on how to request dynamic scans.

16.10.1. Viewing OpenText DAST analysis results in Application Security

OpenText Fortify DAST saves analysis results (results data and audit data) in FPR format, which you can upload to Application Security. See Uploading scan artifacts. OpenText Fortify DAST issue details differ from those shown for issues uncovered by other analyzers, such as OpenText Fortify SAST.

Important

To successfully integrate OpenText Fortify DAST with Application Security, you must install a trusted CA certificate on the Java™ Runtime Environment on both the Application Security and OpenText Fortify DAST servers.

In the left pane of the **CODE** tab, the **Overview** section displays summary information about the finding and the **Implications** section. The **Additional References** section lists any pertinent references available.

The center pane displays the following information:

URL—Website page on which the vulnerability was detected

Method—HTTP method used for the attack (for example GET, PUT, and POST)

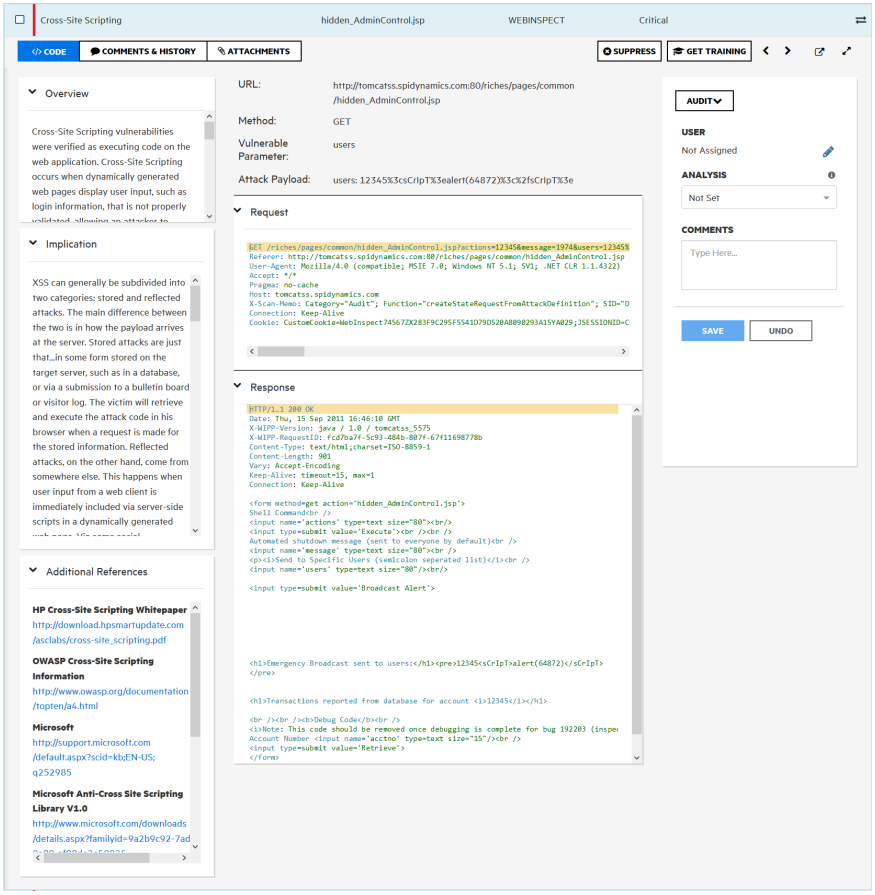
Vulnerable Parameter—Name of the vulnerable parameter

Attack Payload—Shellcode used as the payload for exploiting the vulnerability

Below this information, the **Request** section displays the request made, with the attack highlighted. The **Response** section displays the response to the request, with the trigger highlighted.

Note

If responses contain binary data or a large volume of data (more than 50 KB), you can see the **Download Response** button at the bottom of the **Response** section. To download responses such as these in a text file, click **Download Response**.



The **Steps** tab is available only if the steps are included in the OpenText Fortify DAST results file.

Viewing additional details and recommendations

To view additional details and recommendations for the issue, on the issue toolbar, click either the **Open in new tab** button or the **Expand to full screen** button.

The **Details** provides suggestions on what to look for in this issue.

To view recommendations and tips on how to address the issue, from the **AUDIT** list, select **Recommendations**.

For information about how to audit the issue, see Auditing scan results.

16.10.2. OpenText DAST audit data

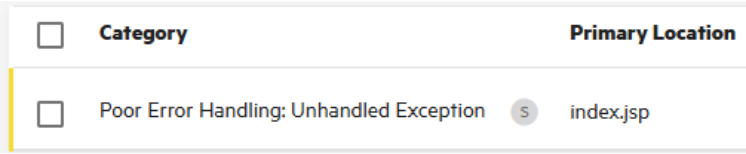
In addition to screen shots, the following types of audit data are transferred from OpenText Fortify DAST to Application Security:

- **Vulnerability Notes**—Vulnerability notes in OpenText Fortify DAST are transferred to Application Security as issue comments.
- **Ignored Vulnerabilities**—Vulnerabilities marked as "Ignored" in OpenText Fortify DAST are marked "Suppressed" after transfer to Application Security.
- **False Positives**

16.10.3. False positives

Application Security does not have a direct equivalent of the OpenText Fortify DAST "false positive" status. If an OpenText Fortify DAST 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 Application Security, you can use the default **Analysis** custom tag. An OpenText Fortify DAST false positive is assigned the **Analysis** value "Not an Issue" in Application Security. To emulate the OpenText Fortify DAST behavior of hiding the issue from lists and counts, the issue is marked as **Suppressed**.



Note

If the selected value for **Analysis** has changed from "Not an Issue" or is missing, or if the **Analysis** list has been removed from your application version, then the false positive status of the issue is lost. The issue is marked as "Suppressed."

See also

Setting issue viewing preferences

16.10.4. Submitting dynamic scan requests to Fortify WebInspect Enterprise

If OpenText Fortify DAST is installed in your environment, and you are assigned to one of the following roles, you can request scans from Application Security:

- Administrator
- Security Lead
- Manager
- Developer

To create a scan request for an application version:

1. From the **Dashboard** or **Applications** view, select the application version that you want to have scanned, and then select **Artifacts**.
2. On the **ARTIFACT HISTORY** page, click **DYNAMIC SCAN**.
3. Provide the information described in the following table.

The following table does not list custom dynamic scan attributes that you or another Application Security Administrator might have added to the system.

Dynamic scan attribute	Description
URL	(Required) URL of the site to scan
Site Login	Username required to log on to the site to scan
Site Passcode	Password to use to gain access to the site
Network Login	Username required for network authentication
Network Passcode	Password required for network authentication
Related Host Name(s)	Allowable hosts for the application to scan
Web Services Used	Comma-delimited list of web services used by the application to scan
Technologies Used	Comma-delimited list of technologies used by the site to scan
Compliance Implications	Information about any potential compliance implications
Allowable Scan Times	Dates and times during which the tester can perform the scan For example: From 17:00 h to 06:00 h, Monday through Friday, from 09/03/18 to 11/30/18 You can run the scan immediately instead of scheduling it to run later.
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 OpenText Fortify DAST might have interest 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**.
   Application Security displays a message to verify that the request submission was successful.
   Next, the OpenText Fortify DAST tester who monitors and responds to scan requests runs the scan during the hours you specified, and then uploads the results to Application Security.
5. If you are a Application Security Administrator or Application Security Tester, you can run the requested dynamic scan immediately from Fortify WebInspect Enterprise.

See also

Viewing OpenText Fortify DAST analysis results in Application Security

Processing dynamic scan requests from Fortify WebInspect Enterprise

16.10.5. 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 Application Security users.

To process dynamic scan requests in Fortify WebInspect Enterprise:

1. From Fortify WebInspect Enterprise, initialize Application Security, and then use the WebInspect Enterprise Console to synchronize Application Security application versions with WebInspect projects (see the *OpenText™ Fortify WebInspect Enterprise User Guide*).
2. From the Application Security **Dashboard** or the **Applications** view, select an application version for which a dynamic scan was requested, and then select **Artifacts**.
3. On the **ARTIFACTS** page, click **LAUNCH WIE**.
4. Under the header, click **Scan Requests**.
   The **SCAN REQUESTS** view lists all dynamic scan requests submitted from Application Security to Fortify WebInspect Enterprise.
5. Select the pending request.
6. In the lower pane, on the **Details** tab, from the **Status** list, select **In Progress**, and then click **Change Status**. In Application Security, 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 Application Security. For detailed instructions, see the *OpenText™ Fortify WebInspect Enterprise User Guide*.

See also

Submitting dynamic scan requests to Fortify WebInspect Enterprise

16.10.6. Editing and canceling dynamic scan requests

To view the status of the last dynamic scan request submitted for an application version:

1. Go 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**.

Application Security displays the date and time the scan request was submitted, and request status information.

Dynamic scan request states

After you submit a dynamic scan request, (see Submitting dynamic scan requests to Fortify WebInspect Enterprise) 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.

If a dynamic scan request is pending, you can edit or cancel it. As soon as the scan starts, however, you can no longer edit or cancel it.

Editing dynamic scan requests

To edit a dynamic scan request:



Note

You can edit only scan requests that you have submitted.

1. Go to the Issues tab on the details page for the application version for which you have requested a dynamic scan.
2. From the **Dynamic Scan Request** list, select **Edit**.
3. In the **Dynamic Scan Request** dialog box, edit the values for the dynamic scan attributes, and then click **Submit**.

Canceling dynamic scan requests

To cancel a pending dynamic scan request, do the following:



Note

You can cancel only scan requests that you have submitted.

1. Go 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**.
   Application Security prompts you to confirm that you want to cancel the last dynamic scan request.
3. Click **Yes**.

16.11. Viewing open source data

After you download, install, and enable the OpenText Fortify SCA or Sonatype parser plugin for Application Security, you can view the open source vulnerability data uploaded for an application version. You can view the results uploaded for an application version either from the **AUDIT** page, or from the **OPEN SOURCE** page.

Viewing open source data from the AUDIT page

To view open source vulnerability results from the **AUDIT** page:

1. On the header, select **Applications**.
2. Select the application version for which open source results have been uploaded.
3. From the **Group by** list on the **AUDIT** page, select **Analysis Type**.
4. Expand the **DEBRICKED** or **SONATYPE** header, and then expand the row for a result you want to examine.

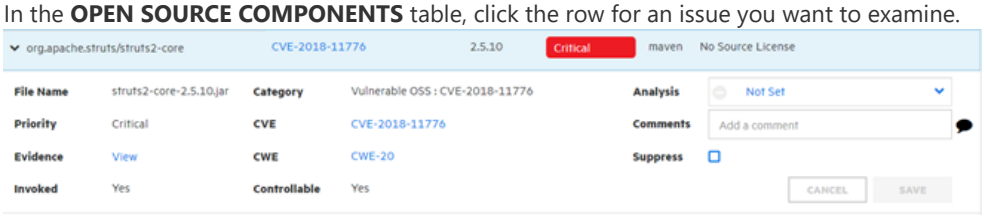
For detailed information about how to interpret OpenText Fortify SCA vulnerability data displayed, see the Debricked documentation. For information about how to interpret Sonatype vulnerability data displayed, see the Sonatype documentation.

For information about how to audit open source results, see Auditing analysis results.

