

OpenText™ Application Security (Fortify Software Security Center)

Software Version: 25.2.0

User Guide

Document Release Date: May 2025

Software Release Date: May 2025

Legal notices

Open Text Corporation

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

Copyright notice

Copyright 2008 - 2025 Open Text.

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

Trademark notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation updates

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

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

This document was produced for OpenText™ Application Security CE 25.2 on May 28, 2025.

Contents

| | |
|---|----|
| Preface | 17 |
| Contacting Customer Support | 17 |
| For more information | 17 |
| Product feature videos | 17 |
| Change log | 18 |
| Chapter 1: Introduction | 23 |
| Product name changes | 23 |
| Audience | 24 |
| Document structure | 24 |
| Related documents | 24 |
| All products | 25 |
| OpenText ScanCentral DAST | 25 |
| Fortify ScanCentral SAST | 26 |
| Fortify Software Security Center | 26 |
| OpenText SAST | 27 |
| OpenText Application Security Tools | 27 |
| OpenText DAST | 28 |
| Fortify WebInspect Enterprise | 30 |
| Chapter 2: System requirements | 32 |
| Hardware requirements | 32 |
| Database hardware requirements | 32 |
| Database performance metrics | 33 |
| Supported platforms and architectures | 33 |
| Supported application server | 34 |
| Database requirements | 34 |
| Kubernetes cluster deployment requirements (optional) | 36 |
| Kubernetes cluster requirements | 36 |
| Locally-installed tools required | 36 |
| Additional requirements | 36 |

| | |
|---|--------|
| Browsers | 37 |
| Supported authentication systems | 37 |
| Single sign-on (SSO) | 37 |
| BIRT report requirements | 38 |
| Installing required fonts (Linux only) | 38 |
| Installing required libraries (non-GUI Linux only) | 38 |
| Supported service integrations | 38 |
| Fortify Project Results (FPR) file compatibility | 39 |
| Acquiring the software | 40 |
| Verifying software downloads | 40 |
| Preparing your system for digital signature verification | 40 |
| Virtual Machine support | 41 |
| Chapter 3: Providing for secure deployment | 42 |
| Securing access to facilities | 42 |
| Securing Tomcat server | 42 |
| Using secure cipher suites | 43 |
| Setting Tomcat server attributes to protect sensitive data in cookies | 43 |
| Using HTTPS and SSL communications | 43 |
| About securing passwords and user roles | 44 |
| Managing computer services and accounts | 45 |
| Chapter 4: Deploying Fortify Software Security Center | 46 |
| Deployment overview | 46 |
| High-level deployment tasks | 48 |
| Downloading and unpacking Fortify Software Security Center files | 50 |
| About the Fortify Software Security Center database | 51 |
| About JDBC drivers | 51 |
| Installing and configuring the database server software | 52 |
| Monitoring disk I/O | 52 |
| Database user account permissions | 52 |
| Database-specific configuration requirements | 53 |
| Using a SQL server database | 53 |
| Windows domain authentication | 54 |

| | |
|--|----|
| Using a MySQL database | 54 |
| Using an Oracle database | 56 |
| Preventing the “No more data to read from socket” error | 56 |
| Partitioning an Oracle database for improved performance | 57 |
| About the Fortify Software Security Center database tables and schema | 58 |
| About seeding the Fortify Software Security Center database | 58 |
| Permanently deleting a Fortify Software Security Center database | 59 |
| About deploying Fortify Software Security Center in Kubernetes | 60 |
| Deploying Fortify Software Security Center to a Kubernetes cluster | 60 |
| Troubleshooting deployment to a Kubernetes cluster | 63 |
| About the <fortify.home> directory | 64 |
| Changing the default location | 64 |
| Directory contents | 65 |
| Migration of secret.key file | 67 |
| Retrieving the secret.key file | 67 |
| Migrating the secret.key file | 67 |
| Applying the migrated secret.key file | 67 |
| Chapter 5: Configuring Fortify Software Security Center for the first time | 68 |
| Signing in to Fortify Software Security Center for the first time | 72 |
| Chapter 6: Additional Fortify Software Security Center configuration | 73 |
| About integrating components with Fortify Software Security Center | 74 |
| Configuring Issue Stats thresholds | 75 |
| Setting the Issue Stats thresholds | 76 |
| Configuring application security training | 77 |
| About Fortify Audit Assistant | 78 |
| Configuring Fortify Audit Assistant | 78 |
| About Fortify Audit Assistant auto-prediction | 80 |
| Configuring security for BIRT reporting | 81 |
| Allocating memory for report generation | 82 |
| Setting report generation timeout | 82 |
| Configuring core settings | 83 |
| About configuring a proxy for Rulepack updates | 86 |
| Blocking data export to CSV files | 86 |
| Changing the support contact link in the About box | 86 |

| | |
|---|-----|
| Adding a Fortify Insight link to the Dashboard | 87 |
| Customizing the banner for your organization | 88 |
| Creating a system-wide banner | 89 |
| Configuring email alert notification settings | 90 |
| Configuring whether to receive email alerts | 92 |
| Setting the strategy for resolving issue audit conflicts | 93 |
| Configuring Java Message Service settings | 94 |
| About Fortify Software Security Center user authentication | 95 |
| LDAP user authentication | 95 |
| Preparing to configure LDAP authentication | 96 |
| Requirements for multiple LDAP servers | 96 |
| About the LDAP server referrals feature | 97 |
| Disabling LDAP referrals support | 98 |
| Configuring LDAP servers | 98 |
| Editing an LDAP server configuration | 108 |
| Deleting an LDAP server configuration | 108 |
| Importing an LDAP server configuration | 109 |
| Registering LDAP entities | 109 |
| Refreshing LDAP entities manually | 111 |
| Handling LDAP entries marked "Invalid" | 111 |
| Enabling persistence of the LDAP cache | 112 |
| Implementation of SCIM 2.0 protocol | 112 |
| Using SCIM 2.0 and SAML 2.0 to configure a connection to Microsoft Entra ID for user provisioning | 115 |
| Enabling SCIM to provision externally managed users and groups | 117 |
| Configuring a proxy for integrations | 117 |
| Enabling the running and management of OpenText ScanCentral DAST scans | 119 |
| Configuring a Kafka Stream to use with OpenText ScanCentral DAST | 120 |
| Enabling integration with Fortify ScanCentral SAST | 122 |
| Configuring job scheduler attributes | 123 |
| Setting job execution priority | 127 |
| Canceling scheduled jobs | 127 |
| Recurring cleanup jobs | 128 |
| About data retention | 130 |
| Enabling data retention | 130 |

| | |
|---|-----|
| Editing the default data retention policy | 132 |
| Configuring secure browser access | 134 |
| About configuring Fortify Software Security Center to work with single sign-on | 136 |
| Configuring SAML 2.0-compliant single sign-on | 137 |
| Troubleshooting SAML SSO integration | 140 |
| Configuring single sign-on and single logout solutions that use HTTP headers | 141 |
| Configuring X.509 certification-based single sign-on | 142 |
| Enabling debug logging for single sign-on authentication | 143 |
| Configuring logging | 144 |
| Running in a Federal Information Processing Standards (FIPS) environment | 144 |
| Setting the required password strength for Fortify Software Security Center sign in | 145 |
| About audit issue history | 145 |
| Enabling audit issue history | 147 |
| Chapter 7: Additional installation-related tasks | 148 |
| About bug tracking system integration | 148 |
| Adding bug tracker plugins | 149 |
| Removing bug tracker plugins | 150 |
| Securing logon credentials for bug tracking systems | 150 |
| Bug tracker parameters | 151 |
| ALM Quality Center parameters | 151 |
| Adding and managing parser plugins | 151 |
| Preparing to display OpenText Core SCA (Debricked) results | 152 |
| Preparing to display Sonatype results | 153 |
| About Fortify Software Security Center user administration | 153 |
| Administrator accounts | 154 |
| User account types | 154 |
| About creating user accounts | 155 |
| Preventing destructive library and template uploads to Fortify Software Security Center | 156 |
| Viewing permissions for Fortify Software Security Center roles | 156 |
| About managing LDAP user roles | 156 |
| Group membership in Fortify Software Security Center | 157 |
| Handling failed LDAP user logins | 157 |
| About mapping Fortify Software Security Center roles to LDAP groups | 158 |
| Global search functionality in Fortify Software Security Center | 158 |
| Troubleshooting search index issues | 159 |

| | |
|---|-----|
| Placing Fortify Software Security Center in maintenance mode | 159 |
| If Fortify Software Security Center is stuck in maintenance mode | 160 |
| Pausing and resuming job execution | 161 |
| About OpenText SAST Application Security Content | 162 |
| Updating Rulepacks from the Rulepack update server | 162 |
| Exporting Rulepacks | 163 |
| Importing OpenText SAST Application Security Content | 164 |
| Deleting Rulepacks | 164 |
| Extending an existing mapping | 165 |
| Creating a new mapping | 165 |
| Enabling OpenText SAST and OpenText Application Security Tools upgrades from Fortify Audit Workbench | 166 |
| Chapter 8: Upgrading Fortify Software Security Center | 169 |
| Upgrade prerequisites | 169 |
| Preparing to upgrade the database | 170 |
| Setting the Innodb buffer pool size when upgrading a MySQL database | 170 |
| Preparing to run the database upgrade script | 170 |
| Upgrade tasks | 171 |
| Updating and deploying the WAR file | 172 |
| Configuring Fortify Software Security Center after an upgrade | 172 |
| Updating expired licenses | 174 |
| Seeding the database with report seed bundles in quarterly OpenText SAST Application Security Content releases | 174 |
| Chapter 9: Using Fortify Software Security Center | 176 |
| Signing in to Fortify Software Security Center | 176 |
| About session logout | 177 |
| Inactive session timeout | 177 |
| Requesting access to Fortify Software Security Center | 178 |
| Changing your password | 178 |
| Setting preferences system-wide and across application versions | 178 |
| Viewing keyboard hotkeys | 179 |
| Accessing the API documentation | 179 |

| | |
|--|-----|
| About the Fortify Software Security Center Dashboard | 180 |
| Issue Stats | 181 |
| Viewing high-level summary metrics for your application versions | 182 |
| Viewing high-level summary metrics (graphical representation) for an application version | 183 |
| Exporting the Dashboard summary table | 183 |
| Chapter 10: Managing user accounts | 185 |
| About tracking teams | 185 |
| About roles | 185 |
| Preconfigured roles | 185 |
| Creating custom roles | 187 |
| Deleting custom roles | 188 |
| Account administration | 188 |
| Creating local user accounts | 188 |
| Editing local user accounts | 190 |
| Unlocking local user accounts | 192 |
| Viewing externally managed users and groups | 193 |
| Assigning roles to externally managed users and groups | 193 |
| Chapter 11: Applications and application versions | 194 |
| About tracking development teams | 195 |
| About the application creation process | 195 |
| Strategies for creating application versions | 195 |
| Strategies for packaged software | 196 |
| Strategies for continuous deployment | 196 |
| About annotating application versions for reporting | 196 |
| About creating application versions | 196 |
| Application version attributes | 197 |
| Creating custom attributes | 198 |
| Deleting attributes and attribute values | 200 |
| Deleting attributes | 200 |
| Deleting attribute values | 201 |
| Applying new custom attributes to application versions | 202 |
| About issue templates | 202 |
| Adding issue templates to the system | 203 |
| Template selection | 203 |

| | |
|--|-----|
| Creating the first version of a new application | 204 |
| Adding a new version to an application | 207 |
| Viewing application versions | 211 |
| Searching applications and application versions from the Applications view | 212 |
| Searching specific application | 212 |
| Searching application version | 213 |
| Recalculating application metrics | 214 |
| Editing application version details | 214 |
| Exporting selected data for an application version | 214 |
| Using bug tracking systems to help manage security vulnerabilities | 215 |
| Bug tracker configuration | 216 |
| Velocity templates for bug filing | 216 |
| Adding Velocity Templates to Bug Tracker Plugins | 217 |
| Customizing Velocity templates for bug tracker plugins | 218 |
| Deleting Velocity templates | 219 |
| Assigning a bug tracking system to an application version | 219 |
| Submitting a bug for a single issue | 220 |
| Submitting a bug for multiple issues | 221 |
| Bug state management | 222 |
| Changing the template associated with an application version | 223 |
| Setting analysis result processing rules for application versions | 223 |
| About processing rules that affect instance ID migration | 228 |
| Configuring Fortify Audit Assistant options for an application version | 229 |
| Enabling auto-apply and auto-predict for an application version | 230 |
| About custom tags | 231 |
| Adding custom tags to the system | 232 |
| Modifying custom tag attributes | 233 |
| Globally hiding custom tags | 234 |
| Deleting custom tags | 234 |
| Adding custom tag values | 235 |
| Add a custom tag value (Fortify Audit Assistant configured) | 235 |
| Setting the Issue State | 238 |
| Editing custom tags | 239 |
| Deleting custom tag values | 240 |
| Associating custom tags with issue templates | 240 |
| Removing custom tags from issue templates | 241 |

| | |
|---|-----|
| Assigning custom tags to application versions | 241 |
| Disassociating a custom tag from an application version | 242 |
| Managing custom tags through issue templates | 243 |
| Managing custom tags through an issue template in an FPR file | 243 |
| About deleting application versions | 243 |
| Deactivating application versions | 244 |
| Reactivating application versions | 244 |
| Deleting an application version | 245 |
| Chapter 12: About webhooks | 246 |
| Webhooks permissions | 246 |
| Creating webhooks | 247 |
| Editing webhooks | 250 |
| Viewing webhook payloads | 250 |
| Redelivering webhook payloads | 251 |
| Deleting webhooks | 252 |
| Chapter 13: Variables, performance indicators, and alerts | 253 |
| Creating variables | 253 |
| Variable syntax | 254 |
| Creating performance indicators | 255 |
| Creating alerts | 256 |
| Editing alerts | 258 |
| Deleting alerts | 259 |
| Viewing and marking alerts | 259 |
| Chapter 14: Working with scan artifacts | 261 |
| Uploading scan artifacts | 261 |
| Viewing file processing errors | 262 |
| Viewing scan artifact details | 263 |
| Downloading analysis results | 264 |
| Downloading the merged FPR file for an application version | 264 |
| Downloading individual analysis results | 265 |
| Approving analysis results for an application version | 265 |

| | |
|--|-----|
| Denying processing approval | 266 |
| Viewing issue metadata | 267 |
| Mapping analysis results to external lists | 268 |
| Purging scan artifacts | 268 |
| Deleting artifacts | 269 |
| Chapter 15: Collaborative auditing | 270 |
| Viewing high-level summary metrics for an application version | 271 |
| About current issues state | 271 |
| Viewing information about issues to audit | 272 |
| Viewing issues based on folders | 273 |
| Viewing issues assigned to you | 274 |
| Filtering issues for display | 275 |
| Searching issues | 276 |
| Search modifiers | 277 |
| Search query examples | 280 |
| Searching globally | 281 |
| Auditing analysis results | 282 |
| Auditing correlated issues | 288 |
| About suppressed, removed, and hidden issues | 288 |
| Setting issue viewing preferences | 290 |
| Viewing removed issues | 290 |
| Changing displayed issues using filter sets | 291 |
| Overriding assigned issue priority | 292 |
| Enabling the priority override capability | 292 |
| Overriding priority values during an audit | 293 |
| Viewing issues that have changed priority values | 293 |
| Viewing priority override information in issue reports | 294 |
| Reverting to original priority values | 295 |
| Viewing bugs submitted for issues | 295 |
| Auditing a batch of issues | 296 |
| Using Fortify Audit Assistant with Fortify Software Security Center | 297 |
| Consistent use of tags | 297 |
| Mapping Fortify Audit Assistant analysis tag values to Fortify Software Security Center custom tag values | 298 |

| | |
|---|-----|
| About setting prediction policies | 300 |
| Fortify Audit Assistant workflow | 301 |
| Reviewing Fortify Audit Assistant results | 302 |
| About Fortify Audit Assistant training | 304 |
| Train your model using decisions your auditors make | 304 |
| Selecting a Fortify Audit Assistant training tag | 305 |
| Submitting training data to Fortify Audit Assistant | 305 |
| Exporting open source data | 306 |
| Integrating Fortify Software Security Center with Fortify WebInspect Enterprise | 306 |
| Viewing OpenText DAST analysis results in Fortify Software Security Center | 307 |
| OpenText DAST audit data | 309 |
| False positives | 309 |
| Submitting dynamic scan requests to Fortify WebInspect Enterprise | 310 |
| Processing dynamic scan requests from Fortify WebInspect Enterprise | 311 |
| Editing and canceling dynamic scan requests | 312 |
| Dynamic scan request states | 312 |
| Editing dynamic scan requests | 312 |
| Canceling dynamic scan requests | 313 |
| Viewing open source data | 313 |
| Viewing open source data from the AUDIT page | 313 |
| Viewing open source data from the OPEN SOURCE page | 313 |
| Downloading an OpenText Core SCA (Debricked) software bill of materials | 315 |
| Chapter 16: Working with OpenText ScanCentral DAST | 316 |
| OpenText ScanCentral DAST permissions | 316 |
| Submitting requests for dynamic scans to OpenText ScanCentral DAST | 317 |
| Synchronizing audit history changes in OpenText ScanCentral DAST using Kafka | 318 |
| Chapter 17: Working with Fortify ScanCentral SAST | 319 |
| Fortify ScanCentral SAST permissions | 319 |
| Viewing Fortify ScanCentral SAST scan request details | 320 |
| Prioritizing a Fortify ScanCentral SAST scan request | 321 |
| Canceling Fortify ScanCentral SAST scan requests | 322 |
| Viewing Fortify ScanCentral SAST sensor information | 322 |
| Viewing Fortify ScanCentral SAST Controller information | 323 |

| | |
|--|-----|
| Stopping the Controller | 323 |
| Placing the Controller in maintenance mode | 323 |
| Safely shutting down Fortify ScanCentral SAST sensors | 324 |
| Removing the Controller from maintenance mode | 324 |
| About Fortify ScanCentral SAST sensor pools | 325 |
| Pre-defined sensor pools | 325 |
| Creating Fortify ScanCentral SAST sensor pools | 326 |
| Moving sensors between pools | 327 |
| Deleting Fortify ScanCentral SAST sensor pools | 328 |
| Chapter 18: BIRT reports | 329 |
| BIRT libraries | 329 |
| Importing report libraries | 330 |
| Generating and downloading reports | 330 |
| Generating and downloading customized BIRT reports in XLSX | 332 |
| Customizing BIRT reports | 333 |
| Acquiring the BIRT Report Designer | 333 |
| Downloading report templates | 333 |
| Importing report definitions | 334 |
| Chapter 19: Authentication tokens | 336 |
| Authentication token types | 336 |
| Generating authentication tokens | 338 |
| Editing authentication tokens | 339 |
| Deleting authentication tokens | 339 |
| Appendix A: Using the fortifyclient utility | 340 |
| Preparing to use fortifyclient | 340 |
| fortifyclient HTTP timeouts | 341 |
| Listing fortifyclient commands and options | 341 |
| Generating an authentication token from the command line | 341 |
| Specifying the number of days before a token expires | 342 |
| Listing authentication tokens | 342 |
| Invalidating tokens | 343 |

| | |
|---|---------|
| Listing application versions | 343 |
| Uploading FPR files | 344 |
| Downloading FPR files | 344 |
| Purging application version artifacts | 345 |
| Importing content bundles | 345 |
| Downloading audit attachment files | 345 |
| Appendix B: Authoring bug tracker plugins | 346 |
| Use case | 346 |
| Component setup | 347 |
| Implementation | 347 |
| Plugin methods and method calls | 348 |
| Plugin helper | 353 |
| Error handling | 353 |
| Almost stateless | 354 |
| Debugging a bug tracker plugin | 354 |
| Deploying a customized bug tracker plugin | 354 |
| Chapter C: Advanced configuration | 356 |
| Automating Fortify Software Security Center configuration | 356 |
| Automating configuration in a root context | 358 |
| Application configuration options | 360 |
| Configuring background job execution strategy | 361 |
| Appendix D: Webhook payloads | 363 |
| Event payloads | 364 |
| Artifact upload payload | 364 |
| Artifact upload approved payload | 364 |
| Project version payload | 365 |
| Project version updated payload | 366 |
| Project version created from previous payload | 366 |
| Report generation payload | 367 |
| User payload | 368 |

| | |
|-----------------------------------|-----|
| Send documentation feedback | 370 |
|-----------------------------------|-----|

Preface

Contacting Customer Support

Visit the [Customer Support](#) website to:

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

For more information

For more information about OpenText Application Security Testing products, visit [OpenText Application Security](#).

Product feature videos

You can find videos that highlight OpenText Application Security Software products and features on the [Fortify Unplugged YouTube™ channel](#).

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 |
|--------------------------------------|--|
| 25.2.0 | <p>Added:</p> <ul style="list-style-type: none">• "System requirements" on page 32• "Automating configuration in a root context" on page 358 <p>Updated:</p> <ul style="list-style-type: none">• Incorporated product name changes (see "Product name changes" on page 23)• The location for plugin log files has changed (see "Directory contents" on page 65)• Introduction of an improved modern Applications view (see "Viewing application versions" on page 211)• Application version processing rules for if the file count or line count increases or decreases by 10% (see "Setting analysis result processing rules for application versions" on page 223)• 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" on page 272 and "Viewing scan artifact details" on page 263)• Improved display and filtering of Fortify ScanCentral SAST analysis results (see "Viewing Fortify ScanCentral SAST scan request details" on page 320) <p>Removed:</p> <ul style="list-style-type: none">• 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 |

| Software release / Document revision | Changes |
|--------------------------------------|--|
| | <p>are no longer supported</p> <ul style="list-style-type: none"> • 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 | <p>Updated:</p> <ul style="list-style-type: none"> • Added information about the service account required to integrate with OpenText ScanCentral DAST (see "Enabling the running and management of OpenText ScanCentral DAST scans" on page 119) |
| 24.4.0 | <p>Added:</p> <ul style="list-style-type: none"> • 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" on page 145) • A Fortify ScanCentral SAST Controller role in "Preconfigured roles" on page 185 and "User account types" on page 154. • "Configuring logging" on page 144 • "Migration of secret.key file" on page 67 <p>Updated:</p> <ul style="list-style-type: none"> • "Running in a Federal Information Processing Standards (FIPS) environment" on page 144 • The description for the secret . key parameter (see "Directory contents" on page 65) <p>Removed:</p> <ul style="list-style-type: none"> • Topics Changing Log Levels for Fortify Software Security Center and |

| Software release / Document revision | Changes |
|--------------------------------------|---|
| | <p>Customizing Fortify Software Security Center Logging are removed and replaced with "Configuring logging " on page 144</p> <ul style="list-style-type: none"> • The topic About Susceptibility Analysis of Web Applications was removed as Fortify SourceAndLibScanner is deprecated |
| 24.2.0 | <p>Added:</p> <ul style="list-style-type: none"> • Ability for Administrators to enable a data retention policy that defines the time period for retaining application version artifacts (see "About data retention" on page 130) • Instructions for changing the UI theme (see "Setting preferences system-wide and across application versions" on page 178) • Instructions on how to download customized BIRT reports in XLSX format (see "Generating and downloading customized BIRT reports in XLSX" on page 332) • Ability to set up Kafka to synchronize audit history changes for suppressed issues, priority override, and analysis tag with OpenText ScanCentral DAST (see "Synchronizing audit history changes in OpenText ScanCentral DAST using Kafka" on page 318, and "Configuring a Kafka Stream to use with OpenText ScanCentral DAST" on page 120) • Ability to set up timeouts for connect, read, and write for fortifyclient (see "fortifyclient HTTP timeouts" on page 341) <p>Updated:</p> <ul style="list-style-type: none"> • Added an informational note to "Monitoring disk I/O" on page 52 • The default schedule for LDAP Refresh (see "Recurring cleanup jobs" on page 128) • Modified the IdP metadata location and keystore location (see "Configuring SAML 2.0-compliant single sign-on" on page 137) • Updated the list of supported operators (see "Creating performance indicators" on page 255) • Added a description for the Issue State (see "Setting the Issue State" on page 238) |

| Software release / Document revision | Changes |
|--------------------------------------|---|
| | <ul style="list-style-type: none"> • Changed the default job execution strategy to Flexible (see "Configuring job scheduler attributes" on page 123) <p>Removed:</p> <ul style="list-style-type: none"> • The activity, requirement, and requirementtemplate table names from "Configuring security for BIRT reporting" on page 81 • The authentication token of type AuditToken • All mentions of the Bug Tracker Plugin for Bugzilla |
| 23.2.0 | <p>Added:</p> <ul style="list-style-type: none"> • "Running in a Federal Information Processing Standards (FIPS) environment " on page 144 • OpenText ScanCentral DAST supports setting a base URL application version attribute. You can set the base URL when "Creating the first version of a new application" on page 204 or "Adding a new version to an application" on page 207. • An authentication token of type AutomationToken that provides access to most of the REST API for longer-running automations (see "Authentication token types" on page 336) • Support for downloading a Software Bill of Materials (SBOM) (see "Downloading an OpenText Core SCA (Debricked) software bill of materials" on page 315) • A system-wide banner for administrators to post a message to Fortify Software Security Center users that persists until removed (see "Creating a system-wide banner" on page 89) <p>Updated:</p> <ul style="list-style-type: none"> • All references to Microsoft Azure AD and Azure Active Directory were changed to Microsoft Entra ID and Microsoft Entra, respectively. • You can remove or change an assigned user from an issue on the Audit page (see "Auditing analysis results" on page 282) • Added instructions about setting the Issue State (see "Setting the Issue State") |

| Software release / Document revision | Changes |
|---|--|
| | <p>on page 238)</p> <ul style="list-style-type: none">• The <code>scan_issue(ID)</code> for MySQL and SQL Server database users has been changed from INT to BIGINT (see "Preparing to upgrade the database" on page 170) <p>Removed:</p> <ul style="list-style-type: none">• The topic Enabling Metadata Sharing was removed because the Fortify Audit Assistant G2 model uses a different training method. |

Chapter 1: Introduction

Fortify Software Security Center 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™ Fortify Static Code Analyzer (OpenText SAST)
- OpenText™ Fortify ScanCentral SAST
- OpenText™ Fortify ScanCentral DAST
- Fortify WebInspect Enterprise
- OpenText™ Core Software Composition Analysis (OpenText Core SCA)
- Sonatype

Fortify Software Security Center 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 | 23 |
| Audience | 24 |
| Related documents | 24 |

Product name changes

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

| Previous name | New name |
|------------------------------|--|
| Fortify Static Code Analyzer | OpenText™ Fortify Static Code Analyzer (OpenText SAST) |

| Previous name | New name |
|----------------------------------|--|
| Fortify Software Security Center | OpenText™ Application Security |
| Fortify WebInspect | OpenText™ Fortify WebInspect (OpenText DAST) |
| Fortify on Demand | OpenText™ Core Application Security |
| Debricked | OpenText™ Core Software Composition Analysis (OpenText Core 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.

Audience

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

The content for Fortify Software Security Center 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 Fortify Software Security Center API documentation, see ["Accessing the API documentation" on page 179](#).

Document structure

This document is presented in two main parts. The first part includes topics that describe how to deploy and configure Fortify Software Security Center starting with ["Providing for secure deployment" on page 42](#). The second part describes how to use Fortify Software Security Center starting with ["Using Fortify Software Security Center" on page 176](#).