Viewing open source data from the OPEN SOURCE page

To view open source results from the **OPEN SOURCE** page:

1. On the header, select **Applications**.
2. Select the application version for which open source results have been uploaded.
3. Click **OPEN SOURCE**.
   The **OPEN SOURCE** page is visible only if open source results have been uploaded for the selected application version.
4. In the **OPEN SOURCE COMPONENTS** table, click the row for an issue you want to examine.



   The following table contains descriptions of the details shown.

Field	Description
File Name	Name of the component file in which the issue was discovered.
Category	OSS index category: Common Vulnerabilities and Exposures ID
Analysis (or other assigned primary tag)	If you audit the issue from the **OPEN SOURCE** page, you can select a primary tag value to assign from this list.
Priority	Fortify priority rating
CVE	CVE (Common Vulnerabilities and Exposures) ID number assigned to the vulnerability. Click the link to go directly to a highly detailed description of that vulnerability on the CVE site.
Comments	If you audit the issue from the **OPEN SOURCE** page, you can add comments.
Evidence	A link to any evidence if the vulnerability is invoked or controllable.
CWE	Common Weakness Enumeration. Click this link (if present) to go to the Common Weakness Enumeration website and see details about the software weakness type uncovered.
Suppress	Select this check box if you think that the issue is not of concern. For more information about issue suppression, see About suppressed, removed, and hidden issues.
Invoked	This field shows whether the issue was invoked in the code.
Controllable	This field shows whether or not user-controlled input reaches the method or function.

For detailed information about how to interpret the OpenText Fortify SCA vulnerability data displayed, see the Debricked documentation. For information about how to interpret Sonatype vulnerability data displayed, see the Sonatype documentation.

See also

Preparing to display Debricked results

Preparing to display Sonatype results

16.12. Downloading an OpenText Core SCA (Debricked) software bill of materials

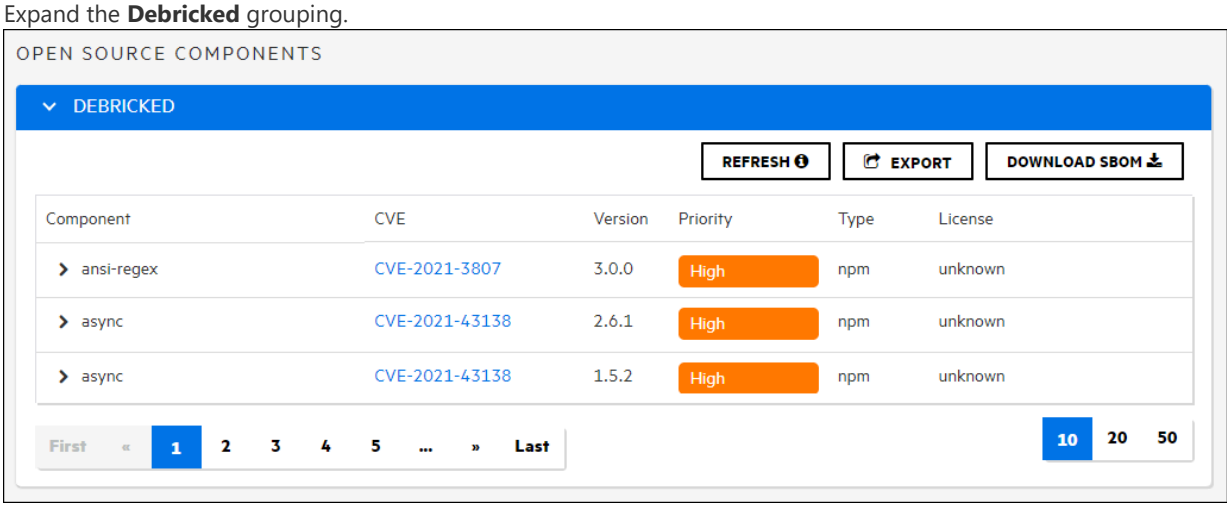
The software bill of materials (SBOM) is a list of the software dependencies included in a software application. In addition to direct dependencies, it also includes dependencies used by those dependencies, also known as indirect or transitive dependencies. It describes the supply chain relationships used when building the software. The SBOM is in the CycloneDX format.

You can download the SBOM as a JSON file to assess the open source components in use. Using the information provided in the SBOM, you can make decisions on whether or not the versions you are using are safe for your project or whether

you need to change to a different version or open source package or a different open source package.

To download an SBOM:

1. On the header, select **Applications**.
2. Select the application version for which open source results have been uploaded.
3. Click **OPEN SOURCE**.
4. Expand the **Debricked** grouping.



5. Click **Download SBOM**.
6. Open the downloaded JSON file in a text editor to view the SBOM.

17. Working with OpenText ScanCentral DAST

If Application Security is configured to communicate with OpenText Fortify ScanCentral DAST to request and manage dynamic scans, then the **DAST** tab in the **ScanCentral** view includes the **Scans**, **Sensors**, **Sensor Pools**, **Settings List**, and **Scan Schedules** pages. For information about how to configure the connection between Application Security and OpenText Fortify ScanCentral DAST, see Enabling the Running and Management of OpenText Fortify ScanCentral DAST Scans.

This section contains the following topics:

- OpenText ScanCentral DAST permissions
- Submitting requests for dynamic scans to OpenText ScanCentral DAST
- Synchronizing audit history changes in OpenText ScanCentral DAST using Kafka

17.1. OpenText ScanCentral DAST permissions

The following table shows which Application Security roles have permission to perform which OpenText Fortify ScanCentral DAST-related tasks.

Role	Permissions
View-Only	• View OpenText Fortify ScanCentral DAST data, except for jobs not assigned to any application version **Restrictions:** • Users see only the scans for application to which they are assigned • Users see only sensor pool assignment for the applications to which they are assigned
Security Lead	• View OpenText Fortify ScanCentral DAST data • Create, run, change, and delete scans, schedules, and settings • Manage pools and sensors • Download artifacts • Run scans from existing templates and base settings • Manage deny intervals, application priority level, and retention policy • Manage global restrictions, restricted scan settings, and private data settings • Manage key stores and artifacts repositories **Restrictions:** • Users can cancel only those scan requests for application versions to which they are assigned. • Users can assign only application versions to which they are assigned to sensor pools.
Manager	• View OpenText Fortify ScanCentral DAST data • Manage pools and sensors **Restrictions:** • Users cannot update scan-related data • Users can cancel only those scan requests for application versions to which they are assigned. • Users can assign only application versions to which they are assigned to sensor pools.
Developer	• View OpenText Fortify ScanCentral DAST data • Run scans from existing templates and base settings • Download artifacts

Application Security Tester	• View OpenText Fortify ScanCentral DAST data • Create, run, modify and delete scans, schedules, and settings • Run scans from existing templates and base settings • Download artifacts

See also

Viewing permission information for Application Security roles

17.2. Submitting requests for dynamic scans to OpenText ScanCentral DAST

If Application Security is integrated with OpenText Fortify ScanCentral DAST, and you are assigned to one of the following roles, you can request dynamic scans from Application Security:

- Administrator
- Application Security Tester
- Security Lead
- Developer

For information about how to configure OpenText Fortify ScanCentral DAST scans and work with scans, sensors, sensor pools, settings, and scan schedules, see the *OpenText™ Fortify ScanCentral DAST Configuration and Usage Guide*.

See also

Enabling the running and management of OpenText Fortify ScanCentral DAST scans

OpenText Fortify ScanCentral DAST permissions

17.3. Synchronizing audit history changes in OpenText ScanCentral DAST using Kafka

Issues in Application Security that are managed in the **AUDIT** page and published to OpenText Fortify ScanCentral DAST are referred to as Findings.

Configure Kafka in Application Security to synchronize audit history changes for suppressed issues, priority override, and analysis tag settings to OpenText Fortify ScanCentral DAST. For more information on how to set up Kafka in Application Security, see Configuring a Kafka Stream.

When you audit an issue in Application Security, a background process requests the audits to be published to the Kafka topic. OpenText Fortify ScanCentral DAST processes the audits and reflects any suppressed issues, priority override, and analysis tag settings in the Scans view and scan visualization.

18. Working with Fortify ScanCentral SAST

If Application Security is configured to communicate with OpenText Fortify ScanCentral SAST, then the **SAST** tab is enabled in the **ScanCentral** view. The **SAST** tab displays the **Scan Requests**, **Sensors**, **Controller**, and **Sensor Pools** pages. For information about how to configure the connection between Application Security and OpenText Fortify ScanCentral SAST, see Enabling integration with OpenText Fortify ScanCentral SAST.

This section contains the following topics:

- Fortify ScanCentral SAST permissions
- Viewing Fortify ScanCentral SAST scan request details
- Prioritizing a Fortify ScanCentral SAST scan request
- Canceling Fortify ScanCentral SAST scan requests
- Viewing Fortify ScanCentral SAST sensor information
- Viewing Fortify ScanCentral SAST Controller information
- About Fortify ScanCentral SAST sensor pools

18.1. Fortify ScanCentral SAST permissions

The following table shows which Application Security roles have permission to perform which OpenText Fortify ScanCentral SAST-related tasks.

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

Roles	Permissions
View-Only	• View OpenText Fortify ScanCentral SAST data, except for jobs not assigned to any application version. **Restrictions:** • Users see only the scan requests for application versions to which they are assigned. • Users see only sensor pool assignment for the application versions to which they are assigned.
Administrator	• View, download, and manage OpenText Fortify ScanCentral SAST data • Perform all tasks that involve changes to sensor pools • Cancel scan requests • Assign sensors and application versions to sensor pools **Restrictions:** • Users can cancel only those scan requests for application versions to which they are assigned. • Users can assign only application versions to which they are assigned to sensor pools.
Security Lead, Manager	• View, download, and manage OpenText Fortify ScanCentral SAST data, except for jobs not assigned to any application version **Restrictions:** • Users can cancel only those scan requests for application versions to which they are assigned. • Users can assign only application versions to which they are assigned to sensor pools.
Developer	• View OpenText Fortify ScanCentral SAST data, except for jobs not assigned to any application version

See also

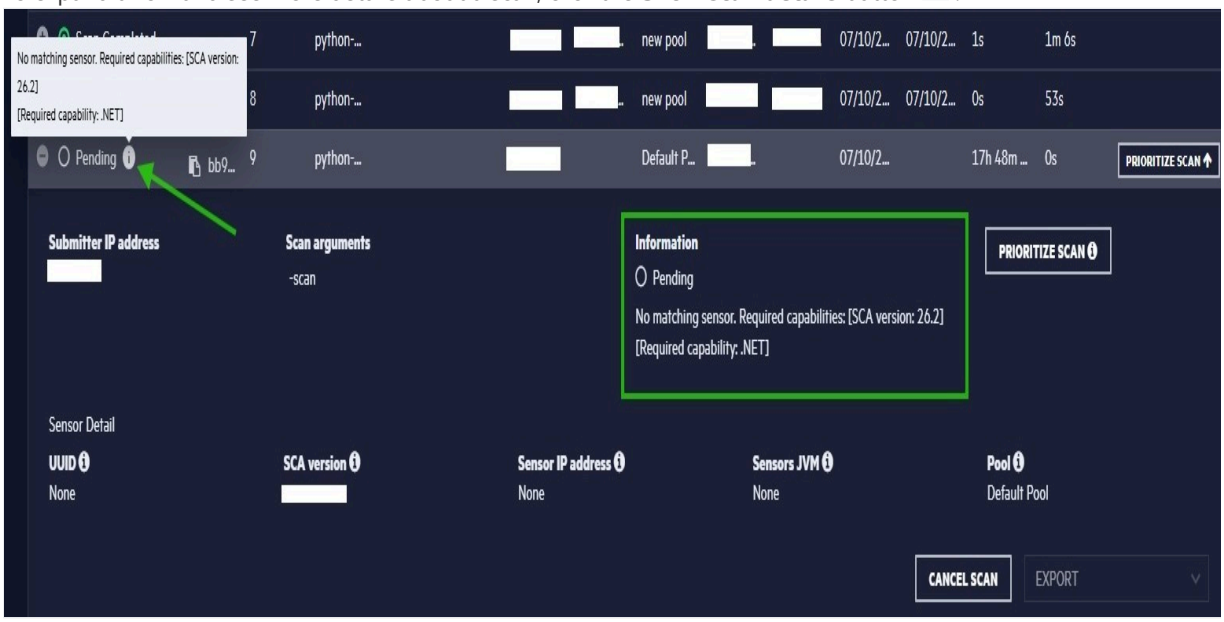
Viewing permission information for Application Security roles