Related documents

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

Note: 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 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 |
|--|--|
| <i>About OpenText Application Security Software Documentation</i> 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. |
| <i>OpenText Application Security Software Release Notes</i> | 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 ScanCentral DAST

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

| Document / file name | Description |
|--|--|
| <i>OpenText™ ScanCentral DAST Configuration and Usage Guide</i> sc-dast-ugd-<version>.pdf | This document provides information about how to configure and use OpenText ScanCentral DAST to conduct dynamic scans of Web applications. |
| <i>OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide</i> 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. |
| <i>OpenText™ Dynamic Application Security Testing and OAST on Docker User Guide</i> dast-docker-ugd-<version>.pdf | This document describes how to download, configure, and use OpenText DAST and Fortify OAST that are available as container images on the Docker platform. The OpenText DAST image is intended to be used in automated processes as a headless sensor configured by |

| Document / file name | Description |
|----------------------|---|
| | way of the command line interface (CLI) or the application programming interface (API). It can also be run as an OpenText ScanCentral DAST sensor and used in conjunction with Fortify Software Security Center. Fortify OAST is an out-of-band application security testing (OAST) server that provides DNS service for the detection of OAST vulnerabilities. |

Fortify ScanCentral SAST

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

Fortify Software Security Center

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

| Document / file name | Description |
|---|---|
| <i>OpenText™ Application Security User Guide</i> ssc-ugd-<version>.pdf | <p>This document provides Fortify Software Security Center users with detailed information about how to deploy and use Fortify Software Security Center. It provides all the information you need to deploy, configure, and use Fortify Software Security Center.</p> <p>It is intended for use by system and instance administrators, database administrators (DBAs), enterprise security leads,</p> |

| Document / file name | Description |
|----------------------|---|
| | development team managers, and developers. Fortify Software Security Center provides security team leads with a high-level overview of the history and status of a project. |

OpenText SAST

The following documents provide information about OpenText 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 |
|---|--|
| <i>OpenText™ Static Application Security Testing User Guide</i> sast-ugd-<version>.pdf | This document describes how to install and use OpenText SAST to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding. |
| <i>OpenText™ Static Application Security Testing Custom Rules Guide</i> sast-cr-ugd-<version>.zip | <p>This document provides the information that you need to create custom rules for OpenText SAST. This guide includes examples that apply rule-writing concepts to real-world security issues.</p> <p>Note: This document is included only with the product download.</p> |
| <i>OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide</i> 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 |
|---------------------------------------|--|
| <i>OpenText™ Application Security</i> | This document describes how to install application |

| Document / file name | Description |
|---|--|
| <i>Tools Guide</i> sast-tgd-<version>.pdf | security tools. It provides an overview of the applications and command-line tools that enable you to scan your code with OpenText SAST, review analysis results, work with analysis results files, and more. |
| <i>OpenText™ Fortify Audit Workbench User Guide</i> 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. |
| <i>OpenText™ Fortify Plugin for Eclipse User Guide</i> 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. |
| <i>OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio User Guide</i> 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 Fortify Software Security Center. |
| <i>OpenText™ Fortify Extension for Visual Studio User Guide</i> 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 DAST

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

| Document / file name | Description |
|--|---|
| <i>OpenText™ Dynamic Application Security Testing Installation Guide</i> dast-igd-<version>.pdf | This document provides an overview of OpenText DAST and instructions for installing and activating the product license. |
| <i>OpenText™ Dynamic Application Security Testing User Guide</i> | This document describes how to configure and use OpenText DAST to scan and analyze Web applications |

| Document / file name | Description |
|---|--|
| dast-ugd-<version>.pdf | <p>and Web services.</p> <p>Note: This document is a PDF version of the OpenText 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.</p> |
| <p><i>OpenText™ Dynamic Application Security Testing and OAST on Docker User Guide</i></p> <p>dast-docker-ugd-<version>.pdf</p> | <p>This document describes how to download, configure, and use OpenText DAST and Fortify OAST that are available as container images on the Docker platform. The OpenText 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 ScanCentral DAST sensor and used in conjunction with Fortify Software Security Center.</p> <p>Fortify OAST is an out-of-band application security testing (OAST) server that provides DNS service for the detection of OAST vulnerabilities.</p> |
| <p><i>OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide</i></p> <p>lim-ugd-<version>.pdf</p> | <p>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.</p> |
| <p><i>OpenText™ Dynamic Application Security Testing Tools Guide</i></p> <p>dast-tgd-<version>.pdf</p> | <p>This document describes how to use the OpenText DAST diagnostic and penetration testing tools and configuration utilities packaged with OpenText DAST and Fortify WebInspect Enterprise.</p> |
| <p><i>OpenText™ Dynamic Application Security Testing Agent Installation and Rulepack Guide</i></p> | <p>This document describes how to install the OpenText DAST Agent and describes the detection capabilities of the OpenText DAST Agent Rulepack Kit. OpenText</p> |

| Document / file name | Description |
|------------------------------|--|
| dast-agent-igd-<version>.pdf | 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 |
|---|--|
| <i>OpenText™ Fortify WebInspect Enterprise Installation and Implementation Guide</i> WIE_Install_<version>.pdf | This document provides an overview of Fortify WebInspect Enterprise and instructions for installing Fortify WebInspect Enterprise, integrating it with Fortify Software Security Center and OpenText 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. |
| <i>OpenText™ Fortify WebInspect Enterprise User Guide</i> WIE_Guide_<version>.pdf | <p>This document describes how to use Fortify WebInspect Enterprise to manage a distributed network of OpenText DAST sensors to scan and analyze Web applications and Web services.</p> <div>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.</div> |
| <i>OpenText™ Dynamic Application</i> | This document describes how to use the OpenText DAST |

| Document / file name | Description |
|---|---|
| <i>Security Testing Tools Guide</i> dast-tgd-<version>.pdf | diagnostic and penetration testing tools and configuration utilities packaged with OpenText DAST and Fortify WebInspect Enterprise. |

Chapter 2: System requirements

This section describes the system requirements for the Fortify Software Security Center server.

This section contains the following topics:

| | |
|---|----|
| Hardware requirements | 32 |
| Supported platforms and architectures | 33 |
| Supported application server | 34 |
| Database requirements | 34 |
| Kubernetes cluster deployment requirements (optional) | 36 |
| Browsers | 37 |
| Supported authentication systems | 37 |
| BIRT report requirements | 38 |
| Supported service integrations | 38 |
| Fortify Project Results (FPR) file compatibility | 39 |
| Acquiring the software | 40 |
| Verifying software downloads | 40 |
| Virtual Machine support | 41 |

Hardware requirements

Fortify Software Security Center requires the hardware specifications listed in the following table.

| Server | Component | Minimum required | Minimum recommended |
|--------------------|----------------|------------------|---------------------|
| Application server | Java heap size | 4 GB | 24 GB |
| Database server | Processor | Quad-core | Eight-core |
| | RAM | 8 GB | 64 GB |

Database hardware requirements

OpenText recommends an eight-core processor with 64 GB of RAM for the Fortify Software Security Center database. Using less than this recommendation can impact Fortify Software Security Center

performance.

Use the following formula to estimate the size (in GB) of the Fortify Software Security Center database disk space:

$$((\text{<num_issues>} * 30 \text{ KB}) + \text{<size_of_artifacts>}) \div 1,000,000$$

where:

- **<num_issues>** represents the total number of issues in the system
- **<size_of_artifacts>** represents the total size in KB of all uploaded artifacts and analysis results

Note: This formula produces only a rough estimate for database disk space allocation. Do not use it to estimate disk space requirements for long-term projects. Disk requirements for Fortify Software Security Center databases increases in proportion to the number of projects, scans, and issues in the system.

Database performance metrics

The following table shows performance metrics (number of issues discovered per hour) for Fortify Software Security Center configured with the minimum and the recommended hardware requirements.

| Database | Issues per hour | Issues per hour |
|------------------------|-----------------------|---------------------------|
| | Minimum configuration | Recommended configuration |
| MySQL | 362,514 | 2,589,385 |
| Oracle® Database | 231,392 | 3,020,950 |
| Microsoft® SQL Server® | 725,028 | 3,625,140 |

Supported platforms and architectures

Fortify Software Security Center supports the platforms and architectures listed in the following table.

| Operating system | Versions |
|--------------------|-------------|
| Microsoft Windows® | Server 2016 |
| | Server 2019 |
| | Server 2022 |

| Operating system | Versions |
|------------------|--|
| Linux® | Red Hat® Enterprise Linux® 8, 9 SUSE® Linux® Enterprise Server 15 Note: Linux® ARM platform supported as technical preview in 25.2.0. |

Note: Although Fortify Software Security Center is not tested on all Linux variants, most distributions are not known to have issues.

Supported application server

Fortify Software Security Center supports Apache® Tomcat™ version 10.1.x for the following Java™ Development Kit (JDK) versions:

- Oracle JDK 17
- Red Hat OpenJDK 17
- SUSE OpenJDK 17
- Zulu OpenJDK 17 from Azul

OpenText only supports the deployment of a single Fortify Software Security Center instance. That instance must not be behind a layer 7 load balancer of your own implementation. However, OpenText does support a Fortify Software Security Center implementation behind a layer 4 load balancer in a deployment to a Kubernetes cluster.

Important! OpenText does not support the installation of any third-party performance monitoring agents on the Tomcat instance that is hosting Fortify Software Security Center.

Database requirements

Fortify Software Security Center requires case-sensitive database schema collations.

Important! Fortify Software Security Center is a high I/O-intensive application, which affects performance. Make sure that your disk subsystem provides low read/write latency. OpenText recommends that you monitor disk I/O as the database grows.

All required database drivers are included in the WAR file. Fortify Software Security Center supports the databases listed in the following table.

| Database | Versions | Collation / character sets |
|----------|---|---|
| MySQL | 8.0 (Community Edition) | latin1_general_cs |
| | Amazon RDS for MySQL (8.0) | utf8mb3_bin (if available, preferred over utf8_bin) utf8_bin (only if utf8 is a synonym for utf8mb3 character set) |
| Oracle | 19c (19.3) | AL32UTF8 for all languages WE8MSWIN1252 for US English |
| | 2019 2022 Amazon RDS for SQL Server (2019, 2022) Microsoft® Azure® SQL Database (2019, 2022) | SQL_Latin1_General_CP1_CS_AS |

Note: Fortify Software Security Center does not support the following cloud managed database platforms:

- Azure Database for MySQL
- Oracle in the cloud
- SQL Server on Google Cloud Platform™

OpenText does not support the direct conversion from one database server type to another, such as converting from MySQL to Oracle. To do this, you must use the Server API to move data from your current Fortify Software Security Center instance to a new instance that uses the database server type you want to use going forward. Professional Services can assist you with this process.

Kubernetes cluster deployment requirements (optional)

To deploy Fortify Software Security Center to a Kubernetes cluster, make sure that the following requirements are met.

Kubernetes cluster requirements

The following are the *minimum* requirements for the default installation:

- Kubernetes versions 1.30, 1.31, or 1.32
- Kubernetes persistent volumes with optional support for Pod security context fsGroup option
Using a non-default container user ID requires fsGroup support.
- Kubernetes LoadBalancer Service type (recommended)
- 28 GB of available RAM and 8 CPUs on a single Kubernetes node
- 4 GiB of storage for persistent volume

Locally-installed tools required

- A kubectl command-line tool
OpenText recommends that you use the same kubectl command-line tool version as the Kubernetes cluster version or follow the Version Skew Policy on the Kubernetes website.
- Helm command-line tool versions 3.16 or 3.17
To determine which Helm command-line tool version matches your Kubernetes cluster version, see the Helm Version Support Policy on the Helm website.
- (Recommended) A Docker® client and server installation (any version)

Additional requirements

- Kubeconfig file for the Kubernetes cluster
- Docker Hub account with access to Fortify Software Security Center images

Note: If you need access to the Fortify Docker repository, contact mfi-fortifydocker@opentext.com with your first name, your last name, and your Docker ID. OpenText will then give you access to the Docker organization that contains the Fortify Software Security Center images.

- DNS name for the Fortify Software Security Center web application (address used to access the service)

- Java keystore for setting up HTTPS

The keystore must contain a CA certificate and a server certificate for the Fortify Software Security Center DNS name with an associated private key.

- Keystore password
- Private key password
- Fortify license file

Browsers

OpenText recommends that you use one of the browsers listed in the following table and a screen resolution of 1400 x 800.

| Browser | Version |
|-------------------|--------------|
| Google Chrome™ | 116 or later |
| Microsoft® Edge | 114 or later |
| Mozilla® Firefox® | 116 or later |
| Apple® Safari | 14 or later |

Supported authentication systems

Fortify Software Security Center supports the following directory services:

- LDAP: LDAP 3 compatible

Important! Although Fortify Software Security Center supports the use of multiple LDAP servers, it does not support the use of multiple LDAP servers behind a load balancer unless they are exact copies.

- Windows Active Directory service

Single sign-on (SSO)

Fortify Software Security Center supports the following single sign-on solutions:

- HTTP Headers SSO (Oracle SSO, CA SSO)
- SAML 2.0 SSO
- X.509 SSO

BIRT report requirements

Fortify Software Security Center custom reports support BIRT Report Designer version 4.16.0.

Installing required fonts (Linux only)

To generate BIRT reports on a Linux system from Fortify Software Security Center, you must install the fontconfig library, DejaVu Sans fonts, and DejaVu Serif fonts on the server. If you need to, you can download these fonts from the [DejaVu Fonts website](#).

Installing required libraries (non-GUI Linux only)

To generate reports on a non-GUI Linux system, you must install the GTK and X Window System (X11) libraries.

Supported service integrations

Fortify Software Security Center supports the service integrations listed in the following table.

| Service | Application | Versions |
|---------------------|--|----------------------|
| Bug tracking | OpenText™ ALM Quality Center | 12.50 |
| | Azure DevOps | Not applicable |
| | Note: Only basic user password authentication is supported. | |
| | Azure DevOps Server | 2019 2020 2022 |
| | Jira Software Server | 9.10 |
| | Jira Software Cloud | Not applicable |
| Static assessments | OpenText™ Fortify ScanCentral SAST | 25.2.0 |
| Dynamic assessments | OpenText ScanCentral DAST | 25.2.0 |
| | Fortify WebInspect Enterprise | 23.2.x |

| Service | Application | Versions |
|----------------|---|-----------------|
| Issue Auditing | OpenText™ Fortify Audit Assistant | Not applicable |
| | OpenText™ Fortify Audit Assistant on Premises | 23.2.0 or later |

Fortify Project Results (FPR) file compatibility

OpenText Application Security Software products support opening and uploading FPR files in adjacent releases. OpenText Application Security Software products can open and accept for upload:

- FPR files that have the same version (<year>.<quarter> portion of the version)
- Older FPR files (within the Product Support Lifecycle policy)
- FPR files that are one version later

OpenText Application Security Software products do not support opening and uploading FPR files generated by later versions of OpenText Application Security Software products when the versions are more than one version apart.

OpenText recommends that you keep your OpenText Application Security Software product versions synchronized so that you are working with FPR file versions that have the same version as your products.

The FPR file version is determined as follows:

- The FPR version is the same version of the analyzer that generated it.
- The FPR version is the same version of Fortify Software Security Center or OpenText Application Security Tools that changed or audited the FPR.
- If you merge two FPRs, the resulting FPR has the version of the more recently generated FPR.

Caution regarding uploading FPR files to Fortify Software Security Center

Fortify Software Security Center keeps an FPR file that contains the latest scan results and audit information for each application. Fortify Audit Workbench and the Secure Code Plugins also use this FPR file for collaborative auditing.

Each time you upload an FPR to Fortify Software Security Center, it is merged with the existing FPR. If the FPR has a later version number than the existing FPR, the existing FPR version changes to match the newest FPR.

Acquiring the software

Fortify Software Security Center is available as an electronic download. For instructions on how to download the software from the [Software Licenses and Downloads \(SLD\) portal](#), click **Contact Us / Self Help** to review the videos and the *Quick Start Guide*.

The following table lists the available packages and describes their contents.

| File name | Description |
|--|---|
| Fortify_SSC_Server_ <version>.zip | Fortify Software Security Center package This package includes: <ul style="list-style-type: none">• Fortify Software Security Center WAR file• Fortify Software Security Center seed bundles• About OpenText Application Security Software Documentation |
| Fortify_SSC_Server_ <version>.zip.sig | Signature file for the Fortify Software Security Center package |

Verifying software downloads

This topic describes how to verify the digital signature of the signed file that you downloaded from the Customer Support website. Verification ensures that the downloaded package has not been altered since it was signed and posted to the site. Before proceeding with verification, download the OpenText Application Security Software product files and their associated signature (*.sig) files. You are not required to verify the package to use the software, but your organization might require it for security reasons.

Preparing your system for digital signature verification

Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

To prepare your system for electronic media verification:

1. Go to the [GnuPG](#) website.
2. Download and install GnuPG Privacy Guard.
3. Generate a private key, as follows:
 - a. Run the following command (on a Windows system, run the command without the \$ prompt):

```
$ gpg --gen-key
```


- b. When prompted for key type, select DSA and Elgamal.
 - c. When prompted for a key size, select 2048.
 - d. When prompted for the length of time the key should be valid, select key does not expire.
 - e. Answer the user identification questions and provide a passphrase to protect your private key.
4. Download the OpenText GPG public keys (compressed tar file) from https://mysupport.microfocus.com/documents/10180/0/MF_public_keys.tar.gz.
5. Extract the public keys.
6. Import each downloaded key with GnuPG with the following command:

```
gpg --import <path_to_key>/<key_file>
```

Virtual Machine support

You can run OpenText Application Security Software products on an approved operating system in virtual machine environments. You must provide dedicated CPU and memory resources that meet the minimum hardware requirements. If you find issues that cannot be reproduced on the native environments with the recommended processing, memory, and disk resources, you must work with the provider of the virtual environment to resolve them.

Note: If you run OpenText Application Security Software products in a VM environment, OpenText strongly recommends that you have CPU and memory resources fully committed to the VM to avoid performance degradation.

Chapter 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 Fortify Software Security Center.

This section contains the following topics:

| | |
|---|----|
| Securing access to facilities | 42 |
| Securing Tomcat server | 42 |
| Setting Tomcat server attributes to protect sensitive data in cookies | 43 |
| Using HTTPS and SSL communications | 43 |
| About securing passwords and user roles | 44 |
| Managing computer services and accounts | 45 |

Securing access to facilities

Fortify Software Security Center 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 Fortify Software Security Center in a secure operations facility. You must also secure the underlying Fortify Software Security Center file system and restrict access to the installation directory.

Securing Tomcat server

You must ensure the operational security of the application server that runs Fortify Software Security Center. At a minimum, configure 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.

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.

Using HTTPS and SSL communications

OpenText strongly recommends that you configure Fortify Software Security Center 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 Fortify Software Security Center. The certificate is trusted because these root CA certificates are in the keystore that OpenText Application Security Software client products use.

However, by default, Fortify Software Security Center, 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 Fortify Software Security Center, you must import the self- or locally-signed certificate into the Java Runtime certificate store.

Important! If you used a third-party Certification Authority to issue a locally-signed certificate, 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 Fortify Software Security Center 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 Fortify Software Security Center. Do not simply use the short hostname or localhost.

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

About securing passwords and user roles

OpenText recommends that, after you deploy Fortify Software Security Center and sign in for the first time, you immediately create one or more new local Administrator accounts and delete the default Administrator 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 Fortify Software Security Center users, configure your LDAP server to use secure LDAP communications.

See also

["Signing in to Fortify Software Security Center for the first time" on page 72](#)

["Managing user accounts" on page 185](#)

["LDAP user authentication" on page 95](#)

Managing computer services and accounts

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

Chapter 4: Deploying Fortify Software Security Center

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

This section contains the following topics:

| | |
|--|----|
| Deployment overview | 46 |
| High-level deployment tasks | 48 |
| Downloading and unpacking Fortify Software Security Center files | 50 |
| About the Fortify Software Security Center database | 51 |
| About deploying Fortify Software Security Center in Kubernetes | 60 |
| About the <fortify.home> directory | 64 |

Deployment overview

Fortify Software Security Center 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 Fortify Software Security Center Setup wizard to complete the preliminary configuration. This enables Fortify Software Security Center 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 Fortify Software Security Center 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 Fortify Software Security Center configuration" on page 356](#).

For system requirements information, see ["System requirements" on page 32](#).

To provide centralized management, Fortify Software Security Center inter-operates with the external components described in the following table.

| Component | Description |
|----------------------------|--|
| Required components | |
| Fortify Software Security | Fortify Software Security Center is delivered as a Web Archive |

| Component | Description |
|---|--|
| Center | (WAR) file run by Tomcat server or as a Helm chart for Kubernetes deployment. |
| Fortify Software Security Center database | <p>Database to store user and artifact data. Before you put Fortify Software Security Center into production, you must install a supported third-party database.</p> <p>Important! You must not deploy multiple Fortify Software Security Center instances that share the same database schema. Ensure each Fortify Software Security Center instance operates with its own dedicated database schema to maintain data integrity.</p> |
| 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 SAST (Fortify Static Code Analyzer) | OpenText SAST scans source code and identifies issues. |
| Fortify ScanCentral SAST | OpenText SAST users can use 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 DAST (Fortify WebInspect) | Analysis agent that connects with OpenText DAST Agents to retrieve potential dynamic issues. |
| OpenText ScanCentral DAST | Tool that enables you to configure and run dynamic scans of your web applications with OpenText DAST from Fortify Software Security Center. |
| Fortify Audit Workbench and Secure Code Plugins | Tools to collaboratively audit analysis results on Fortify Software Security Center. These tools can also scan source code and upload analysis results. |
| Jenkins Plugin Azure DevOps Extension | Plugins to scan source code with OpenText SAST and upload analysis results. |

| Component | Description |
|--|--|
| 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" on page 346 . |
| Parser plugin | Plugins to enable display of open source security data from OpenText Core (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 Fortify Software Security Center deployment. |

High-level deployment tasks

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

Note: If you are upgrading Fortify Software Security Center, see ["Upgrading Fortify Software Security Center" on page 169](#).

| 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 <code>fortify.license</code> file. | "Downloading and unpacking Fortify Software Security Center files" on page 50 |
| 2 | Install and configure the database server software you plan to use. | "About the Fortify Software Security Center database" on page 51 |
| 3 | (Optional for advanced users only) Set up an | "Automating Fortify Software |

| Task | Description | Information and instructions |
|---|--|--|
| | autoconfig file before you deploy Fortify Software Security Center to automate the deployment and configuration. | Security Center configuration" on page 356 |
| Deploying in Tomcat server | | |
| 4 | Deploy Fortify Software Security Center in Tomcat server. | Copy the WAR file to the <code><tomcat>/webapps/</code> 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). | <p>There are two ways to do this:</p> <ul style="list-style-type: none"> • Use the Setup wizard to perform the initial configuration "Configuring Fortify Software Security Center for the first time" on page 68 • <i>Advanced users only</i> Automatic initial configuration "Automating Fortify Software Security Center configuration" on page 356 |
| 6 | Sign into Fortify Software Security Center for the first time to set up a non-default Administrator account. | "Signing in to Fortify Software Security Center for the first time" on page 72 |
| 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 Fortify Software Security Center configuration" on page 73 |
| 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" on page 148 |

Downloading and unpacking Fortify Software Security Center 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 Fortify Software Security Center 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 Fortify Software Security Center and migrating applications from previous versions.

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

| Seed bundle file name | Description |
|---|--|
| | 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" on page 48](#)

About the Fortify Software Security Center database

If you are deploying a new instance of Fortify Software Security Center, you must first install and configure the third-party database server software. For database requirements, see ["Database requirements" on page 34](#).

Important!

- Fortify Software Security Center 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" on page 53](#) or ["Using a MySQL database" on page 54](#).

Later, when you configure Fortify Software Security Center for the first time, you will use the Setup wizard to configure connectivity to the database and then seed the database (see ["Configuring Fortify Software Security Center for the first time" on page 68](#)).

About JDBC drivers

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

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 ["Database requirements" on page 34](#).

Monitoring disk I/O

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

Fortify Software Security Center 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 Fortify Software Security Center databases.

Database user account permissions

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

- **Perform runtime tasks**

A user who performs runtime tasks requires 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 Fortify Software Security Center database in a dedicated instance
- Back up and then update the existing Fortify Software Security Center dedicated database instance
- Bind a Fortify Software Security Center user account to the dedicated database instance
- Assign a Fortify Software Security Center user account the read-write permission required to create, initialize, and manage the Fortify Software Security Center database

At a minimum, this user must have a database account that enables the web application to connect to the database.

- **Create and generate reports**

To add an extra measure of security to reporting, create a database user account with read-only access to the Fortify Software Security Center database, and then use the account credentials to configure security for your BIRT reports (see ["Configuring security for BIRT reporting" on page 81](#)).

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 Fortify Software Security Center.

Using a SQL server database

To use SQL Server as the Fortify Software Security Center database, perform the following checks:

- Enable the Auto Update Stats Asynchronously (AUTO_UPDATE_STATISTICS_ASYNC) option for the database.

For instructions, see the [Microsoft SQL documentation](#) website.

- 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 Fortify Software Security Center:

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 Fortify Software Security Center (see ["Automating Fortify Software Security Center configuration" on page 356](#)).
 - Configure Fortify Software Security Center 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.

Using a MySQL database

To use MySQL as the Fortify Software Security Center database, you must configure the MySQL options file. For information about the supported versions of MySQL, see ["Database requirements" on page 34](#).

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

Tip: If you use SSL to connect Fortify Software Security Center 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 8.0 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`.
The default location for MySQL 8.0 is `C:\ProgramData\MySQL\MySQLServer 8.0\`.
 - On Linux systems, the default options file is `my.cnf`.
4. In both the `[mysqld]` and `[mysqldump]` sections, set `max_allowed_packet` to 1G.
If the `[mysqldump]` section is not there, create it.
 5. In the `[mysqld]` section, configure the settings described in the following table. If a listed setting is not included in the file, add it.

| Setting | Value |
|--------------------------------------|--|
| <code>default_storage_engine</code> | INNODB |
| <code>innodb_buffer_pool_size</code> | <p>512M (OpenText recommends 10GB or more)</p> <p>The best performance is achieved when all data and indexes fit.</p> <p>Together with per-connection memory, the <code>innodb_lock_wait_timeout</code> value must not exceed the total available memory on the server. You can estimate the maximum memory usage as follows:</p> $\text{max_connections} * \text{max_allowed_packet} + \text{innodb_buffer_pool_size}$ <p>An <code>innodb_buffer_pool_size</code> value between 60 and 80 percent of available memory is appropriate.</p> |

| Setting | Value |
|---------------------------------------|---|
| | <p>The larger the <code>innodb_buffer_pool_size</code> 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:</p> <ul style="list-style-type: none">• 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 8.0 Reference Manual. |
| <code>innodb_lock_wait_timeout</code> | 300 (recommended) Expressed in seconds |
| <code>innodb_log_file_size</code> | 512M |
| <code>max_allowed_packet</code> | 1G |
| <code>sql-mode</code> | "TRADITIONAL" |

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

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

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

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

1. 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.

Partitioning an Oracle database for improved performance

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

Preparing to partition an Oracle database

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

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

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

Try to achieve record distribution that does not exceed a couple hundred thousand records per partition. OpenText recommends a record distribution of less than one million records per partition.

4. Schedule enough application downtime to partition data. In doing so, consider the time required to:
 - Partition the database

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

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

Partitioning the database

To use the partitioning script:

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

The script execution time depends on the size of your database.

During script execution:

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

Increasing the number of job execution threads

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

1. Open the `<fortify.home>/<app_context>/conf/app.properties` file in a text editor.
2. Increase the value of the `jobs.threadCount` property.

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

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

About the Fortify Software Security Center database tables and schema

The Fortify Software Security Center distribution directory (`<ssc_distribution_dir>`) contains an initialization SQL script for each supported third-party database type. During the initial configuration (see ["Configuring Fortify Software Security Center for the first time" on page 68](#)), run this script for your database type to create the database tables and initialize the database schema for Fortify Software Security Center.

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

- ["Database user account permissions" on page 52](#)
- ["Database-specific configuration requirements" on page 53](#)

About seeding the Fortify Software Security Center database

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

Seeding the Fortify Software Security Center database is necessary to maintain a consistent post-installation configuration. This includes the creation of the default Administrator user account, as well

as required entities such as issue templates, report definitions, and other default data required to make Fortify Software Security Center operational.

Fortify Software Security Center requires two of the downloaded seed bundles (see ["Downloading and unpacking Fortify Software Security Center files" on page 50](#)):

- 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 Fortify Software Security Center 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 Fortify Software Security Center release into a Fortify Software Security Center instance of that same version (either a fresh install or an older instance upgraded to the current version).

After you finish seeding the database, you can modify any user-configurable data entities that were created in the seeding process from the Fortify Software Security Center user interface. For more information, see ["Additional Fortify Software Security Center configuration" on page 73](#).

See also

["Seeding the database with report seed bundles in quarterly OpenText SAST Application Security Content releases" on page 174](#)

Permanently deleting a Fortify Software Security Center database

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

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

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

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

```
drop-tables.sql
```

About deploying Fortify Software Security Center in Kubernetes

You can configure and use the `helm-ssc` Helm chart for complete Fortify Software Security Center 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 [Fortify Software Security Center Documentation](#) website.

For steps to prepare for and perform a Fortify Software Security Center Kubernetes deployment, refer to [Deploying_SSC_in_Kubernetes_25.2.0.html](#).

For information about supported versions of the required software, see "[Kubernetes cluster deployment requirements \(optional\)](#)" on [page 36](#).

Deploying Fortify Software Security Center to a Kubernetes cluster

You can deploy Fortify Software Security Center 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 Fortify Software Security Center Docker image (`fortifydocker/ssc-webapp`) from the Docker Hub

registry. If you must deploy the application in an air-gapped environment, you must use a private registry for the deployment and transfer the Fortify Software Security Center container image to it.

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

To deploy Fortify Software Security Center to a Kubernetes cluster:

1. Create a Docker Hub account, and then supply your account name to Customer Support.

Customer Support can give you access to the Fortify Docker repository.

To request access to the Fortify Software Security Center 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 Fortify Software Security Center container image to your private registry, as follows:
 - a. Log in to the Docker Hub using `docker login`.
 - b. Log in to your private registry using `docker login <priv_reg_host_and_port>`, where `<priv_reg_host_and_port>` represents the host and port of your private registry.
 - c. Transfer the Fortify Software Security Center container image, as follows:
 - i. `docker pull "fortifydocker/ssc-webapp:<tag>"`
 - ii. `docker tag "fortifydocker/ssc-webapp:<tag>" "<priv_reg_host_and_port>/<priv_reg_path>/ssc-webapp:<tag>"`
 - iii. `docker push "<priv_reg_host_and_port>/<priv_reg_path>/ssc-webapp:<tag>"`

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

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

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

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

- d. Enter the <priv_reg_host_and_port>/<priv_reg_path>/ as the value for image.repositoryPrefix parameter in the <ssc_helm_dir>/ssc-values.yaml file.
The value you specify for the image.repositoryPrefix parameter must include a trailing forward slash (/).
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.
 - a. If you are deploying Fortify Software Security Center 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.
 - b. If you are migrating a non-containerized Fortify Software Security Center 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" on page 64](#).
6. Enter any other required parameters to the values.yaml file.
 - The urlHost must contain the fully-qualified DNS name intended for accessing Fortify Software Security Center. The address for accessing the Fortify Software Security Center installation is <https://<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 Fortify Software Security Center secret referenced by secretRef.name, you must manually remove the ssc-webapp pod (it is later automatically

re-created).