18.2. Viewing Fortify ScanCentral SAST scan request details

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

To view details about scan requests:

1. On the header, select **ScanCentral**, and then select **SAST**.
   The **Scan Requests** page lists all scan requests and the details for each scan.
2. (Optional) To filter the displayed scan requests, click a column heading and select from a list, select a date and time, or type a search string depending on the selected column type.
   For example, to filter the results by application name, click the **Application** column heading and type the first few letters of the name. To filter by job status, click the **Status** column heading and select a status from the list.
   When a status message is available, an information icon appears after the status type. Hover over the icon to view the message. Currently, only the **Pending** status includes a status message.
   To clear any applied filtering, click **RESET**.
3. (Optional) To modify the display, such as clearing sorting, or selecting the columns to display, click the **Display options** button .
4. To expand a row and see more details about a scan, click the **Show scan details** button .



   When a status message is available, the expanded details display an **Information** label. Below the label, the status icon, type, and message appear.
5. To export the scan request details, from the **EXPORT** list, select either **FPR** to export an FPR file with vulnerabilities uncovered by the scan, or **Log** to export the log file from the scan.
6. To update the data displayed, click **REFRESH**.

See also

Prioritizing a OpenText Fortify ScanCentral SAST scan request

Canceling OpenText Fortify ScanCentral SAST scan requests

Viewing OpenText Fortify ScanCentral SAST sensor information

Viewing OpenText Fortify ScanCentral SAST Controller information

18.3. Prioritizing a Fortify ScanCentral SAST scan request

If several scan requests are assigned to a sensor pool, and you want one of these to be run before any of the others, you can prioritize it, which moves it to the top of the job queue for that pool.

To prioritize a scan request:

1. On the header, select **ScanCentral**, and then select **SAST**.
2. From the **Status** list, select **Pending**.
   The numbers in the **Priority** column indicate the order the scan jobs are run. The lower the number, the sooner the scan is run in the pool. For example, a scan request with a priority of -10 is run before a scan request in the same pool with a priority of -2.
3. Click **PRIORITIZE SCAN** in the row for the scan you want to run first.

18.4. Canceling Fortify ScanCentral SAST scan requests

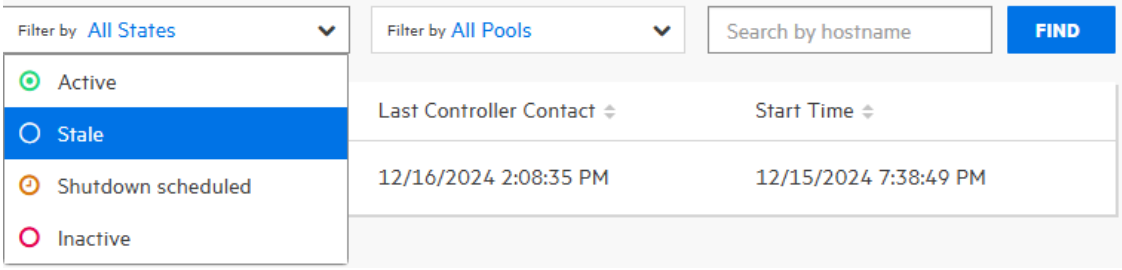
To cancel a pending scan request:

1. On the header, select **ScanCentral**, and then select **SAST**.
2. From the Status list, select **Pending**.
3. Expand the row for the pending scan request that you want to cancel.
4. Click **CANCEL SCAN**.
5. Confirm the cancellation of the scan request.
6. To update the data displayed on the **Scan Requests** page, click **REFRESH**.

18.5. Viewing Fortify ScanCentral SAST sensor information

To view current information about sensor states and activities:

1. On the header, select **ScanCentral**, and then select **SAST**.
2. On the navigation pane, select **Sensors**.
3. To filter the sensors displayed based on the current sensor state, from the **Filter by** state list, select **Active**, **Inactive**, **Stale**, or **Shutdown scheduled**.



   By default, all sensors in any state are displayed.
4. To filter the sensors displayed based on the pool, from the **Filter by** pool list, select either **Unassigned Pool**, or a named pool.
   By default, all sensors in any pool are displayed.
5. To see the details for a sensor, click its row.

See also

Canceling OpenText Fortify ScanCentral SAST scan requests

Viewing OpenText Fortify ScanCentral SAST scan request details

18.6. Viewing Fortify ScanCentral SAST Controller information

To view Controller information:

1. On the header, select **ScanCentral**, and then select **SAST**.
2. On the navigation pane, select **Controller**.
3. For descriptions of each value displayed, click the information button .

See also

Viewing OpenText Fortify ScanCentral SAST scan request details

Canceling OpenText Fortify ScanCentral SAST scan requests

Viewing OpenText Fortify ScanCentral SAST sensor information

18.6.1. Stopping the Controller

You can stop the Controller immediately using the following procedure. However, OpenText strongly recommends that you first place the Controller in maintenance mode to preserve any scans that are running.

To stop the Controller:

1. On the machine where the Controller is installed, type the following command:

   ```
   cd <controller_install_dir>/tomcat/bin
   ```

Type one of the following commands:

On a Windows system: `shutdown.bat`

On a Linux system: `./shutdown.sh`

See also

Placing the Controller in maintenance mode

18.6.2. Placing the Controller in maintenance mode

An abrupt shutdown of the OpenText Fortify ScanCentral SAST Controller can result in the loss of scans already started on sensors. To prevent this from happening, place your Controller in maintenance mode. After you do, the Controller accepts no new job requests from clients and assigns no queued jobs to sensors.

After the Controller is placed in maintenance mode, sensors complete the scans they are currently running, but accept no new scans. After the Controller is back up and running, the sensors again become available.

To place the Controller in maintenance mode:

1. Sign in as an Administrator.
2. On the header, select **ScanCentral**, and then select the **SAST** page.
3. On the navigation pane, select **Controller**.
4. Click **START MAINTENANCE MODE**.

The Controller receives the maintenance request from Application Security and, if any sensors are running scans, the Controller mode changes from **ACTIVE** to **WAITING_FOR_JOB_COMPLETED**. If no job is being processed, the mode changes directly from **ACTIVE** to **MAINTENANCE**. At this point, you can safely shut down the Controller.

18.6.3. Safely shutting down Fortify ScanCentral SAST sensors

This topic describes how to move sensors to shutdown, or shutdown scheduled mode.

> **Important**
>
> If the Controller is in maintenance mode (see Placing the Controller in maintenance mode), you cannot shut down sensors from the Application Security user interface.

To shut down active sensors:

1. Sign in as an Administrator.
2. On the header, select **ScanCentral**, and then select the **SAST** page.
3. On the navigation pane, select **Sensors**.
4. Do one of the following:
   - Expand the row for a sensor you want to shut down, and then click **SHUT DOWN**.
   - Select the check boxes for one or more sensors you want to shut down, and then click **SHUT DOWN**.

Note

If the **SHUT DOWN** button is not enabled, it can mean that:

- The sensor was already shut down
- The Controller is in maintenance mode
- The sensor is inactive or disabled

If a sensor you shut down is running a scan, the **State** value for the sensor changes from **Active** to **Shutdown scheduled**. After the scan is completed, the state then changes to **Inactive**.

18.6.4. Removing the Controller from maintenance mode

To remove the Controller from maintenance mode:

1. Sign in as an Administrator
2. On the header, select **ScanCentral**, and then select the **SAST** page.
3. On the navigation pane, select **CONTROLLER**.
4. Click **END MAINTENANCE MODE**.

See also

Placing the Controller in maintenance mode

Stopping the Controller

18.7. About Fortify ScanCentral SAST sensor pools

If your Application Security server is integrated with OpenText Fortify ScanCentral SAST, and you are an Administrator, Manager, or Security Lead, you can create groups of sensors, or *sensor pools* based on any criteria, which you can then target for scan requests.

Sensor pools give you more control over the sensors used for scan requests. The following are examples of how you might use sensor pools:

- Create pools based on sensor computing power (physical memory size) and assign scan requests that require a lot of memory to those pools.
- Create pools based on teams or business units in your organization. This ensures that your resources are distributed, and no team can consume all sensors and block scan requests submitted by other teams.

If a scan request is associated with an application version, the Controller queries Application Security for available sensor pools. If the scan request is not associated with an application version, OpenText Fortify ScanCentral SAST clients can request a specific sensor pool for a scan request.

Note

By default, sensors are removed 168 hours (7 days) after they become inactive. For details on how to change this default value, see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

Pre-defined sensor pools

Application Security provides two pre-defined sensor pools: the *unassigned sensor pool* and the *default pool*. The unassigned sensor pool, which contains all newly-registered sensors, serves as a shared sensor pool for other pools. If when you create a sensor pool the **Use unassigned sensors** check box is selected, the default sensor pool uses sensors from the unassigned sensor pool. It contains scan requests that were not assigned to a specific sensor pool.

See also

Creating OpenText Fortify ScanCentral SAST sensor pools

OpenText Fortify ScanCentral SAST permissions

Deleting ScanCentral pools

18.7.1. Creating Fortify ScanCentral SAST sensor pools

If your Application Security server is integrated with OpenText Fortify ScanCentral SAST, you can create sensor pools, which you can then target for scan requests.

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

To create a new sensor pool:

1. On the header, select **ScanCentral**, and then select **SAST**.
2. On the navigation pane, select **Sensor Pools**.
   The **Sensor Pools** page lists the default pool and any other sensor pools created on the system.

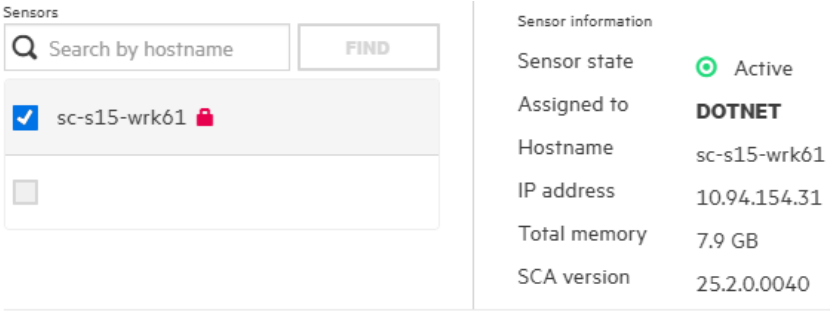
   > **Note**
   >
   > The default pool includes all application versions that have not been assigned to a sensor pool.

3. Click **+ NEW POOL**.
   If the **+ NEW POOL** button is unavailable, Application Security is not connected to the Controller. Check your OpenText Fortify ScanCentral SAST configuration (see Enabling integration with OpenText Fortify ScanCentral SAST).
4. In the **Name** box, type a name for the new pool.
   The first character of the pool name must be a Unicode alphanumeric character (lowercase or uppercase a through z, or 0 through 9).
5. (Optional) In the **Description** box, type a description of the new pool (its properties or purpose).
6. To enable the new pool to use any unassigned sensors, select the **Use unassigned sensors** check box.

   > **Note**
   >
   > Selecting the **Use unassigned sensors** check box does not assign those sensors to the new pool. Instead, it enables the pool to take advantage of available unassigned sensors. The sensors remain unassigned.

   > **Note**
   >
   > You can have up to ten sensors in a pool.

   The **Sensors** table lists the host names of all of the sensors in the system, including those that are assigned to other pools. A padlock symbol next to the host name indicates that the sensor is assigned to a pool. To see information about a sensor, select its row. The **Sensor information** area lists basic information about the sensor, including the pool to which it is currently assigned, if any.



7. To find a specific sensor, type its host name in the **Search by hostname** box, and then click **FIND**.
8. Select the check box for each sensor you want to assign to the new pool.

If you select the check box for a sensor that is already assigned, that sensor will be moved from the pool to which it is currently assigned.

9. To assign application versions to the pool:
    1. Under **Versions**, click **ADD**.
    2. In the **APPLICATION** pane, select an application that you want to assign to this pool.
       The **VERSIONS** pane lists all active versions of the selected application.
    3. To list any inactive versions of the selected application, select the **Show inactive** check box.
    4. To assign all the listed versions to the new pool, select the **Select all** check box. Otherwise, to assign only a subset of the application versions, select the check boxes next to the version names.
       The **SELECTED VERSIONS** pane lists your selections.
    5. To assign versions of another application to this pool, repeat steps b through d.
    6. To remove an application version from the **SELECTED VERSIONS** list, click the **Delete** button next to its name.
    7. Click **DONE**.
10. In the **CREATE NEW POOL** dialog box, click **SAVE**.

The **Sensor Pools** table now lists your new pool.

You can edit or delete the pool at any time.

See also

Deleting ScanCentral pools

Viewing OpenText Fortify ScanCentral SAST sensor information

18.7.2. Moving sensors between pools

To move OpenText Fortify ScanCentral SAST sensors between pools:

1. On the header, select **ScanCentral**, and then select **SAST**.
2. On the navigation pane, select **Sensor Pools**.
3. On the **SENSOR POOLS** page, select the sensor pool with sensor that you want to assign to a different pool or pools.
4. Click **EDIT POOL**.
5. Under **Sensors**, clear the check box for the sensors you want to assign to a different pool.
6. Click **SAVE**.
7. On the **SENSOR POOLS** page, select the sensor pool to which you want to assign the now unassigned sensors, and then use the steps provided in Creating OpenText Fortify ScanCentral SAST sensor pools to assign the now unassigned sensors.

See also

About OpenText Fortify ScanCentral SAST sensor pools

18.7.3. Deleting Fortify ScanCentral SAST sensor pools

To delete a sensor pool:

1. On the header, select **ScanCentral**, and then select **SAST**.
2. On the navigation pane, select **Sensor Pools**.
   The **Sensor Pools** page lists all existing pools. The last column of the table displays a **Delete Pool** button for each pool. If the button appears dimmed, you cannot delete the pool.
3. Click the **Delete Pool** button that corresponds to the pool you want to delete.

Application Security removes the pool from the list and adds all sensors assigned to the deleted pool to the **Unassigned Sensors** tab.

See also

Viewing OpenText Fortify ScanCentral SAST sensor information

Creating OpenText Fortify ScanCentral SAST sensor pools

19. BIRT reports

Application Security 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, go to the BIRT website.

Templates are available in the following report categories:

- Application Reports
  The Application Summary report summarizes one 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 application version.
- Portfolio Reports
  The Portfolio report group contains reports that enable you to compare issues trends and indicators across multiple application versions.

This section contains the following topics:

- BIRT libraries
- Importing report libraries
- Generating and downloading reports
- Generating and downloading customized BIRT reports in XLSX
- Customizing BIRT reports
- Acquiring the BIRT Report Designer
- Downloading report templates
- Importing report definitions

19.1. BIRT libraries

You can use BIRT libraries to encapsulate commonly required functions and report items. You can then import these libraries 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.

Before you can use the BIRT report libraries, you must acquire the BIRT Report Designer. For instructions, see Acquiring the BIRT Report Designer.

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 many report designs, then a change to the logo only requires a change to the library. All referencing reports would reflect the change automatically.

19.2. Importing report libraries

An Administrator can add report libraries to the Application Security server.

To add a report library:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then select **Report Libraries**.
   The **Report Libraries** page lists all of the report libraries in the system.
3. Click **IMPORT**.
4. (Optional) In the **Description** box, type a description of the library you are importing.
5. Click **BROWSE**, and then find and select the report library resource.
6. Click **SAVE**.

The **Report Libraries** table now includes the added library.

See also

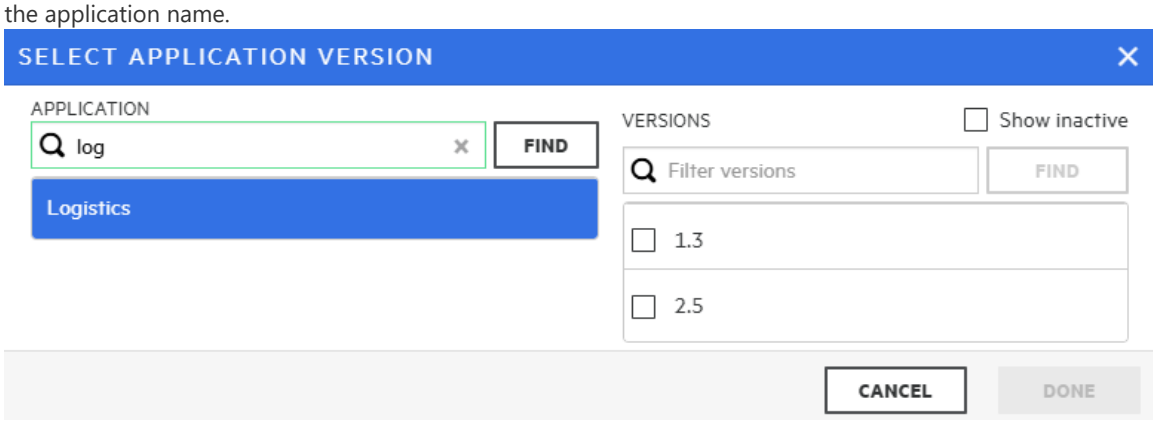
Preventing destructive library and template uploads to Application Security

Generating and viewing reports

19.3. Generating and downloading reports

To generate and download a report:

1. On the header, select **Reports**.
2. On the **Reports** toolbar, click **+ NEW REPORT**.
3. Select the report template you want to use.
   The **Parameters** pane displays the configuration fields for the template you select.
4. Specify the required report settings, including the report name and output format.
5. To specify the application versions to include in the report:
   1. Under **Application version**, click **BROWSE**.
   2. In the **SELECT APPLICATION VERSION** dialog box, under **APPLICATION**, select one of the applications listed, or, in the **Filter applications** box, enter part or all of the application name, press **Enter**, and then select the application name.



   The active versions of the selected application are listed under **VERSIONS**.
   3. Select the check box for the version to include in the report. (You can select only one.)
      For Portfolio Reports, you can select multiple application versions to include in the report.
   4. Click **DONE**.
6. On the **Parameters** pane, do the following:
   - If multiple editions of a report template are available, from the **Options** list, select the edition you want to generate.
   - Depending on the report type, additional settings might be required or available.
7. Click **GENERATE**.
   Application Security adds the report to the **Reports** table, which lists all reports, grouped by the report template. After the report generation is completed, the **Status** column displays the value **Complete**.

> **Note**
> If you typed content in the **Notes** box when you configured the report, the **Notes** column contains a note icon.

8. To download the report, point to the report name, and then click the **Download** button .

For information about how to specify the number of days to keep reports before they are automatically removed from the system, see Configuring job scheduler settings.

See also

Downloading report templates

Importing report definitions

19.4. Generating and downloading customized BIRT reports in XLSX

To download a customized BIRT report in XLSX format:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then select **Report Templates**.
   The **Reports** page lists the name, type, and description of each report in the system.
3. Click the row for the customized report template of interest.
4. Click **EDIT**.
5. Click **+ADD PARAMETER**.
6. 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 customized report template.
Description	(Optional) Type a description of the parameter.
Identifier	Type `enableXlsxGeneration` to add XLSX output format to the customized report template.
Data Type	Select **Boolean**.

7. Click **APPLY**.
8. Click **SAVE** to apply the changes.
9. On the header, select **Reports**.
10. Click **+ NEW REPORT**.
11. From the **Templates** pane, select the customized report template that you configured earlier.
12. In the **Report name** box, type a name for the customized BIRT report.
13. For **Output format**, select **XLSX**.
14. Click **GENERATE**.
    Application Security adds the customized BIRT report to the **Reports** table. After the report generation is complete, the **Status** field displays **Complete**.
15. To download the report, point to the report name, and then click the **Download** button .

19.5. 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 with Eclipse BIRT Report Designer. OpenText recommends that you have Professional Services assist you with your custom reports.

To customize a Application Security BIRT report:

1. Acquire a supported version of Eclipse BIRT Report Designer (*Report Designer*).
   For information about downloading Eclipse BIRT Report Designer, see Acquiring the BIRT Report Designer.
2. Load a Application Security report definition into Report Designer.
   You typically first export a report definition from Application Security, and then upload that report definition into Report Designer. For information about how to export a Application Security report definition, see Downloading report templates.
3. Connect Report Designer to a running instance of the Application Security database.
   Connecting Report Designer to the Application Security 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 Application Security to test the operation of a customized BIRT report.

6. Import the customized report definition into Application Security.

See also

Importing report definitions

19.6. Acquiring the BIRT Report Designer

To customize reports, you must use a supported version of the Eclipse BIRT Report Designer (Report Designer). For information about supported versions, see the *Application Security Software System Requirements* document.

To download the Eclipse BIRT Report Designer:

1. In a web browser, go to the Eclipse Downloads page.
2. Download the Report Designer Full Eclipse Install for your operating system.
3. Install the designer.
   For instructions, see the BIRT webpage.

19.7. Downloading report templates

You can download a Application Security report template for modification.



Caution

Although you can download, modify, and re-import report templates, keep in mind that OpenText does not support customized report templates.



Note

You cannot modify a parameter named "Options" in a BIRT report.

To download a Application Security report template:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then select **Report Templates**.
   The **Reports** page lists the name, type, and description of each report in the system.
3. Click the row for the report of interest.
4. Click **DOWNLOAD TEMPLATE**.

You can use the BIRT Report Designer to modify the downloaded report, and then re-import the file into Application Security. If you do, ensure that you rename the modified report file so that it does not replace the original template when you import it.

For information about how to import a customized BIRT report into Application Security, see Importing report definitions.

See also

Generating and viewing reports

19.8. Importing report definitions

A BIRT report definition provides the Application Security report engine the information it needs to generate a report. This includes information such as the report name, report parameters, and the name of the report template file.