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

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 Fortify Software Security Center does not run as expected, and logs alone do not provide enough information, run the following to inspect the container file system, check the state of the environment, and perform advanced debugging tasks:

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

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

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](#).

About the <fortify.home> directory

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

After Fortify Software Security Center deployment, you can find <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

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 Fortify Software Security Center is configured (see ["Configuring Fortify Software Security Center for the first time" on page 68](#)), 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.

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 Fortify Software Security Center is deployed. For details, see ["Automating Fortify Software Security Center configuration" on page 356](#).
- `app.properties`
is a file that contains the application properties that the customer can configure. If you automate the Fortify Software Security Center configuration, this file is generated based on the `appProperties` key in the `autoconfig` file on every startup. For more information, see ["Automating Fortify Software Security Center configuration" on page 356](#).
- `datasource.properties`
is a file that contains the database connection properties. If you automate the Fortify Software Security Center configuration, this file is generated based on the `datasourceProperties` key in the `autoconfig` file on every startup. For more information, see ["Automating Fortify Software Security Center configuration" on page 356](#).
- `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" on page 144](#)).

- `secret.key`
is an encryption key file used to encrypt and decrypt sensitive configuration information in Fortify Software Security Center. Fortify Software Security Center never overwrites this file. However, the file is generated if it is missing from the `<fortify.home>/<app_context>/conf/` directory. If you deployed Fortify Software Security Center version older than 23.1.0, OpenText recommends that you migrate your `secret.key` to the new format. To run Fortify Software Security Center in FIPS environment, you must migrate your `secret.key` to the new format. For more information, see ["Migration of secret.key file" on the next page](#).

Note: The `datasource.properties` file and some database fields contain encrypted entries that rely on the `secret.key` file. If you move your Fortify Software Security Center instance from one computer to another, you must also move the `secret.key` file (not just your database files).

- `version.properties`
is a file that stores information about current and previous versions of Fortify Software Security Center for application upgrade purposes.
- `logs`
is a directory that contains Fortify Software Security Center 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 Fortify Software Security Center uses this token to access the Setup wizard (see ["Configuring Fortify Software Security Center for the first time" on page 68](#)).
- `plugin-framework`
is a directory that contains unpacked plugins and is fully managed by Fortify Software Security Center.

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

- `fortify.license`
is the Fortify Software Security Center 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, Fortify Software Security Center either runs auto-configuration, or starts the Setup wizard to re-create the missing files.

Migration of secret.key file

Fortify Software Security Center 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" on page 64](#).

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 Fortify Software Security Center.

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 Fortify Software Security Center webapp pod to restart.

Chapter 5: Configuring Fortify Software Security Center for the first time

After you deploy Fortify Software Security Center for the first time and then enter the Fortify Software Security Center URL in a browser window, the 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 Fortify Software Security Center, after you upgrade it, or after you place Fortify Software Security Center in maintenance mode (see ["Placing Fortify Software Security Center in maintenance mode" on page 159](#)).

To configure Fortify Software Security Center for the first time:

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

Note: For a standard deployment, the default Fortify Software Security Center 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 Fortify Software Security Center 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:
 - a. Click **UPLOAD**.
 - b. 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" on page 64](#).

9. On the **CORE CONFIGURATION SETTINGS** page, do the following:
 - a. Under **FORTIFY SOFTWARE SECURITY CENTER URL**, type the URL for your Fortify Software Security Center server.
 - b. Select the **Enable HTTP host header validation** check box to ensure that the HTTP Host header value matches the value configured in the Fortify Software Security Center URL (`host.url` property).

Both the host and port must match. This affects both browsers and direct REST API access. If validation is turned off, any HTTP Host header can access Fortify Software Security Center.
 - c. To enable global searches, in the **GLOBAL SEARCH** pane, do the following:
 - i. Select the **Enable global search** check box.
 - ii. 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.

- iii. 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:
 - a. From the **DATABASE TYPE** list, select the database type you are using for Fortify Software Security Center.
 - b. In the **DATABASE USERNAME** box, type the user name for your database account.

For more information, see ["Database user account permissions" on page 52](#).
 - c. 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" on page 52](#).
 - d. In the **JDBC URL** box, type the URL for Fortify Software Security Center, keeping in mind the following:

For MySQL databases:

 - If MySQL server is configured to use the `sha256_password` or the `caching_sha2_password` authentication plugin, you must provide the server RSA public key to the JDBC driver with the `serverRsaPublicKeyFile` option. Alternatively, you can use the less secure `allowPublicKeyRetrieval` option. For more 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! Fortify Software Security Center 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.

- e. In the **MAXIMUM IDLE CONNECTIONS** box, type the maximum number of idle connections that can remain in the pool.
The default value is 50.
- f. In the **MAXIMUM ACTIVE CONNECTIONS** box, type the maximum number of active connections that can remain in the pool.
The default value is 100.
- g. In the **MAXIMUM WAIT TIME (MS)** box, type the maximum number of milliseconds for the pool to wait for a connection (when no connections are available) before the system throws

an exception.

The default value is 60000. To extend the wait indefinitely, set the value to zero.

- h. 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 Fortify Software Security Center configuration and you have enabled database migration in the `<app_context>.autoconfig` file, you do not need to run the `create-tables.sql` script. For information about how to automate the configuration, see ["Automating Fortify Software Security Center configuration" on page 356](#).

13. After you initialize the database, click **NEXT**.

14. On the **DATABASE SEEDING** page, do the following:

- a. Click **BROWSE** to locate and select your `Fortify_Process_Seed_Bundle-2025_Q2_<build>.zip` file, and then click **SEED DATABASE**.
- b. Click **BROWSE** to locate and select your `Fortify_Report_Seed_Bundle-2025_Q2_<build>.zip` file, and then click **SEED DATABASE**.
- c. (Optional) Click **BROWSE** to locate and select your `Fortify_PCI_SSF_Basic_Seed_Bundle-2025_Q2_<build>.zip` file, and then click **SEED DATABASE**.
- d. (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 Unpacking and deploying Fortify Software Security Center software.

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

16. 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.

17. Restart Tomcat server.

After you finish the initial Fortify Software Security Center configuration, then you can complete the configuration of the core attributes and additional settings. For information, see ["Additional Fortify Software Security Center configuration" on page 73](#).

If you later need to change any of the configuration settings, you can place Fortify Software Security Center in maintenance mode, and then make any necessary changes. For instructions on how to place Fortify Software Security Center in maintenance mode, see ["Placing Fortify Software Security Center in maintenance mode" on page 159](#).

See also

["Configuring Fortify Software Security Center after an upgrade" on page 172](#)

Signing in to Fortify Software Security Center for the first time

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

Important! After you sign in, create at least one non-default Administrator account, and then delete the default Administrator account. For more information about how to manage user accounts and roles, see ["About Fortify Software Security Center user administration" on page 153](#).

To sign in to Fortify Software Security Center:

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

Note: For a standard deployment, the default Fortify Software Security Center 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. Type your user name and password.
Type **admin** in both the **Username** and **Password** fields. These are the default credentials for a new installation.
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, you can save it, and then sign in.

See next

["Additional Fortify Software Security Center configuration" on page 73](#)

["Setting the required password strength for Fortify Software Security Center sign in" on page 145](#)

Chapter 6: Additional Fortify Software Security Center configuration

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

This section contains the following topics:

| | |
|--|-----|
| About integrating components with Fortify Software Security Center | 74 |
| Configuring Issue Stats thresholds | 75 |
| Configuring application security training | 77 |
| About Fortify Audit Assistant | 78 |
| Configuring security for BIRT reporting | 81 |
| Configuring core settings | 83 |
| Blocking data export to CSV files | 86 |
| Changing the support contact link in the About box | 86 |
| Adding a Fortify Insight link to the Dashboard | 87 |
| Customizing the banner for your organization | 88 |
| Creating a system-wide banner | 89 |
| Configuring email alert notification settings | 90 |
| Setting the strategy for resolving issue audit conflicts | 93 |
| Configuring Java Message Service settings | 94 |
| About Fortify Software Security Center user authentication | 95 |
| LDAP user authentication | 95 |
| Implementation of SCIM 2.0 protocol | 112 |
| Configuring a proxy for integrations | 117 |
| Enabling the running and management of OpenText ScanCentral DAST scans | 119 |
| Configuring a Kafka Stream to use with OpenText ScanCentral DAST | 120 |
| Enabling integration with Fortify ScanCentral SAST | 122 |
| Configuring job scheduler attributes | 123 |
| Recurring cleanup jobs | 128 |
| About data retention | 130 |

| | |
|---|-----|
| Configuring secure browser access | 134 |
| About configuring Fortify Software Security Center to work with single sign-on | 136 |
| Configuring logging | 144 |
| Running in a Federal Information Processing Standards (FIPS) environment | 144 |
| Setting the required password strength for Fortify Software Security Center sign in | 145 |
| About audit issue history | 145 |

About integrating components with Fortify Software Security Center

The following table lists the components you can integrate with Fortify Software Security Center.

| Component | Integration instructions |
|--|--|
| Security training vendors | "Configuring application security training" on page 77 |
| OpenText™ Fortify Audit Assistant | "Configuring Fortify Audit Assistant" on page 78 |
| Java Message Service (JMS) | "Configuring Java Message Service settings" on page 94 |
| LDAP servers | "Configuring LDAP servers" on page 98 |
| System for Cross-domain Identity Management (SCIM) | "Implementation of SCIM 2.0 protocol" on page 112 |
| OpenText ScanCentral DAST | "Enabling the running and management of OpenText ScanCentral DAST scans" on page 119 |
| Fortify ScanCentral SAST | "Enabling integration with Fortify ScanCentral SAST" on page 122 |
| Single sign-on (SSO) | "About configuring Fortify Software Security Center to work with single sign-on" on page 136 |
| Bug tracking systems | "About bug tracking system integration" on page 148 |
| Software composition analysis | <ul style="list-style-type: none">• "Preparing to display OpenText Core SCA (Debricked) results" on page 152• "Preparing to display Sonatype results" on page 153 |

| Component | Integration instructions |
|---|--|
| 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 Fortify Software Security Center 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 Fortify Software Security Center can fail.

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, Fortify Software Security Center applies the following rules:

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

These adjustments are required to calculate average dates correctly. For example, without these adjustments, the calculated averages would be zero for issues that were found and audited on the same date, which is not correct. For an issue found on March 2 and audited 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, Fortify Software Security Center calculates the average of two values—(auditTime - foundDate) and (removedDate - foundDate)—to get average number of days to audit and remediate issues.

Setting the Issue Stats thresholds

You set the thresholds that determine what users see when they review summary information about the application versions to which they have access. By default, the **Issue Stats** page displays values of fewer than 100 days (minimum) in 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.

THRESHOLDS

Max Issue Age ⓘ

365

Average Days to Review ⓘ

Min. 100 Max. 365

Average Days to Remediate ⓘ

Min. 100 Max. 365

CANCEL **SAVE**

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

Configuring application security training

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

To enable application security training on Fortify Software Security Center:

1. On the 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 Fortify Software Security Center 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" on page 282](#)

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. Fortify Software Security Center can work with Fortify Audit Assistant to help determine whether the issues returned in OpenText 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 Core Application Security (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.

See also

["Configuring Fortify Audit Assistant" below](#)

["Using Fortify Audit Assistant with Fortify Software Security Center" on page 297](#)

["Fortify Audit Assistant workflow" on page 301](#)

Configuring Fortify Audit Assistant

Fortify Software Security Center 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](#).

To configure Fortify Software Security Center 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 **Audit Assistant**.
4. 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 Fortify Software Security Center integrations (see "Configuring a proxy for integrations" on page 117 , you can select this check box to use that proxy for Fortify Audit Assistant. |

5. 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.
6. 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. Fortify Software Security Center verifies new policies it receives from Fortify Audit Assistant every time a user clicks **REFRESH POLICIES**.) If Fortify Software Security Center detects one or more invalid policies, it displays a table that shows the mapping from the original policy to the changed policy. You can then identify each obsolete policy and map its valid replacement. Fortify Software Security Center updates the policies based on the changes you submit in the mapping table.

7. 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.)
8. 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" on page 229](#).

9. To enable Fortify Software Security Center 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" on page 229](#)). For information about the auto-predict feature, see ["About Fortify Audit Assistant auto-prediction" below](#).

10. 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" on page 229](#)).

Important! Before you can use the auto-apply feature, you must first map Fortify Audit Assistant analysis tag values to Fortify Software Security Center Analysis tag values (see ["Mapping Fortify Audit Assistant analysis tag values to Fortify Software Security Center custom tag values" on page 298](#)).

11. Click **SAVE**.

See also

Updating the Fortify Audit Assistant configuration

["Using Fortify Audit Assistant with Fortify Software Security Center" on page 297](#)

["Fortify Audit Assistant workflow" on page 301](#)

["Mapping Fortify Audit Assistant analysis tag values to Fortify Software Security Center custom tag values" on page 298](#)

About Fortify Audit Assistant auto-prediction

By setting auto-predict to yes, you can configure Fortify Software Security Center 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" on page 78](#)). 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" on page 230](#)).

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 Fortify Software Security Center 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" below](#)

["Setting report generation timeout" below](#)

Allocating memory for report generation

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

1. On the 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**.

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**.

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™ Fortify WebInspect 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" on page 86](#).

To configure Fortify Software Security Center 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**.
4. 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 Fortify Software Security Center password is valid before the user must change it. The default value is 30. |
| Login attempts allowed before a user is locked out | Number of times a local user can try to sign in to Fortify Software Security Center using invalid credentials before the user's account is locked. If Fortify Software Security Center locks a user out, that user is prevented from attempting a new login for the number of minutes specified in the Lockout time (minutes) box. For information about how to unlock a user account, see "Unlocking local user accounts" on page 192 . 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 Fortify Software Security Center the number of times specified for Login Attempts before Lockout , Fortify Software Security Center locks the user account for the number of |

| Field | Description |
|---|---|
| | <p>minutes specified in the Lockout time (minutes) box.</p> <p>The default value is 30.</p> |
| User lookup strategy | <p>If LDAP is enabled, select one of the following user lookup strategies from this list:</p> <ul style="list-style-type: none"> • 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 | <p>Select this check box to display the following user information, when applicable: login name, first and last names, and email address.</p> |
| Maximum events per WebInspect Agent Issue | <p>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.</p> <p>The default value is 5.</p> |
| Inactive session timeout (minutes) | <p>Number of minutes a user can be inactive before Fortify Software Security Center automatically logs the user off.</p> <p>The default value is 30.</p> |

| Field | Description |
|--|---|
| Locale for Rulepacks | <p>Type one of the following:</p> <ul style="list-style-type: none"> • ja (Japanese) • zh_CN (simplified Chinese) • zh_TW (traditional Chinese) • es (Spanish) • pt_BR (Portuguese Brazilian) <p>Note: There is no need to specify a value for English.</p> |
| Rulepack update URL | <p>URL for the Rulepack update server. The default value is <code>https://update.fortify.com</code>.</p> <p>Important! Do not change the default value of the Rulepack Update URL field unless your Customer Support representative directs you to do so.</p> |
| Use SSC proxy for Rulepack update | <p>Select this check box to enable use of the Fortify Software Security Center proxy, if the Rulepack update server is behind it.</p> <p>Note: You must enable and correctly configure the Fortify Software Security Center proxy. For information, see "Configuring a proxy for integrations" on page 117.</p> |
| User administrator's email address (for user account requests) | <p>Email address of the user who is to receive system email alerts and notifications when email notifications are enabled.</p> <p>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.</p> |
| Enable export to CSV from the Dashboard and AUDIT views | <p>By default, users can export Fortify Software Security Center 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.</p> <p>Note: If you are changing only this setting on the Core page, a server restart is not required to implement the change.</p> |

5. Click **SAVE**.

6. Restart the server.

See also

["Unlocking local user accounts" on page 192](#)

About configuring a proxy for Rulepack updates

By default, Fortify Software Security Center 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 Fortify Software Security Center integrations, see ["Configuring a proxy for integrations" on page 117](#).

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" on page 83](#)

Blocking data export to CSV files

By default, users can export Fortify Software Security Center 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 Fortify Software Security Center data to CSV files:

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

See also

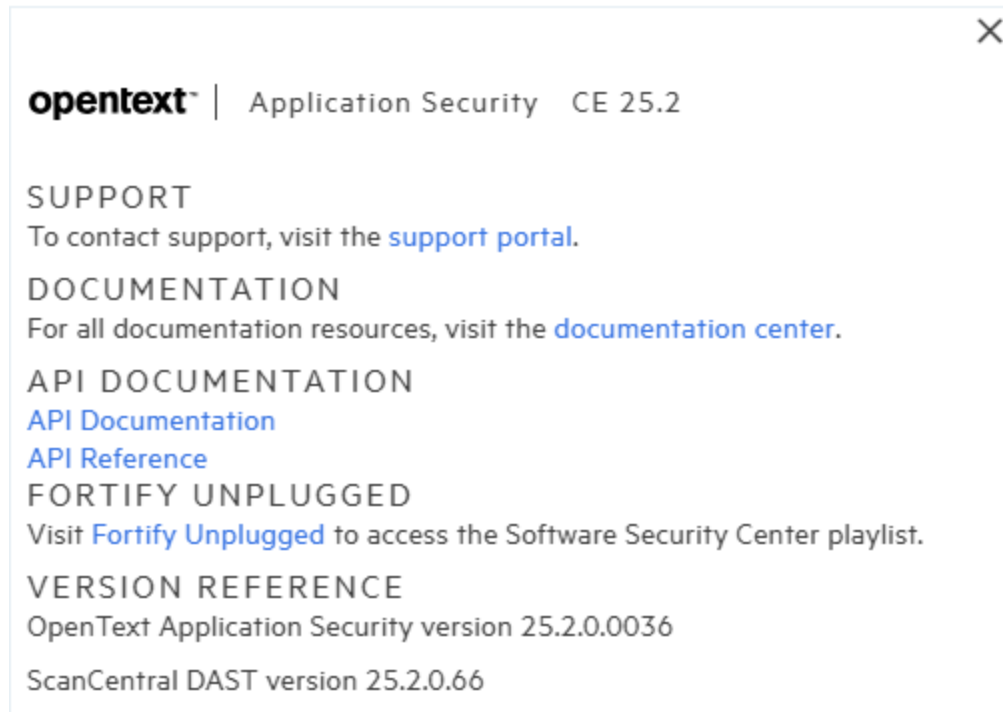
["Configuring core settings" on page 83](#)

["Exporting the Dashboard summary table" on page 183](#)

["Exporting selected data for an application version" on page 214](#)

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 Fortify Software Security Center 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" on the next page](#)

["Adding a Fortify Insight link to the Dashboard" below](#)

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

See also

["Customizing the banner for your organization" below](#)

["Changing the support contact link in the About box" on page 86](#)

["Creating a system-wide banner" on the next page](#)

Customizing the banner for your organization

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

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

To create a custom 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>Add your custom banner here</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 Fortify Software Security Center 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 Fortify Software Security Center 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;">Add your custom banner here</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 Fortify Software Security Center 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 Fortify Software Security Center server.

See also

["Adding a Fortify Insight link to the Dashboard" on page 87](#)

["Creating a system-wide banner" below](#)

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 Fortify Software Security Center 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**.

See also

["Customizing the banner for your organization" on page 88](#)

["Adding a Fortify Insight link to the Dashboard" on page 87](#)

Configuring email alert notification settings

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

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

Note: For information about how to configure the receipt of email alerts, see ["Configuring whether to receive email alerts" on page 92](#).

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 Fortify Software Security Center, you must enable and configure the email service settings.

1. Sign in to Fortify Software Security Center 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 in the following table.

| Field | Description |
|---------------------------------------|---|
| Enable email | Select this check box to enable Fortify Software Security Center to send email messages of all types and to add the "Can't access or need an account?" link to the sign in dialog box. This check box is cleared by default. |
| From email address | Type the email address that Fortify Software Security Center uses to identify emails sent from Fortify Software Security Center. For example, <code>fortifyserver@example.com</code> . |
| Default encoding of the email content | Type the encoding method to be used for the email content. The default value is UTF-8. |
| SMTP server | Type the fully-qualified domain name for the SMTP server. For example, <code>mail.example.com</code> . |
| SMTP server port | Type the port number for the SMTP server. The default value is 25. |
| SMTP username | If authentication is required on the SMTP server, type the SMTP username. |
| SMTP password | If authentication is required on the SMTP server, type the SMTP password. |
| 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: <ul style="list-style-type: none">• (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. |

| Field | Description |
|---|--|
| 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. |

5. Click **SAVE**.

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**.

PREFERENCES

System-wide Preferences

☒ Receive email alerts from Software Security Center

☐ Disable hotkeys

☐ Turn on enhanced accessibility features

Date format **MM/DD/YYYY**

Time format **12 Hour AM/PM**

UI Theme **Light**

Preferences for all application versions (To override these settings for a specific application version, go to the Profile page for that application version)

☐ Show suppressed issues

☐ Show removed issues

☐ Show hidden issues

☒ Use short filenames ⓘ

CANCEL

SAVE

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" on page 90](#)

["Creating alerts" on page 256](#)

["Deleting alerts" on page 259](#)

Setting the strategy for resolving issue audit conflicts

If multiple auditors are working on the same issue using different products (Fortify Software Security Center, Fortify Audit Workbench, or any of the Secure Code Plugins), they might assign different values to a given custom tag. Previously, if Fortify Software Security Center detected an audit conflict such as this, it ignored all client-side changes and resolved the conflict in favor of the existing custom tag value on Fortify Software Security Center.

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

Example of the default strategy for resolving audit conflicts

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 Fortify Software Security Center.

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

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

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

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

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

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

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

1. Sign in to Fortify Software Security Center 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 Fortify Software Security Center 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" on page 271](#)

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. |

| Field | Description |
|-----------|--|
| | This check box is selected by default. |
| JMS topic | Type the JMS message topic. The default value is <code>Fortify.Advisory.EventNotification</code> . |

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

About Fortify Software Security Center user authentication

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

Database-only authentication imposes a separate administrative process for creating and managing Fortify Software Security Center user accounts and roles. You can augment the Fortify Software Security Center default database-only authentication using LDAP or a SCIM 2.0 API client. For Information about LDAP user authentication, see ["LDAP user authentication" below](#). For Information about SCIM 2.0 user provisioning, see ["Implementation of SCIM 2.0 protocol" on page 112](#).

LDAP user authentication

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

The topics in this section provide information about user authentication in Fortify Software Security Center 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" on page 109](#)

["About managing LDAP user roles" on page 156](#)

Preparing to configure LDAP authentication

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

1. Download an LDAP management application.

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

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

Note: For information about how to configure the primary source for looking up users, see ["Configuring core settings" on page 83](#).

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

3. Check for conflicts between account names.

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

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

4. Gather and record required information.
5. OpenText recommends that you disable the referrals feature.

See ["About the LDAP server referrals feature" on the next page](#) and ["Disabling LDAP referrals support" on page 98](#).

See also

["Configuring LDAP servers" on page 98](#)

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. Fortify Software Security Center searches for users based on the `usernameAttribute` specified for a given LDAP server configuration. Because the searches are performed across all the servers, it is important that the searches return just a single result. Be sure to use username attributes that

result in unique search hits across all your configured LDAP servers. For example, if you use multiple Active Directories, it 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 Fortify Software Security Center finds a given username in more than one LDAP server during login, it tries to resolve this by using the password with all instances of the username, and then uses the instance that the password authenticates first. In most cases, a user with a non-unique username can successfully sign in to Fortify Software Security Center and access most of the user interface functionality. However, some functionality, including report generation, token-based authentication, and OpenText 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 DN's by Fortify Software Security Center. The simplest (and recommended) way to achieve this is to ensure that none of the configured baseDN's 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 DN's) must also be managed by the second LDAP server. For example, if you have one LDAP server configuration with the base DN `DC=acme,DC=com`, but the `OU=org,DC=acme,DC=com` subtree is managed by another LDAP server, you can set up a second LDAP configuration to manage just the `OU=org,DC=acme,DC=com` LDAP subtree. But you *must* ensure that none of the LDAP objects registered in Fortify Software Security Center from the first LDAP server reference (directly or transitively) the `OU=org,DC=acme,DC=com` subtree, and vice versa.

If this requirement is not satisfied...

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

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

If referrals are not used on your LDAP server, OpenText recommends that you disable referrals support in the LDAP library. Disabling this option on the Fortify Software Security Center server side

makes Fortify Software Security Center-to-LDAP communication much faster. For instructions, see ["Disabling LDAP referrals support" below](#).

Note: For a complete description of referrals, go to [Referrals in the LDAP](#) in the Oracle documentation.

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**.

Configuring LDAP servers

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

Important! Before you configure the properties on the **LDAP** page, you must prepare for LDAP authentication as described in ["LDAP user authentication" on page 95](#). 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 Fortify Software Security Center:

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 | |

| Field | Description |
|--------------------------------|--|
| Enable this LDAP configuration | Select this check box to make this LDAP server available for Fortify Software Security Center to use. |
| Server name | <p>Type a unique name for this server.</p> <p>Important! If you configure multiple LDAP servers, ensure that you specify a unique server name for each.</p> |
| Server URL | <p>Type the LDAP authentication server URL.</p> <p>If you use unsecured LDAP, type the URL in the following format:</p> <pre>ldap://<hostname>:<port></pre> <p>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.</p> <p>If you use secured LDAPS, type the URL in the following format:</p> <pre>ldaps://<hostname>:<port></pre> <p>LDAPS ensures that only encrypted user credentials are transmitted.</p> |
| Base DN | <p>Type the base distinguished name (DN) for LDAP directory structure searches.</p> <p>Important! If you configure more than one LDAP server for Fortify Software Security Center, then you must set a unique base DN for each of them.</p> <p>For example, the base DN for <code>companyName.com</code> is <code>dc=companyName,dc=com</code>.</p> <p>All DN values are case-sensitive, must not</p> |

| Field | Description |
|--------------------|--|
| | <p>contain extra spaces, and must exactly match LDAP server entries.</p> <p>If you specify no value, Fortify Software Security Center searches from the root of LDAP objects tree. With multiple LDAP servers, the base DN must be unique for each. If the base DN for one server is empty, it cannot be empty for another LDAP server.</p> |
| Bind user DN | <p>Type the full distinguished name (DN) of the account Fortify Software Security Center 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 Fortify Software Security Center.</p> <p>This account must be a minimum privilege, read-only authentication server account that you created for exclusive use by Fortify Software Security Center.</p> <div> <p>Important! For security reasons, never use a real user account name in a production environment.</p> </div> <p>If you use Active Directory, specify the domain name and username in the following format:</p> <p><code><domain_name>\<username></code></p> |
| Bind user password | Type the password for the bind user DN account. |
| Show password | Select this check box to show entered passwords. |

| Field | Description |
|---------------------------------|--|
| Relative search DN (1 per line) | <p>(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 Fortify Software Security Center users takes too long, use an RDN to limit the number of LDAP entries searched. You can also use an RDN to hide some part of the LDAP tree from Fortify Software Security Center for security reasons.</p> <p>For example, to search within the base DN <code>companyName.com</code> and all entries under that base DN, specify the following to recursively search all entries under that path:</p> <pre>cn=users or cn=users,ou=divisionName</pre> |
| Ignore partial result exception | <p>To avoid search failures when search results include more records than the LDAP server can return, leave this check box selected.</p> <p>You can also enable this 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, Fortify Software Security Center silently returns only 500 records.</p> |
| LDAP server type | <p>From this list, select the type of LDAP server you are connecting with Fortify Software Security Center (either ACTIVE_DIRECTORY or OTHER).</p> |

| Field | Description |
|----------------------------|--|
| 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 Fortify Software Security Center 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 <code>objectClass</code> , Fortify Software Security Center looks at the <code>objectClass</code> attribute to determine the entity type to search. The default value is <code>objectClass</code> . |
| Organizational unit class | Type the object class that defines an LDAP object as an organizational unit. The default value is <code>container</code> . |
| User class | Type the object class that identifies an LDAP object type as a user. The default |

| Field | Description |
|------------------------------------|--|
| | 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 Fortify Software Security Center looks at to find the distinguished name of the entity. The default value is distinguishedName. |
| USER LOOKUP SCHEMA | |
| User firstname attribute | Type the user object attribute that specifies a user's first name. The default value is givenName. |
| User lastname attribute | Type the user object attribute that specifies a user's last name. The default value is sn. |
| Group name attribute | Type the group attribute that specifies the group name. The default value is cn. |
| User username attribute | Type the user object attribute that specifies a username. The default value is sAMAccountName. |
| User password attribute | Type the user object attribute that specifies a user's password. The default value is userPassword. |
| Group member attribute | Type the group attribute that defines the members of the group. The default value is member. |

| Field | Description |
|--|---|
| 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 | <p>Select this check box to enable LDAP user data caching in Fortify Software Security Center.</p> <p>You can refresh the LDAP cache manually from the Administration view in Fortify Software Security Center. For instructions, see "Refreshing LDAP entities manually" on page 111.</p> <div> <p>Note: OpenText recommends that you leave LDAP user caching enabled. Fortify Software Security Center periodically updates the LDAP cache automatically.</p> </div> |
| 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. |

| Field | Description |
|--|--|
| 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, see "About the LDAP server referrals feature" on page 97 . |
| LDAP authenticator type | From this list, select one of the following LDAP authentication types to use: <ul style="list-style-type: none">• BIND_AUTHENTICATOR— |

| Field | Description |
|---|---|
| | <p>Authentication directly to the LDAP server ("bind" authentication).</p> <ul style="list-style-type: none"> • PASSWORD_COMPARISON_AUTHENTICATOR—The password the user supplies is compared to the one stored in the repository. <p>For more information about LDAP authentication types, go to https://spring.io/projects/spring-security.</p> |
| LDAP password encoder type | <p>Select a value from this list only if the LDAP authentication method is password comparison.</p> <p>You must select the encoder type that the LDAP server uses. Fortify Software Security Center compares encoded passwords. If, for example, the LDAP server uses LDAP_SHA_PASSWORD_ENCODER to encode passwords, but you select MD4_PASSWORD_ENCODER, password comparisons will fail.</p> |
| Enable nested LDAP groups | <p>Select this check box to enable nested group support for LDAP in Fortify Software Security Center (wherein a given group member might itself be a group).</p> <div> <p>Note: Use nested LDAP groups only if absolutely required. Enabling nested LDAP groups forces Fortify Software Security Center 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.</p> </div> |
| Interval between LDAP server validation | Type the number of milliseconds the LDAP |

| Field | Description |
|--------------------------------------|--|
| attempts (ms) | server waits after a validation attempt before next attempting a validation. The default value is 5000. |
| Time to wait LDAP validation (ms) | Type the length of time (in milliseconds) that Fortify Software Security Center 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" on the next page](#)