BIRT enables you to import report definitions files to Application Security. To do this, you need a Application Security BIRT definition file (with the `.rptdesign` extension).



Caution

When you develop BIRT reports, any database credentials specified are stored insecurely in the report design file. Ensure that you delete credentials from a report before you deploy it to Application Security.

To import a report definition:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Templates**, and then select **Report Templates**.
   The **Reports** page lists the name, type, and description of each report in the system.
3. Click **IMPORT**.
4. In the **IMPORT NEW REPORT TEMPLATE** dialog box, provide the information described in the following table.

Field	Description
Name	Type a name for the template.
Description	(Optional) Type a description of the template and its purpose.
Category	Select a category for the template.
Report Engine	Leave **BIRT** selected.
Template	Browse to and select a Application Security BIRT definition file (with the `.rptdesign` extension).

5. (Optional) Add one or more parameters to the report definition, as follows:
   1. Click **ADD PARAMETER**.
   2. 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	Select the data type of this parameter.

6. Click **APPLY**.
7. Click **SAVE**.

See also

Generating and viewing reports

20. Authentication tokens

Authentication tokens are unique keys that allow users to automate actions in Application Security, and use scripted processes to perform operations without revealing user names and passwords.

An authentication tokens 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, Application Security logs the operation under the account name used to create the token.

This section contains the following topics:

- Authentication token types
- Generating authentication tokens
- Editing authentication tokens
- Deleting authentication tokens

20.1. Authentication token types

There are several token types available, and each provides a different capability, usually for a small set of time-limited actions. For example, the AnalysisUploadToken token does not allow the user to sign in to the interface or view results. Common actions include uploading analysis results and downloading reports.

The following table describes the available token types.

Token type	Description
AnalysisDownloadToken	Gives the ability to download of merged result files.
AnalysisUploadToken	Gives the ability to upload analysis results to Application Security and to list applications.
AutomationToken	Gives access to most of the REST API endpoints permitted to its issuing user. Intended for use with longer-running automations. Max Usages: Unlimited Max Days to Live: 365 **Caution** Because of the access this token provides, and its maximum allowed lifetime, you must take extra care to secure it to reduce risk of API misuse or unintended use. OpenText strongly recommends that you evaluate the planned use of this token and ensure that you limit its life based on your environments' tolerance for risk.
CIToken	Allows integration of Application Security with continuous integration plugins.
PurgeProjectVersionToken	Gives the ability to programmatically request a list of all application versions, and to purge application versions.
ReportFileTransferToken	Typically created programmatically by automation scripts using the /fileTokens endpoint to enable 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
ScanCentralCtrlToken	For communications with the OpenText Fortify ScanCentral SAST client.
ToolsConnectToken	For use with OpenText Application Security Tools (Fortify Audit Workbench and Secure Code Plugins) that connect to Application Security for collaborative auditing, remediation, and uploading of analysis results.

Token type	Description
UnifiedLoginToken	Gives access to most of the REST API. It is intended for short-run automations that last less than a day.

20.2. Generating authentication tokens

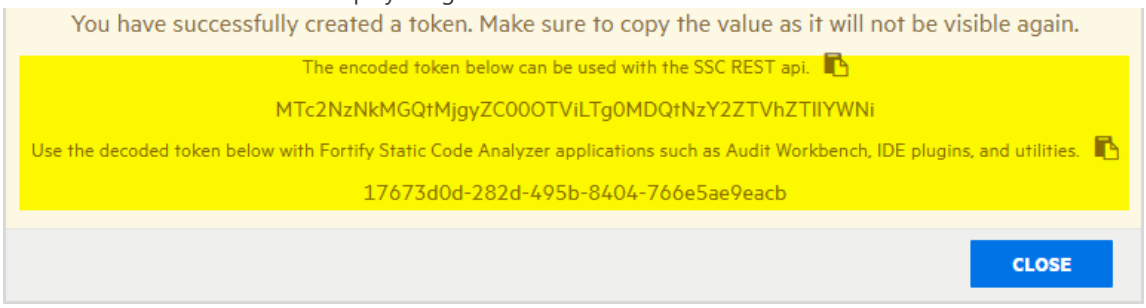
You can generate authentication tokens from either the **Administration** view in Application Security, or from the command line using the fortifyclient utility. Only you can see the details of your tokens. A Application Security Administrator can extend the life of a token you create, but not beyond the maximum days to live for that token.

Note

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 cannot use the token.

To generate an authentication token:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Users**, and then select **Token Management**.
3. Click **NEW** to open the **Create Token** dialog box.
4. From the **Token Type** list, select the type of token you want to create.
   For a list of available token types, see the table in Authentication token types.
   The **Create Token** dialog box displays a description of the selected token type.
5. Use the **Expiration** calendar to specify the date on which the token is to expire.
   The expiration time is set to the current time on the specified date. By default, the expiration date value is set to the maximum number of days to live for the selected token type. You can set this to an earlier date to give the token a shorter life.
6. In the **Description** box, type a description of the intended use of the new token.
7. Click **SAVE**.
   The **Create Token** dialog box displays a message to let you know the token was successfully created.
8. Copy either the encoded or decoded token string and save it.
   These token values will not be displayed again.



9. Click **CLOSE**.

The **Token Management** page lists the new token.

Authentication tokens are defined at runtime in `<ssc_deploy_dir>/WEB-INF/internal/serviceContext.xml`.

See also

Generating an authentication token from the command line

Specifying DaysToLive for fortifyclient authentication tokens

20.3. 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 header, select **Administration**.
2. On the navigation pane, expand **Users**, 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, click the **Expiration** calendar, and then specify a different expiration date.
   By default, the expiration date value is set to the maximum number of days to live for the selected token type. You can set this to an earlier date to give the token a shorter life.
6. Click **SAVE**.

See also

Generating authentication tokens

20.4. Deleting authentication tokens

To delete an authentication token that you no longer need or that is no longer usable:

1. On the header, select **Administration**.
2. On the navigation pane, expand **Users**, 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**.
4. Click **OK** to confirm that you want to delete the token.

See also

Generating authentication tokens

21. Fortify CLI (fcli) documentation

Fortify CLI (fcli) is a unified command-line interface tool that provides a consistent way to interact with various Fortify products, including OpenText™ Application Security, OpenText SAST, and OpenText Fortify DAST. Instead of using separate tools or APIs for each Fortify product, fcli offers a single, streamlined interface for performing common tasks such as managing applications and versions, uploading scan results, generating reports, and automating security workflows.

For OpenText™ Application Security users, fcli simplifies operations like creating and configuring application versions, managing artifacts and scans, querying vulnerabilities, and integrating Fortify into CI/CD pipelines. It is useful for automation scenarios, scripting, and DevSecOps workflows where you need to interact with OpenText™ Application Security features through scripts without manually using the web interface. The tool supports JSON output for easy parsing and integration with other systems, making it an essential utility for users who are looking to scale their application security testing and management processes.

The following are the references to fcli documentation:

- Repository: https://github.com/fortify/fcli
- Releases: https://github.com/fortify/fcli/releases
- Latest release: https://github.com/fortify/fcli/releases/tag/latest
- Documentation Home page: https://fortify.github.io/fcli/
- Latest Installation and Usage guide: https://fortify.github.io/fcli/latest/

22. Using the fortifyclient utility



Important
The `fortifyclient` feature is deprecated as of version 26.2 and will be removed in version 26.4.

You can use the fortifyclient utility to generate authentication tokens, securely transfer objects to and from Application Security, and purge application version artifacts from the command line.

This section contains the following topics:

- Preparing to use fortifyclient
- Listing fortifyclient commands and options
- Generating an authentication token from the command line
- Listing authentication tokens
- Invalidating tokens
- Listing application versions
- Uploading FPR files
- Downloading FPR files
- Purging application version artifacts
- Importing content bundles
- Downloading audit attachment files

22.1. Preparing to use fortifyclient

The fortifyclient utility is located in `<ssc_distribution_dir>/Tools/fortifyclient/bin/`.

To use fortifyclient, ensure you have the following information:

- All commands require the Application Security URL. See "host.url" in Application configuration options.
- The commands to generate tokens and list existing tokens require the credentials for a Application Security user account
- The command to invalidate tokens requires either user account credentials or an authentication token
- All other commands require an authentication token
  When fortifyclient uses an authentication token to perform an operation, Application Security logs the operation under the account name used to create the token.

See also

Downloading and unpacking Application Security files

22.1.1. fortifyclient HTTP timeouts

You can configure connect, read, and write HTTP timeouts for fortifyclient. The valid range for all timeouts is `1` to `2147483` seconds. The following table describes the environment variables you can use to change the HTTP timeouts.

Environment variable	Description
`FORTIFYCLIENT_CONNECT_TIMEOUT_SEC`	Specifies the HTTP connection timeout in seconds in which the client should establish a connection. The default value is `10` seconds.
`FORTIFYCLIENT_READ_TIMEOUT_SEC`	Specifies the HTTP read timeout in seconds in which the client should receive a response. The default value is `600` seconds.
`FORTIFYCLIENT_WRITE_TIMEOUT_SEC`	Specifies the HTTP write timeout in seconds in which the client should deliver a request body. The default value is `60` seconds.

22.2. Listing fortifyclient commands and options

To list the fortifyclient commands and options:

1. At the command prompt, type:
   `cd <ssc_distribution_dir>/Tools/fortifyclient/bin/` .
2. To list all the available commands, type `fortifyclient -h` .
3. To list all the options for a specific command, type `fortifyclient -h <command>` .

The fortifyclient utility command and option names are case-sensitive.

22.3. Generating an authentication token from the command line

Use the fortifyclient utility to generate an authentication token from the command line. You can use the credentials for any existing Application Security user account to create an authentication token. Authentication tokens inherit the permissions of the account type (Administrator, Security Lead, Manager, or Developer) of the user who creates the token.

The following example generates an authentication token to upload analysis results to Application Security:

```
fortifyclient token -url <host.url> -gettoken AnalysisUploadToken -user Developer1 -password <password>
```

See also

Authentication token types

Generating authentication tokens

22.3.1. Specifying the number of days before a token expires

You can use the `-daysToLive` option when you create an authentication token to specify the number of days before it expires.

The following example command generates an analysis upload token that expires after two days:

```
fortifyclient token -url <host.url> -gettoken AnalysisUploadToken -user Developer1 -password <password> -daysToLive 2
```

You must type the case-sensitive `daysToLive` parameter exactly as shown in the previous example.

See also

Generating an authentication token from the command line

22.4. Listing authentication tokens

Application Security administrators can use fortifyclient to list all existing authentication tokens for all Application Security user accounts. The fortifyclient utility does not support filtering the list of tokens by Application Security account name or account privilege level.

The following example command lists the authentication tokens that exist for all user accounts:

```
fortifyclient listtokens -url <host.url> -user Admin1 -password <password>
```

The fortifyclient utility returns a list that includes the token ID, owner, creation date, and expiration date for all authentication tokens.

Note

The utility does not list session tokens, which are tokens associated with a session Application Security created automatically.

22.5. Invalidating tokens

You can invalidate an existing authentication token by deleting it from the Application Security user interface or by running the `invalidatetoken` command. You can invalidate all tokens for a specific user account, a single token by specifying a token ID and user credentials, or a single token by specifying a token value.