["Importing an LDAP server configuration" on page 109](#)

["LDAP user authentication" on page 95](#)

["Registering LDAP entities" on the next page](#)

["Deleting an LDAP server configuration" below](#)

["About managing LDAP user roles" on page 156](#)

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" on page 98](#).
6. To check the validity of the configuration, click **VALIDATE CONNECTION**.
7. To save the configuration after successful validation, click **SAVE**.

See also

["Registering LDAP entities" on the next page](#)

["LDAP user authentication" on page 95](#)

["About managing LDAP user roles" on page 156](#)

Deleting an LDAP server configuration

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

To delete an LDAP server 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 Fortify Software Security Center server.

See also

["LDAP user authentication" on page 95](#)

["Registering LDAP entities" below](#)

["About managing LDAP user roles" on page 156](#)

Importing an LDAP server configuration

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

To import your legacy LDAP server configuration:

1. On the 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 Fortify Software Security Center 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" on page 98](#)).

5. Correct any problems, and then click **NEXT**.
6. Configure the attributes described in the table in step 4 in ["Configuring LDAP servers" on page 98](#).
7. To check the validity of the configuration, click **VALIDATE CONNECTION**.
8. To check the validity of and save the configuration, click **SAVE**.

See also

["Registering LDAP entities" below](#)

["LDAP user authentication" on page 95](#)

["About managing LDAP user roles" on page 156](#)

Registering LDAP entities

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

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

1. Sign in to Fortify Software Security Center 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.

| Name | Distinguished Name | Last Name | First Name | Email |
|---------|--------------------------------------|-----------|------------|-------|
| ssuser1 | CN=SSCUser1,CN=Users,DC=sscqa,DC=com | User1 | SSCUser1 | |

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.

- a. Click **+ ADD**.
- b. From the **Application** list in the **SELECT APPLICATION VERSION** dialog box, select the name of an application that you want the LDAP entity to access.
Fortify Software Security Center lists all active versions of the application.
- c. To display inactive versions of the application, select the **Show inactive versions** check box.
- d. Select the check boxes for all of the versions that you want the entity to access.
- e. Click **DONE**.

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

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**.

Fortify Software Security Center 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" on page 98](#).

See also

["LDAP user authentication" on page 95](#)

["About managing LDAP user roles" on page 156](#)

Refreshing LDAP entities manually

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

To initiate the LDAP refresh process manually:

1. 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" on page 98](#).

See also

["LDAP user authentication" on page 95](#)

["Registering LDAP entities" on page 109](#)

["About managing LDAP user roles" on page 156](#)

Handling LDAP entries marked "Invalid"

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

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

To update the DN value for an LDAP entity:

1. On the 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" on page 98](#)

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

Changing the default cache refresh interval

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

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

1. Shut down Fortify Software Security Center.
2. 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 Fortify Software Security Center.

Implementation of SCIM 2.0 protocol

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

Note: You can integrate with any SCIM 2.0 API client. However, if you do, you must test its interoperability with Fortify Software Security Center independently. 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 Fortify Software Security Center.
- Users can only sign in using SSO.
- If a username created locally (**Administration** > **Users** > **Local Users**) already exists in Fortify Software Security Center, a user with the same username cannot be provisioned using SCIM. Users created from the **Administration** view are read-only for SCIM provisioning.

Supported SCIM resources

Fortify Software Security Center supports the following SCIM resources:

- User (urn:ietf:params:scim:schemas:core:2.0:User schema)
Fortify Software Security Center accepts all standard attributes of the User Schema, but stores only a subset of these (see ["User attribute mappings" below](#)). Also accepts Enterprise User extension attributes (urn:ietf:params:scim:schemas:extension:enterprise:2.0:User schema) but does not store them.
- Group (urn:ietf:params:scim:schemas:core:2.0:Group schema)
Fortify Software Security Center accepts all standard attributes from the Group Schema, but stores only a subset of these (see ["Group attribute mappings" on the next page](#)).

Optional features supported:

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

User attribute mappings

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

| SCIM user attribute | Fortify Software Security Center 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 |

| SCIM user attribute | Fortify Software Security Center user attribute | Comment |
|---------------------------|---|--|
| | | Fortify Software Security Center is set accordingly. |
| name.givenName | firstName | |
| name.familyName | lastName | |
| emails[type="work"].value | email | |

Group attribute mappings

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

| SCIM group attribute | Fortify Software Security Center 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" on the next page](#)

["Configuring SAML 2.0-compliant single sign-on" on page 137](#)

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 Fortify Software Security Center 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 Fortify Software Security Center. | "Enabling SCIM to provision externally managed users and groups" on page 117 |
| In Microsoft Entra, go to Microsoft Entra ID and create an enterprise application. | Microsoft Entra ID documentation <div> <p>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.</p> </div> |
| From Entra ID, assign users and groups to the new application. | Microsoft Entra ID documentation |
| <p>From Entra ID, provision the application.</p> <p>Note the following:</p> <ul style="list-style-type: none"> Set Provisioning Mode to Automatic. Use the Fortify Software Security Center URL for the Tenant URL value, and append to it the following string: <code>/api/scim/v2?aadOptscim062020</code> <div> <p>Note: <code>/api/scim/v2</code> is the URL for the Fortify Software Security Center SCIM endpoint. The <code>aadOptscim062020</code> query parameter improves Entra ID compliance with SCIM v2.0.</p> </div> <ul style="list-style-type: none"> For the Secret Token value, use the token you created in Fortify Software Security Center (SCIM Token - see "Enabling SCIM to provision externally managed users and groups" on page 117.) | Microsoft Entra ID documentation |

| Task | For details |
|--|--|
| <p>From Entra ID, change the attribute mappings for data flow between Entra ID and Fortify Software Security Center.</p> <p>Delete all but the following attributes for your users (for groups, you change no attribute mappings):</p> <ul style="list-style-type: none"> • userName • active • emails[type eg "work"].value • name.givenName • name.familyName • externalID <p>Ensure that you move the Provisioning Status toggle to On.</p> | <p>Microsoft Entra ID documentation</p> |
| <p>Entra ID SAML metadata is signed. For Fortify Software Security Center 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).</p> <p>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.</p> | <p>Microsoft Entra ID documentation</p> <p>"Configuring SAML 2.0-compliant single sign-on" on page 137</p> |
| <p>Set up SAML single sign-on from Fortify Software Security Center.</p> | <p>"Configuring SAML 2.0-compliant single sign-on" on page 137</p> |
| <p>Acquire the metadata XML file from Fortify Software Security Center and save it locally. This file can be accessed only if SAML SSO is enabled in Fortify Software Security Center and successfully initialized.</p> | <pre><hostname>:<port>/<app_ context>/saml/<metadata></pre> |

| Task | For details |
|---|---|
| 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 Fortify Software Security Center, assign roles and application versions to externally managed users and groups. | "Viewing externally managed users and groups" on page 193 |

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 Fortify Software Security Center SCIM API.
Use that token as a Secret Token in Entra ID when you configure the connection between Fortify Software Security Center 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 Fortify Software Security Center, it must be protected. OpenText recommends that you use a secure random string generator to generate the token.

6. Click **SAVE**.

See also

["Configuring SAML 2.0-compliant single sign-on" on page 137](#)

["Implementation of SCIM 2.0 protocol" on page 112](#)

["Viewing externally managed users and groups" on page 193](#)

Configuring a proxy for integrations

You can configure a single proxy for use with all HTTP(s) protocol-based integrations with Fortify Software Security Center. 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 Fortify Software Security Center 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" on page 78](#)

["Configuring core settings" on page 83](#)

["Assigning a bug tracking system to an application version" on page 219](#)

Enabling the running and management of OpenText ScanCentral DAST scans

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

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

1. Create a service account for OpenText ScanCentral DAST to authenticate with Fortify Software Security Center. For instructions on how to use this service account in the OpenText ScanCentral DAST deployment, see the *OpenText™ 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 ScanCentral DAST and Fortify Software Security Center. Do not use the account for access by an OpenText ScanCentral DAST user.
2. Enable OpenText ScanCentral DAST integration in Fortify Software Security Center by doing the following:
 - a. Sign in to Fortify Software Security Center as an Administrator.
 - b. On the header, select **Administration**.
 - c. On the navigation pane, expand **Configuration**, and then select **ScanCentral DAST**.
 - d. On the **ScanCentral DAST** page, select the **Enable ScanCentral DAST** check box.
 - e. In the **ScanCentral DAST server URL** box, type your OpenText ScanCentral DAST server URL.

The OpenText 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.

- f. Click **SAVE**.

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

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

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 Fortify Software Security Center with OpenText ScanCentral DAST.

To configure Fortify Software Security Center 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 Fortify Software Security Center 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. Fortify Software Security Center 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 |

| Field | Description |
|-------|---|
| | 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.

Enabling integration with Fortify ScanCentral SAST

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

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

To configure the integration:

1. Sign in to Fortify Software Security Center 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 Fortify Software Security Center.

6. In the **ScanCentral poll period (seconds)** box, type the number of seconds to elapse between sessions of data polling from Fortify ScanCentral SAST.
7. In the **SSC and ScanCentral controller shared secret** box, type the shared secret key (unencrypted) so that Fortify Software Security Center 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 Fortify Software Security Center server.

See also

["Fortify ScanCentral SAST permissions" on page 319](#)

["Viewing Fortify ScanCentral SAST Controller information" on page 323](#)

["About Fortify ScanCentral SAST sensor pools" on page 325](#)

["Creating Fortify ScanCentral SAST sensor pools" on page 326](#)

Configuring job scheduler attributes

You can configure scheduling attributes for processing Fortify Software Security Center 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 | <p>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.</p> <p>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.</p> <p>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.</p> <div>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</div> |

| Field | Description |
|---|---|
| | <p>volume of jobs from queuing up for processing later.</p> <p>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.</p> |
| Token management | |
| Token expiration alerts | <p>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.</p> <p>The default value is 7 (days).</p> <p>Note: The start of the day is 12 AM in the Fortify Software Security Center server locale.</p> |
| <p>Snapshot refresh Use the fields in this area to schedule the snapshot job.</p> <p>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.</p> <p>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.</p> | |
| Days of the week | <p>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.</p> <p>Note: Use uppercase letters for three-letter abbreviations. Spaces between the entries are optional.</p> <p>To specify consecutive days, separate the entries with a dash. For example, enter MON-FRI to run the scheduler on week days only.</p> <p>Enter an asterisk (*) run the scheduler every day (the default).</p> |

| Field | Description |
|--|--|
| Hours | <p>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.</p> <p>Enter an asterisk (*) to run the scheduler every hour.</p> <p>The default value is 0 (midnight).</p> |
| Minutes | <p>Type the minute at which the recurring scheduler job is to start running. For example, enter 24 to start the job at 24 minutes past the hour that you entered in the Hours box.</p> <p>The default value is 0, which indicates that the job starts running in the first minute.</p> |
| <p>Index maintenance Use the fields in this area to schedule your Fortify Software Security Center full text search index maintenance. OpenText recommends that you run this job daily.</p> <p>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.</p> | |
| Days of the week | <p>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.</p> <p>To run the scheduler on multiple days, separate the entries with a comma. For example, enter SUN, WED, FRI or 1, 4, 6.</p> <p>Note: Use uppercase letters for three-letter abbreviations. Spaces between the entries are optional.</p> <p>To specify consecutive days, separate the entries with a dash. For example, enter MON-FRI to run the scheduler on week days only.</p> <p>Enter an asterisk (*) to run the scheduler every day (the default).</p> |
| Hours | <p>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.</p> <p>Enter an asterisk (*) to run the scheduler every hour.</p> <p>The default value is 0 (midnight).</p> |

| Field | Description |
|--------------------------------|---|
| Minutes | <p>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.</p> <p>The default value is 0, which indicates the job starts running in the first minute.</p> |
| Events maintenance | |
| Days to preserve | <p>Type the number of days after which Fortify Software Security Center removes past events. To specify no event removal, enter 0 (zero).</p> <p>Fortify Software Security Center uses the new value during the next run of the dedicated cleaning job. A new job is created daily at 11:30 PM and if it is not blocked, it starts its work immediately.</p> <p>The default value is 0, which indicates that no cleanup occurs.</p> |
| Reports maintenance | |
| Days to preserve | <p>Type the number of days Fortify Software Security Center is to retain generated reports. The default value is 0, which indicates that no cleanup occurs.</p> <p>To ensure that the cleanup job is not too time- or resource-intensive, each nightly run clears a maximum of 2000 old reports (and associated entities). Fortify Software Security Center then gradually cleans up the remaining reports over the following days.</p> |
| Data export maintenance | |
| Days to preserve | <p>Type the number of days Fortify Software Security Center is to retain exported audit reports.</p> <p>The default value is 2.</p> <p>Note: This job is run every day at 11:45 PM (23:45)</p> |

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

See also

["Setting job execution priority" on the next page](#)

["Configuring background job execution strategy" on page 361](#)

["Canceling scheduled jobs" on the next page](#)

["Recurring cleanup jobs" on the next page](#)

Setting job execution priority

All new jobs in Fortify Software Security Center are scheduled with priority set to **Very Low**. Multiple jobs that have the same priority are processed in the order in which they are added to the 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 Fortify Software Security Center 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" below](#)

["Configuring job scheduler attributes" on page 123](#)

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 Fortify Software Security Center 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" on page 123](#)

Recurring cleanup jobs

Fortify Software Security Center 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 attributes" on page 123). | dataexport documentinfo datablob | Daily at 23:45 h For instructions on how to schedule this job, see "Configuring job scheduler attributes" on page 123 . |
| 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 attributes" on page 123 . |
| 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 attributes" on page 123 . |
| 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 |

| Job name | Description | Affected tables | Default schedule |
|-------------------------------|--|---|--|
| 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 attributes" on page 123 . |
| 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 attributes" on page 123 . |
| 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 attributes" on page 123 . "Configuring job scheduler attributes" on page 123 |
| Alert Reminder | Sends reminder alerts. | N/A | Daily at 03:00 h |

| Job name | Description | Affected tables | Default schedule |
|---------------------|--|-----------------|------------------|
| Token Expiry Alerts | Notifies users of any tokens to expire soon. | N/A | Daily at 03:00 h |

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 Fortify Software Security Center. 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 Fortify Software Security Center. You can schedule the data cleanup service that purges artifacts from Fortify Software Security Center when you enable data retention.