The following example command deletes all authentication tokens for a specific user account:

```
fortifyclient invalidatetoken -url <host.url> -invalidateForUser -user Developer1 -password <password>
```

The following example command deletes an existing authentication token for a specific user account by specifying a token ID:

```
fortifyclient invalidatetoken -url <host.url> -invalidateByID <token_ID> -user Developer2 -password <password>
```

The following example command invalidates an existing authentication token by specifying a token value:

```
fortifyclient invalidatetoken -url <host.url> -invalidate <token>
```

See also

Listing authentication tokens

Deleting authentication tokens

22.6. Listing application versions

You can use fortifyclient to list the Application Security application versions accessible by the account that was used to create a particular authentication token.

Note

Administrators can view all application versions. Security Leads can view all application versions they created or to which they have been granted access. Managers and Developers 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 Generating an authentication token from the command line.)

The following example command lists the application version identifiers, application names, and application versions for a specific user account:

```
fortifyclient listApplicationVersions -url <host.url> -authtoken <token>
```

The fortifyclient utility lists the application version ID, application name, and version for all application versions accessible to the user account that created the token.

See also

Generating an authentication token from the command line

22.7. Uploading FPR files

Users periodically upload application analysis results files (in FPR format) to Application Security. To do this from the command line, you must have an authentication token. You can upload an FPR file by specifying either the application identifier or the application name and version.



Note

When naming an FPR, only a limited set of characters is supported. Ensure to use supported characters and avoid unsupported characters in file names.

Supported characters

- Uppercase and lowercase letters (`A–Z` , `a–z`)
- Numbers (`0–9`)
- Periods (`.`)
- Dashes (`-`)
- Underscores (`_`)

Unsupported characters

- Special character `#`

If a special character is used, it is automatically replaced with an underscore (`_`). This replacement does not change the meaning or integrity of the FPR.

Examples

Upload an FPR file to Application Security using an application version identifier:

```
fortifyclient uploadFPR -url <host.url> -authtoken <token> -file MyScan.fpr -applicationVersionID <id>
```

Upload an FPR file to Application Security using an application name and version:

```
fortifyclient uploadFPR -url <host.url> -authtoken <token> -file MyScan.fpr -application MyApp -applicationVersion 1.0
```

See also

Generating an authentication token from the command line

Listing application versions

22.8. Downloading FPR files

You can use fortifyclient to download FPR files by specifying either the application version identifier or the application name and version.

Examples

Download an FPR file from Application Security using an application version identifier:

```
fortifyclient downloadFPR -url <host.url> -authtoken <token> -file MyScan.fpr -applicationVersionID <id>
```

Download an FPR file from Application Security using an application name and version:

```
fortifyclient downloadFPR -url <host.url> -authtoken <token> -file MyScan.fpr -application MyApp -applicationVersion 1.0
```

See also

Generating an authentication token from the command line

Listing application versions

22.9. Purging application version artifacts

You can purge all the artifacts associated with an application version that were scanned before a specified date.

The following example command purges all artifacts from an application version that were scanned before MMMM dd, yyyy:

```
fortifyclient purgeApplicationVersion -url <host.url> -authtoken <token> -application MyApp -applicationVersion 1.0 -scanDate
```

`MMddyyyy`

You can also specify the application version using an application version identifier.

See also

Generating an authentication token from the command line

Listing application versions

22.10. Importing content bundles

OpenText periodically provides security content bundles (as ZIP files) that contain one or more issue templates or report definitions.

The following example command imports a security content bundle into Application Security:

```
fortifyclient import -url <host.url> -authtoken <token> -bundle bundle.zip
```

22.11. Downloading audit attachment files

The following example command downloads an audit attachment file from Application Security:

```
fortifyclient downloadAttachment -url <host.url> -authtoken <token> -file xyz.png -attachmentId
<attachment_id>
```

23. Authoring bug tracker plugins

Application Security supports integration with external bug tracking applications, which enables users to log bugs for issues as they audit them. As delivered, the system can integrate with Jira, ALM, and Azure DevOps Server. For specific versions supported, see the *Application Security Software System Requirements* document. If your company uses a different bug tracking system, you can author a new plugin for it. This section provides information about how to author and deploy a custom bug tracker plugin.

Note

In this Helpguide and in the Application Security user interface, the terms *bug* and *defect* are used interchangeably.

Important

OpenText 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_distribution_dir>/Samples/<bugtracker_plugin_name>/`

This section contains the following topics:

- Use case
- Component setup
- Implementation
- Plugin methods and method calls
- Plugin helper
- Error handling
- Almost stateless
- Debugging a bug tracker plugin
- Deploying a customized bug tracker plugin

23.1. Use case

As a Application Security Administrator, you can configure an external bug tracking system to use with a given application version, as described in About Bug Tracker integration. Application Security 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 access 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.

23.2. Component setup

The bug tracker plugin can be an independent component that you write using your preferred IDE.

Configure a bug tracker plugin with the following dependencies:

- Plugin must implement a public API defined and distributed in `fortify-public-<version>.jar` (required)
- Apache Commons Logging (optional)
- Apache Commons Lang (optional)

You can use your preferred build system to build your distributable.



Note

If a plugin has any dependencies on JavaEE packages, the plugin developer must bundle the necessary JavaEE JAR files into the plugin's own library path, and must not rely on these packages being available from the Java™ Runtime Environment. The JavaEE modules were deprecated with Java 9. Such packages include JAXB API and implementation, javax.activation, javax.annotation, javax.transaction, javax.xml.ws, and CORBA-related packages.

23.3. Implementation

Application Security versions that use the plugin framework require that all plugins implement the `com.fortify.pub.bugtracker.plugin.BatchBugTrackerPlugin` interface. OpenText strongly recommends that your implementation class extends `com.fortify.pub.bugtracker.plugin.AbstractBatchBugTrackerPlugin` so that you can take advantage of any backward-compatibility support that becomes available in future releases.

The BatchBugTrackerPlugin interface, which is an extension of the BatchBugTrackerPlugin is as follows:

```
public interface BatchBugTrackerPlugin extends BugTrackerPlugin {
        public void addCommentToBug (Bug bug, java.lang.String comment,
          UserAuthenticationStore credentials);
        public Bug fileMultiIssueBug (MultiIssueBugSubmission bug,
          UserAuthenticationStore credentials);
        public java.util.List<BugParam> getBatchBugParameters (UserAuthenticationStore credentials);
        public boolean isBugClosed (Bug bug, UserAuthenticationStore credentials);
        public boolean isBugClosedAndCanReOpen (Bug bug, UserAuthenticationStore credentials);
        public boolean isBugOpen (Bug bug, UserAuthenticationStore credentials);
        public java.util.List<BugParam> onBatchBugParameterChange
          (java.lang.String changedParamIdentifier, java.util.List<BugParam> currentValues,
          UserAuthenticationStore credentials);
        public void reOpenBug (Bug bug, java.lang.String comment, UserAuthenticationStore credentials);
}
```

The BugTrackerPlugin interface, which is the base interface of the BatchBugTrackerPlugin (maintained separately for backward compatibility) is as follows:

```
public interface BugTrackerPlugin {
        public boolean requiresAuthentication();
        public List<BugTrackerConfig> getConfiguration();
        public void setConfiguration(Map<String, String> configuration);
        public void testConfiguration(UserAuthenticationStore credentials);
        public String getShortDisplayName();
        public String getLongDisplayName();
        public List<BugParam> getBugParameters(IssueDetail issueDetail,
          UserAuthenticationStore credentials);
        public List<BugParam> onParameterChange(IssueDetail issueDetail, String changedParamIdentifier,
          List<BugParam> currentValues, UserAuthenticationStore credentials);
        public Bug fileBug(BugSubmission bug, UserAuthenticationStore credentials);
        public void validateCredentials(UserAuthenticationStore credentials);
        public Bug fetchBugDetails(String bugId, UserAuthenticationStorecredentials);
        public String getBugDeepLink(String bugId);
}
```

23.4. Plugin methods and method calls

The following table lists the methods and calls to use with your plugin.

Method or call	Description
requiresAuthentication	This method is expected to return `true` if it requires the framework to request credentials from the user for any bug-tracking operation. This returns `true`, except when the plugin gets its credentials using a different mechanism, such as from the credential store or if the plugin interacts with the bug-tracking system asynchronously and not in real time. If the method returns `false`, the system passes null for all the `UserAuthenticationStore` parameters of the plugin methods.
getBatchBugParameters	Used by the plugin framework to get the list of bug parameters the plugin needs to submit batch bugs. Provides default or null values. The `BugTrackerPlugin.setConfiguration(java.util.Map)` method is called on the plugin instance before this method is invoked. Parameter choice lists and defaults can be made dynamic by having the implementation go to the bug tracking system to determine the list of valid choices.
getConfiguration	The plugin framework uses this method to get metadata about the questions to be presented to the user during plugin configuration. The return value is a list of BugTrackerConfig objects that provide required information about the configuration item. Each item corresponds to a text box in the user interface. The value field of each item specifies the default value for the text box.
setConfiguration (call)	After you select the bug-tracking system for the application version and save the configuration to the database, all future interactions with the plugin are preceded by the `setConfiguration` call, which sets the configuration for the plugin using which operations are to be carried out.
testConfiguration (call)	The plugin framework uses the `testConfiguration` call to test the configuration previously set using the `setConfiguration` call. This method is expected to hit the bug-tracking system using the configuration details set and validate them to the fullest extent possible. The user credentials are fetched from the user if this plugin declared that it requires authentication.

Method or call	Description
getShortDisplayName	The `getShortDisplayName` method returns a short display name for the plugin. This string populates the list of available bug tracker plugins. **Important** If you customize the sample bug-trackers code that Application Security provides, but you use the same plugin classname, do not change the short display name of the plugin. (For consistency, also avoid changing the long display name.) If you *do* change the name of the main implementation class, then you must also change the display name(s) for the plugin.
getLongDisplayName	The `getLongDisplayName` method returns 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. **Important** If you customize the sample bug-trackers code that Application Security provides, but you use the same plugin classname, do not change the short display name of the plugin. (For consistency, also avoid changing the long display name.) If you *do* change the name of the main implementation class, then you must also change the display name(s) for the plugin.

Method or call	Description
getBugParameters	The `getBugParameters` method returns metadata about the bug parameters to present to users. Application Security supports the following three bug parameter types: • BugParamText translates to a text box. • BugParamTextArea translates to a multiple-line text box and is typically used for bug descriptions. • BugParamChoice translates to a list. • The `issueDetail` object encompasses the details of the issue for which the user is attempting to log a bug. This defaults to several bug parameters such as the description and summary, which can be extracted from this object. The pluginHelper protected member has a helper method to build a suggested default bug description. (See Plugin Helper.)

onBatchBugParameterChange	If a user changes the value of a parameter in the user interface, this method fetches the updated choice list for other batch bug parameters. The `BugTrackerPlugin.setConfiguration(Map)` method is called on the plugin instance before this method is invoked. If the `BugParamChoice.getHasDependentParams()` attribute for a plugin bug parameter is set to `true`, then this method is called whenever the parameter value changes in the user interface layer.
	Recommendations:
	• Act on each bug parameter that has dependent parameters.
	• Do not forget to handle the case in which a parameter value changes to null (no selection made).
	• Do not forget to set the parameter value in return list to null when its choices change.
	• Before you add a new parameter, ensure that it is not already in the return list.
	• Return null if there is no change
	• Use either of the following strategies:
	  ○ Modify the `currentValues` parameter and return it.
	  ○ Construct the return value from the raw parameters maintained. Set the values and choice lists before returning.

Method or call	Description

onParameterChange	The plugin framework calls the `onParameterChange` method whenever the value for a bug parameter marked as `hasDependentParams` (see BugParamChoice class javadoc) changes. This method can take action and return a new list of bug parameters to display.
	Keep the following guidelines in mind:
	• Act on each bug parameter that has dependent parameters.
	• Do not forget handling case when parameter value changes to null (no selection made).
	• Do not forget to set the parameter value in a return list to null when its selections change.
	• Before you add a new parameter, check the return list to ensure that it does not already include the parameter.
	• Return null if there is no change.
	• Use one of the following strategies:
	  ○ Modify the `currentValues` parameter and return it.
	  ○ Construct the return value from raw parameters maintained. Set values and choice lists before returning.

fileBug	This method files a bug on the external bug-tracking system. The `BugSubmission` object passed encompasses all bug details. Ensure that you correctly differentiate between the `bug.getIssueDetail()` object and the `bug.getParams()` object. The `bug.getIssueDetail()` object returns details of the issue, whereas the `bug.getParams()` object returns the bug parameter values that the user provides. If you added Bug Description as a user-editable bug parameter, then fetch the bug description from the `bug.getParams()` object instead of from the `bug.getIssueDetail()` object. The return value of the fileBug object must be a bugId, which can be used to fetch the bug with the `fetchBug` method and formulate the deep link with the `getBugDeepLink` method. Use fields in B`ugSubmission.getIssueDetail()`, namely `getLastBuildWithoutIssue()`, `getDetectedInBuild()`, and `getFileName()` to perform changeset discovery if you have access to your repository.

Method or call	Description
fileMultiIssueBug	File bugs that contain multiple issues on the bug tracking system. The `BugTrackerPlugin.setConfiguration(Map)` method is called on the plugin instance before this method is invoked. Recommendations: • Application Security provides the summary and description obtained using `MultiIssueBugSubmission.getIssueDetails()`. The user does not supply these values. If you added the summary and description as bug parameters, use `bug.getParams()` to retrieve the user-supplied values. • If you have access to your repository, use the `getLastBuildWithoutIssue()`, `getDetectedInBuild()`, and `getFileName()` fields in `MultiIssueBugSubmission.getIssueDetails()` to perform changeset discovery.
fetchBug	This method fetches the current bug status.
getBugDeepLink	This method formulates 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.

23.5. Plugin helper

If your bug tracker plugin class extended from the class **AbstractBatchBugTrackerPlugin** provided, you will find a protected member **BugTrackerPluginHelper** available. You can use this helper object to perform frequently used plugin operations for locating parameters, loading default values, and so on. See the javadoc for more details. Also look at its usage in the plugin samples.

23.6. 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. Examples are invalid configuration, errors arising from the bug tracking system, bug tracking system failing, and so on. The message with this exception is relayed 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.

23.7. Almost stateless

With every top-level request that Application Security 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. Application Security does not cache or reuse plugin instances across plugin operations. New states must be opened

on each call and cleaned up before method exit.

23.8. Debugging a bug tracker plugin

The plugins support Apache Commons logging. The resulting logs are appended into the `ssc_plugins.log` file located in the `<fortify.home>/<app_context>/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.

23.9. Deploying a customized bug tracker plugin

To deploy a customized bug tracker plugin, build a JAR file that contains the plugin classes and any of its dependent classes.

The following example script builds a bug tracker plugin with Gradle:

```
 apply plugin: 'java'sourceCompatibility = '1.8'
targetCompatibility = '1.8'
dependencies {
 compile fileTree(dir: 'lib', include: '*.jar')
}
jar.enabled = false // There is no need to generate a default non-osgi jar during build.
clean {
 delete "${projectDir}/dist"
}
task pluginJar(type: Jar) {
 baseName "com.fortify.BugTrackerPluginAlm"
 from sourceSets.main.output
 destinationDir = file("${projectDir}/dist")
 manifest {
  from "${projectDir}/META-INF/MANIFEST.MF"
 }
 from(projectDir) {
  include "plugin.properties"
  include "plugin.xml"
 }
 into("lib") {
  from "${projectDir}/lib"
  include "*.jar"
  exclude "fortify-public*.jar"
 }
}
build.dependsOn(pluginJar)
```

Important

If you customize the sample bug tracker code that comes with Application Security, 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_distribution_dir>/Samples/<bugtracker_plugin_name>/README` file.

See also

Authoring bug tracker plugins

24. Advanced configuration

This section covers advanced configuration topics for Administrators.

This section contains the following topics:

- Automating Application Security configuration
- Application configuration options

24.1. Automating Application Security configuration

You can automate Application Security configuration before deployment using the autoconfig file. This file includes sections for each configurable aspect of Application Security. The autoconfig file enables automated deployment by providing settings and seed bundles for silent Application Security update and installation. You can use the autoconfig file to automate all Setup wizard tasks. The Setup wizard picks up this file at server startup and automates the entire installation.



Note

The `datasource.properties` file and some database fields contain encrypted entries that rely on the `secret.key` file. So, if you are moving your Application Security instance from one computer to another, you must also move the `secret.key` file (not just your properties file).

To automate Application Security configuration:



Important

To automate the configuration in a root context, see Automating configuration in a root context.

1. Open a text editor and create a file named `<app_context>.autoconfig`, where <*app_context*> is the application server context in which Application Security is deployed (the name of the directory created under `<fortify.home>`).

   Note

   Ensure that all lines in the autoconfig file, including the last line uses proper line termination according to the expected format (for example, LF or CRLF). Improper or inconsistent line endings may lead to parsing errors, unexpected behavior, or configuration processing failures.

2. Add the following to the `<app_context>.autoconfig` file in the YAML format shown.

   Note

   - Make sure that properties in the `autoconfig` file are indented correctly under the relevant sections according to YAML syntax.
   - Copy only the database properties for the database engine you use, and ensure that you remove the hash symbol (#) before each property you want to use.
   - For a fresh installation that uses `autoconfig`, you must specify both `init.admin.email` and `init.admin.password` in the `appProperties` section so that initial seeding can create the admin user. If no admin user exists and these values are missing, initialization fails. If the admin user already exists, these properties are optional, and the values are ignored.
   - Password strength is enforced by the `password.strength.min.score` property, which defaults to `3` (see, Application configuration options). For information about the `zxcvbn4j` library used to check password strength, see Setting the required password strength for Application Security sign in.

```
appProperties:
 # Include any property found in <fortify.home>/<app_context>/conf/app.properties
 # For example, host.url: 'https://ssc.example.com/ssc/'
 # searchIndex.location: '/home/<app_context>/search_index'
 # host.validation: false
 # Required for fresh installations that use autoconfig and do not already have an admin user:
   init.admin.email: admin@example.com
   init.admin.password: <strong_password>
datasourceProperties:
 # Include any property found in <fortify.home>/<app_context>/conf/datasource.properties
 # For example:
 # db.username: ssc_db_admin_username
 # db.password: ssc_db_admin_password
 # MSSQL Server database
 # jdbc.url: 'jdbc:sqlserver://mssql-host:1433;database=ssc_db;sendStringParametersAsUnicode=false'
 # MySQL Server database
 # jdbc.url: 'jdbc:mysql://mysql-host:3306/ssc_db?
sessionVariables=collation_connection=latin1_general_cs&rewriteBatchedStatements=true'
 # Oracle database
 # jdbc.url: 'jdbc:oracle:thin:oracle-host:1521:ssc_db'
dbMigrationProperties:
 # Enable automatic database migration
 # migration.enabled: true
 # Optionally specify alternative migration credentials
 # migration.username: ssc_db_admin_username
 # migration.password: ssc_db_admin_password
seeds:
 # Modify the path to the appropriate location for your environment
 - '/home/ssc/bundles/Fortify_Process_Seed_Bundle-2025_Q2_<build>.zip'
 - '/home/ssc/bundles/Fortify_PCI_Basic_Seed_Bundle-2025_Q2_<build>.zip'
 - '/home/ssc/bundles/Fortify_PCI_SSF_Basic_Seed_Bundle-2025_Q2_<build>.zip'
 - '/home/ssc/bundles/Fortify_Report_Seed_Bundle-2025_Q2_<build>.zip'
```

3. Save the `<app_context>.autoconfig` file in the `<fortify.home>/` directory.
4. Place a copy of the `fortify.license` file in your `<fortify.home>/` directory.
5. Ensure that the WAR file name is `<app_context>.war` .
6. Start Tomcat server.

After the auto-configuration is complete, Application Security computes the effective configuration checksum and saves it in the `version.properties` file as the value for the `autoconfig.checksum` property.

When Application Security starts with the `autoconfig` file present, it computes an effective configuration checksum and compares it to the checksum stored in the `version.properties` file. If the checksums do not match, Application Security runs a lightweight auto-configuration, and updates the `autoconfig.checksum` value.

If the auto-configuration fails for any reason, Application Security is put to maintenance mode (`maintenance.mode=true` in the `version.properties` file, which forces either full auto-configuration or the display of the Setup wizard on the next server startup.

The checksum includes:

- Effective properties from autoconfig `appProperties` key
- Effective properties from autoconfig `datasourceProperties` key
- File names from effective autoconfig `seeds` key
- All properties in the `conf/app.properties` file
- All properties in the `conf/datasource.properties` file

Properties from `dbMigrationProperties` are not included in the checksum.

Application Security performs the complete automatic configuration only if it is not fully configured. Application Security performs lightweight auto-configuration only if the checksums do not match, but it is otherwise already configured.

Lightweight auto-configuration skips database migration (regardless of the settings in the `autoconfig` file) and it skips the initial internal bundle seeding. The seeding of bundles provided by the autoconfig `seeds` key is still performed.

24.1.1. Automating configuration in a root context

To automate Application Security configuration in a root context:

1. Open a text editor and create a file named `_default_.autoconfig`.
2. Add the following to the `_default_.autoconfig` file in the YAML format shown.



Note

- Make sure that properties in the `autoconfig` file are indented correctly under the relevant sections according to YAML syntax
- Copy only the database properties for the database engine you use, and ensure that you remove the hash symbol (#) before each property.
- For a fresh installation that uses `autoconfig`, you must specify both `init.admin.email` and `init.admin.password` in the `appProperties` section so that initial seeding can create the admin user. If no admin user exists and these values are missing, initialization fails. If the admin user already exists, these properties are optional, and the values are ignored.
- Password strength is enforced by the `password.strength.min.score` property, which defaults to `3` (see, Application configuration options). For information about the `zxcvbn4j` library used to check password strength, see Setting the required password strength for Application Security sign in.

```
appProperties:
 # Include any property found in <fortify.home>/_default_/conf/app.properties.
 # For example, host.url: 'https://ssc.example.com/'
 # searchIndex.location: '<fortify.home>/_default_/index'
 # host.validation: false
 # Required for fresh installations that use autoconfig and do not already have an admin user:
   init.admin.email: admin@example.com
   init.admin.password: <strong_password>
datasourceProperties:
 # Include any property found in <fortify.home>/_default_/conf/datasource.properties.
 # For example:
 # db.username: ssc_db_admin_username
 # db.password: ssc_db_admin_password
 # MSSQL database
 # jdbc.url: 'jdbc:sqlserver://mssql-host:1433;database=ssc_db;sendStringParametersAsUnicode=false'
 # MySQL database
 # jdbc.url: 'jdbc:mysql://mysql-host:3306/ssc_db?
sessionVariables=collation_connection=latin1_general_cs&rewriteBatchedStatements=true'
 # Oracle database
 # jdbc.url: 'jdbc:oracle:thin:oracle-host:1521:ssc_db'
dbMigrationProperties:
 # Enable automatic database migration
 migration.enabled: true
 # Optionally specify alternative migration credentials
 # migration.username: ssc_db_admin_username
 # migration.password: ssc_db_admin_password
seeds:
 # Modify the path to the appropriate location for your environment
 - '/home/ssc/bundles/Fortify_Process_Seed_Bundle-2025_Q2_<build>.zip'
 - '/home/ssc/bundles/Fortify_PCI_Basic_Seed_Bundle-2025_Q2_<build>.zip'
 - '/home/ssc/bundles/Fortify_PCI_SSF_Basic_Seed_Bundle-2025_Q2_<build>.zip'
 - '/home/ssc/bundles/Fortify_Report_Seed_Bundle-2025_Q2_<build>.zip'
```

The values for `init.admin.email` and `init.admin.password` are consumed during seeding. Application Security keeps these values in memory and does not write them to property files or logs.

3. Save the `_default_.autoconfig` file in the `<fortify.home>` directory.
4. Place a copy of the `fortify.license` file in your `<fortify.home>` folder.
5. Rename the `ssc.war` file to `ROOT.war`.
6. Start Tomcat server.

See also

Automating Application Security configuration

24.2. Application configuration options

Administrators can update Application Security configuration settings in the `<fortify.home>/<app_context>/conf/app.properties` file or the `appProperties` section of an **autoconfig** file used to automate the Application Security configuration.

Property name	Description
Application Security URL	
host.url	Specifies the web address for accessing Application Security (Automating Application Security configuration)
host.validation	If set to `true`, enables HTTP host validation against the `host.url` value (Automating Application Security configuration). The default is `false`.
Global search	
searchIndex.location	Specifies the absolute path to the full text index directory on local file system (Automating Application Security configuration)
Background job execution	
jobs.threadCount	Specifies the size of the job processing thread pool (Partitioning an Oracle database for improved performance). The default value is `10`.
job.exclusiveJobOverheadPercentage	Specifies a percentage by which to reduce the `jobs.threadCount` value when an exclusive job is running such as artifact purge, artifact delete or app version delete. The default value is `20`. The valid values are `0` to `100`.
job.numberOfDedicatedDataExports	Specifies the number of job processing threads reserved for data exports. The default value is `2`.
job.numberOfConcurrentReports	Specifies the maximum number of concurrent report jobs that can run at the same time. The default value is `2`.
job.numberOfConcurrentExclusiveJobs	Specifies the maximum number of concurrent exclusive jobs that can run at the same time. The default value is `1`.
Authentication	

password.strength.min.score	Specifies the minimum acceptable strength score for saving a new password (Setting the required password strength for Application Security sign in). The default value is `3`.
sso.localAuthenticationEnabled	If set to `true`, allows local password authentication for use with X.509 SSO (About configuring Application Security to work with single sign-on). The default is `false`.
LDAP cache	
ldap.cache.persistence.enabled	If set to `true`, Application Security stores the ldap cache in the database for faster startup (Enabling persistence of the LDAP cache). The default is `true`.
ldap.cache.refresh.interval.hours	Specifies the cache refresh interval (in hours) (Enabling persistence of the LDAP cache). The default is `1 hour`. The valid values are `1` to `12`.
Audit issue history	
issue.attrChangelog.enabled	If set to `true`, enables the audit issue history feature (Enabling audit issue history). The default is `false`.

24.2.1. Configuring background job execution strategy

The following table describes how to replicate the background job execution strategies that existed prior to Application Security version 25.2.0.

Legacy job execution strategy	Description	Configuration instructions
Conservative	Balances job concurrency, throughput, and job stability.	No changes required.
Aggressive	Enables high concurrency. With this strategy, the job scheduler does not enforce any limitations on how jobs are executed. All jobs are equal and executed on all available workers. OpenText does not recommend using this job execution strategy.	• Set `job.exclusiveJobOverheadPercentage` to `0`. • Set `job.numberOfConcurrentReports` to the same value as the `jobs.threadCount` value. OpenText recommends using a smaller value than the `jobs.threadCount` value or the default value of `2` to increase scan processing throughput and reduce peak memory that report generation can consume. • Set `job.numberOfConcurrentExclusiveJobs` to the same value as the `jobs.threadCount` value. OpenText recommends that you use the default value of `1` to increase scan processing throughput and avoid lock contention in the database.
Exclusive jobs	Enables jobs to run in sequence and one at a time. OpenText does not recommend using this job execution strategy.	• Set `jobs.threadCount` to `1`. • Set `job.numberOfDedicatedDataExports` to `0`.

25. Webhook payloads

Every webhook payload contains the following fields:

- events—Webhook event list (information about events triggered)
- sscUrl—URL address of the server
- webhookId—Associated webhook ID
- triggeredAt—Date on which the payload was created in (created and stored in the database)

Example:

```
{
  "events":[
  {
    "event":"ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS",
    "artifactId":1,
    "projectVersionId":1,
    "filename":"file.fpr",
    "username":"testUser1"
  }
  ],
  "triggeredAt":"2020-08-21T12:19:24.502+0000",
  "sscUrl":"http://localhost:8180/ssc",
  "webhookId":1
}
```

This section contains the following topics:

- Event payloads
- Artifact upload payload
- Project version payload
- Report generation payload
- User payload

25.1. Event payloads

An "events" array is filled with actual event payloads, which are described below. Every event has an "event" field that describes the event type.



Note

Currently, there is just one event in an array. Event aggregation is not supported.

25.2. Artifact upload payload

Payloads generated for artifact events include the following fields:

- artifactId—ID of uploaded artifact
- projectVersionId—ID of the application version to which the artifact was uploaded
- filename—Artifact filename
- username—Username of the user who uploaded the event
- event—Artifact upload event type
  Upload event types:
  - ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS
  - ANALYSIS_RESULT_UPLOAD_FAILURE
  - ANALYSIS_RESULT_UPLOAD_REQUIRES_APPROVAL
  - ANALYSIS_RESULT_INDEXING_COMPLETED

Example:

```
{
  "event":"ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS",
  "artifactId":1,
  "projectVersionId":l,
  "filename":"file.fpr",
  "username":"testUser1"
}
```

Artifact upload approved payload

This is an extension of the artifact upload payload, and contains additional fields to identify the approving user and the approval comment.

Fields:

- artifactId—ID of uploaded artifact
- projectVersionId—ID of application version to which the artifact was uploaded
- filename—Artifact filename
- username—Username of uploading user
- approvalUsername—Approving user's username
- approvalComment—Comment submitted with approval

Example:

```
{
  "event":"ANALYSIS_RESULT_UPLOAD_APPROVED",
  "artifactId":1,
  "projectVersionId":1,
  "filename":"file.fpr",
  "username":"testUser1",
  "approvalUsername":"testUser2",
  "approvalComment":"upload has been approved"
}
```

25.3. Project version payload

Payloads generated for application version events include the following fields:

- projectId—Application ID
- projectName— Application name
- projectVersionId—Application version ID
- projectVersionName—Application version name
- event—Application version event type
  Event types:
  - APP_VERSION_CREATED
  - APP_VERSION_UPDATED
  - APP_VERSION_DELETED

Example:

```
{
  "event":"APP_VERSION_CREATED",
  "projectId":1,
  "projectName":"Test application",
  "projectVersionId":1,
  "projectVersionName":"vl"
}
```

Project version updated payload

This is an extension of the project version payload, and contains additional fields to identify changes made.

Fields:

- projectId—Application ID
- projectName—Application name
- projectVersionId—Application version id
- projectVersionName—Application version name
- event—APP_VERSION_UPDATED
- changes—Value list that defines what changed in application version
  Available values:
  - ACTIVE—If application version "active" status has changed
  - COMMITTED—If application version was committed or uncommitted
  - PROJECT_VERSION_NAME—If application version name changed
  - PROJECT_TEMPLATE—If issue template has changed
  - ATTRIBUTES—If business/technical attributes changed
  - USER_ACCESS_ADDED—If one or more users were added to application version
  - USER_ACCESS_REMOVED—If one or more users were removed from application version
  - CUSTOM_TAG—If application version had custom attribute added or removed
  - PRIMARY_TAG—If primary tag of application version has changed

Example:

```
{
  "event" APP_VERSION_UPDATED",
  "projectId":1,
  "projectName":"Test application",
  "projectVersionId":1,
  "projectVersionName":"v1",
  "changes":["ACTIVE","COMMITTED"]
}
```

Project version created from previous payload

This is an extension of the project version updated payload. In this case, the configuration values of an existing application version were copied over to a new application version. The payload contains additional information about the application version on which the new application version is based.

Fields:

- projectId—ID of the parent application
- projectName—Name of the parent application
- projectVersionId—(child) Application version ID
- projectVersionName—Application version name

- previousProjectId—ID of the (parent) application
- previousProjectName—Name of the (parent) application
- previousProjectVersionId—ID of the (parent) application version
- previousProjectVersionName—Name of the (parent) application version
- event—APP_VERSION_CREATED

Example:

```
{
  "event":"APP_VERSION_CREATED",
  "projectId":1,
  "projectName":"Test application",
  "projectVersionId":2,
  "projectVersionName":"v2",
  "previousProjectId":1,
  "previousProjectName":"Test application",
  "previousProjectVersionId":1,
  "previousProjectVersionName":"v1"
}
```

25.4. Report generation payload

Payloads generated for report events.

Fields:

- reportId—ID of the requested report
- reportName—Name specified for report generation
- renderingEngine—Report rendering engine
- reportType—Report type
- event—Type of the report generation event
  Available values:
  - REPORT_GENERATION_COMPLETE
  - REPORT_GENERATION_REQUESTED

Example:

```
{
  "event":"REPORT_GENERATION_COMPLETE",
  "reportId":1,
  "reportName":Test report",
  "renderingEngine":"BIRT",
  "reportType":"PROJECT"
}
```

25.5. User payload

Payloads generated for user lifecycle events.

Fields:

- id—User id
- username—User's username
- event—User event
  - USER_CREATED - Authentication entity (LOCAL_USER, LOCAL_GROUP, LDAP_USER, LDAP_GROUP, or LDAP_ORGANIZATIONAL_UNIT) was created in Application Security.

    - USER_DELETED - Authentication entity (LOCAL_USER, LOCAL_GROUP, LDAP_USER, LDAP_GROUP, or LDAP_ORGANIZATIONAL_UNIT) was deleted from Application Security.
    - USER_UPDATED - Authentication entity (LOCAL_USER, LOCAL_GROUP, LDAP_USER, LDAP_GROUP, or LDAP_ORGANIZATIONAL_UNIT) was updated in Application Security.
    - LOCAL_USER_ACCOUNT_LOCKED
- userType—Type of user
  Available types:
    - LOCAL_USER
    - LOCAL_GROUP
    - LDAP_USER
    - LDAP_GROUP
    - LDAP_ORGANIZATIONAL_UNIT

Example:

```
{
  "id":1,
  "username":"testUser",
  "event":"USER_CREATED",
  "userType":"LOCAL_USER"
}
```

© Copyright 2026 Open Text

For more info, visit https://docs.microfocus.com