Caution! After an artifact is purged, the artifact is permanently removed from Fortify Software Security Center and cannot be recovered.

When you enable data retention, Fortify Software Security Center 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.

Enabling data retention

To enable the Fortify Software Security Center 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. |

| Field | Description |
|-------|--|
| | <p>Use the values 1 to 7 to specify the day of the week (Sunday to Saturday) where 1 represents Sunday and 7 represents Saturday</p> <p>Use cron syntax to specify one or more days of the week as described in the following examples:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> |
| Hours | <p>(Required) Type the time of day the data cleanup service will run.</p> <p>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.</p> <p>Use cron syntax to specify one or more hours in the day as described in the following examples:</p> <ul style="list-style-type: none"> • 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. |

| Field | Description |
|-------|--|
| | <ul style="list-style-type: none"> • 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. <p>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 Fortify Software Security Center nightly maintenance jobs are scheduled to run by default.</p> |

4. Click **SAVE**.

See also

["Editing the default data retention policy" below](#)

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:

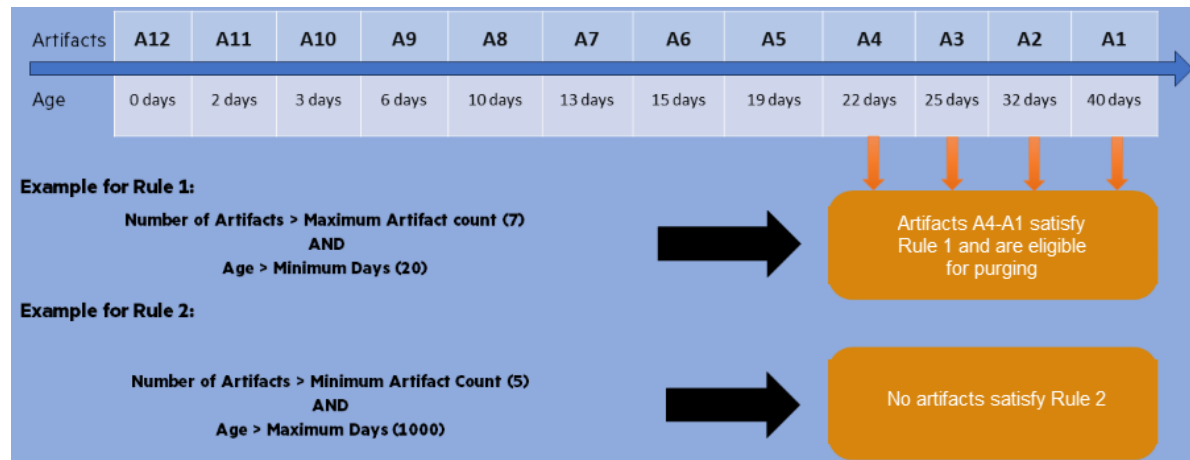
What is the maximum number of unpurged artifacts you want to keep per application? * 

Excluding artifacts which are less than days old. * 

What is the maximum age of unpurged artifacts you want to keep per application? Days * 

Except when purging an artifact makes the unpurged artifact count of the application less than * 

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



Fortify Software Security Center purges the artifacts that satisfy at least one rule. Fortify Software Security Center purges artifacts A1 to A4.

5. Click **SAVE**.

Configuring secure browser access

To configure security for browsers that access the Fortify Software Security Center 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 | <p>Specify what (if any) level of CSP to use. Using the HTTP Content-Security-Policy header controls, the resources browsers can load and what actions they can perform on pages loaded from Fortify Software Security Center. This helps guard against cross-site scripting attacks.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> To restrict access to only the base URL configured by the <code>host.url</code> 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 Fortify Software Security Center domain from any host:port. To disable the Content-Security-Policy header, select Disabled. Although OpenText recommends that you <i>not</i> disable the Content-Security-Policy header, this option is available if CSP causes unexpected problems. |
| Set value for Strict-Transport-Security header | <p>Type the value for the Strict-Transport-Security header. This header signals browsers to use HTTPS instead of HTTP to communicate with Fortify Software Security Center.</p> <div> <p>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.</p> </div> <p>The Strict-Transport-Security header is sent only through a secure channel determined by Tomcat server.</p> |
| Set value for Public-Key-Pins header | <p>Type the value for the Public-Key-Pins header. This decreases the risk of man-in-the-middle (MITM) attacks.</p> <div> <p>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.</p> </div> <p>The Public-Key-Pins header is sent only through a secure channel determined by Tomcat server.</p> |

4. Click **SAVE**.

About configuring Fortify Software Security Center 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 Fortify Software Security Center to work with the following single sign-on (SSO) solutions.

| SSO solution | Instructions |
|-----------------------------------|--|
| SAML 2.0-compliant single sign-on | "Configuring SAML 2.0-compliant single sign-on" on the next page |
| HTTP headers | "Configuring single sign-on and single logout solutions that use HTTP headers" on page 141 |
| X.509 certification | "Configuring X.509 certification-based single sign-on" on page 142 |

Configuration restrictions

The following restrictions apply to configuring Fortify Software Security Center to work with SSO solutions:

- You can only use the SSO solutions that Fortify Software Security Center supports to give users access to the user interface.
- At any given time, you can configure only one SSO solution for use with Fortify Software Security Center.
- A user who wants to access Fortify Audit Workbench, fortifyclient, or any of the Secure Code Plugins, must use an LDAP or local Fortify Software Security Center 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, Fortify Software Security Center 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 Fortify Software Security Center. 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 X.509 certification-based single sign-on" on page 142](#).

See also

["About session logout" on page 177](#)

Configuring SAML 2.0-compliant single sign-on

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

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

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

1. If you are using an LDAP directory for users in Fortify Software Security Center and IdP, configure Fortify Software Security Center to use LDAP authentication. Otherwise, IdP users must match local users. For information, see ["LDAP user authentication" on page 95](#).
2. If your IdP runs with SSL (https), configure Fortify Software Security Center to run with SSL. Otherwise, protocol switching while authenticating against IdP could interfere with authentication.
3. Prepare a public/private key pair to be used to digitally sign SAML messages and encrypt SAML Assertions. If your IdP does not require keys signed by a specific certification authority, you can generate your own self-signed key using, for example, OpenSSL or Java's keytool. The following example command generates a keystore that stores a self-signed key under a given alias:

```
keytool -genkeypair -alias <key_alias> -keyalg <RSA_or_EC_algorithm> -  
keystore <keystore_filename> -storepass <password_to_protect_keystore>  
-keypass <password_to_protect_key> -validity <number_of_days_the_key_  
is_valid>
```

Make a note of the values for the alias and both passwords. You must provide them later in the Fortify Software Security Center Administration view.

4. Get SAML metadata from the IdP server and store it on the Fortify Software Security Center file system.
5. Open the metadata file and make a note of the entityID for your IdP EntityDescriptor (<EntityDescriptor entityID="THE_VALUE_YOU_ARE_LOOKING_FOR">).
Also check to see whether the metadata is signed (the <Signature> section is present). If the metadata is signed, the signature is verified with the PKIX validation algorithm and uses all public keys present in the keystore as trust anchors.
Ensure that you include the root CA certificate and intermediary CA certificates of the signature in your keystore.
6. Sign in to Fortify Software Security Center 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 | <p>Location of your identity provider metadata (the metadata obtained in step 3).</p> <p>Examples</p> <ul style="list-style-type: none"> On Windows systems: <code>file:///C:/fortify/federation-metadata.xml</code> On Linux systems: <code>file:///home/fortify/federation-metadata.xml</code> <p>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.)</p> <p>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 <i>not</i> support getting metadata over http proxy.</p> |
| Default IdP | <p>entityID of your IdP EntityDescriptor (from IdP metadata)</p> <p>Note: If you are using the SCIM protocol to provision Fortify Software Security Center 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>.)</p> |
| SP entity ID | <p>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 Fortify Software Security Center instance.</p> |
| SP alias | <p>Service provider alias must include only alphanumeric characters, colons, dashes, and underscores. It cannot contain slashes, hash marks, semicolons, or question marks.</p> |

| Field | Description |
|-----------------------------------|--|
| | Because this field value plays no significant role, you can specify any general value. For example, you can use <code>fortify_ssc</code> . |
| Keystore location | <p>Location of your keystore that stores the key pair for signing SAML messages and encrypting SAML Assertions.</p> <p>Examples:</p> <ul style="list-style-type: none"> • For Windows: <code>file:///C:/fortify/keystore.jks</code> • For Linux: <code>file:///home/fortify/keystore.jks</code> <p>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.</p> |
| Keystore password | Keystore file password |
| Signing & encryption key | Signing/encryption key alias in the keystore file |
| Signing & encryption key password | Signing/encryption key password |
| SAML name identifier | Name of the element in the SAML assertion sent by IdP that holds the authenticated user's username, which matches the Fortify Software Security Center user's username. Use the <code>NameID</code> value if the username is released within the <code><NameID></code> element. If the username is released within one of the <code><Attribute></code> elements, provide the name value of the attribute. This information should be available or configurable in your IdP server. |

10. Click **SAVE**.
11. Verify that the `host.url` property in `<fortify.home>/<app_context>/conf/app.properties` designates a URL that the IdP server can access. The URL is used as a base URL to construct `<AssertionConsumerService>` and `<SingleLogoutService>` locations in Fortify Software Security Center SAML metadata.
12. If the SAML assertion sent from IdP is encrypted, make sure that the authentication response message is signed.

Important! If you are integrating with Active Directory Federation Services (AD FS), set the IdP parameter `Sam1ResponseSignature` to the `MessageAndAssertion` (recommended) or

MessageOnly value.

- 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 Fortify Software Security Center does not work correctly.

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

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

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 [Apache Tomcat 10 Configuration Reference](#) documentation.

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

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

Note: For information about how to obtain extra logging information related to SSO authentication, see ["Enabling debug logging for single sign-on authentication" on page 143](#).

Troubleshooting SAML SSO integration

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

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

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

- The username received in the SAML assertion from IdP does not match any LDAP or local Fortify Software Security Center user account (based on user lookup strategy). Verify the following:
 - The "SAML name identifier" in your Fortify Software Security Center SAML configuration is set to an attribute in the SAML assertion that contains the username.

- The user exists in Fortify Software Security Center and has an assigned role.
- The user lookup strategy is correctly configured (see ["Configuring core settings" on page 83](#)).

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

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

See also

["Configuring single sign-on and single logout solutions that use HTTP headers" below](#)

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

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

1. On the 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 <i>username</i> . |
| 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 Fortify Software Security Center. |
| SSO Logout Response Header | Type the dynamic directive header. |
| SSO Logout Response Code | Type the dynamic directive code. |

| Field | Description |
|--------------------------|-------------------------------------|
| SSO Logout Response Text | Type the dynamic directive message. |

5. Click **SAVE**.
6. Configure Fortify Software Security Center to use LDAP authentication.
For details, see ["LDAP user authentication" on page 95](#).
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" on the next page](#).

See also

["About configuring Fortify Software Security Center to work with single sign-on" on page 136](#)

Configuring X.509 certification-based single sign-on

To configure Fortify Software Security Center 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 Fortify Software Security Center 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 Fortify Software Security Center 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 OID 1.3.6.1.4.1.311.20.2.3. 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 Fortify Software Security Center 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.

Enabling debug logging for single sign-on authentication

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

To obtain extra logging information related to SSO authentication:

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

["About configuring Fortify Software Security Center to work with single sign-on" on page 136](#)

Configuring logging

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

Important! Fortify Software Security Center 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 Fortify Software Security Center 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 Fortify Software Security Center 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.

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 Fortify Software Security Center in a FIPS-compliant environment running on Red Hat Enterprise Linux 9 (RHEL 9). While there is no configuration required to run Fortify Software Security Center 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 Fortify Software Security Center.

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

Before you run Fortify Software Security Center in a FIPS environment:

- Ensure that you are using Fortify Software Security Center version 24.4.0 or later. Otherwise, you must migrate the Fortify Software Security Center keystore that stores a `secret.key` file to encrypt sensitive data.

For more information, see ["About the <fortify.home> directory" on page 64](#).

- Ensure that LDAP servers, SMTP servers, and webhooks are configured as secure connections.

Note: The Fortify Software Security Center container does not support enabling FIPS mode for Java.

Setting the required password strength for Fortify Software Security Center 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. The following table lists each valid property value and the strength it represents.

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

Password strength 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.

See also

["About session logout" on page 177](#)

["Additional Fortify Software Security Center configuration" on page 73](#)

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 Fortify Software Security Center 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" on the next page](#).

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, Fortify Software Security Center 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 analysis results" on page 282](#)

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 Fortify Software Security Center server.

Note: You can also enable audit issue history in the automatic Fortify Software Security Center configuration. The automatic configuration overrides any changes made to the `app.properties` file. For instructions, see ["Automating Fortify Software Security Center configuration" on page 356](#).

See also

["About audit issue history" on page 145](#)

Chapter 7: Additional installation-related tasks

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

This section contains the following topics:

| | |
|--|-----|
| About bug tracking system integration | 148 |
| Adding and managing parser plugins | 151 |
| About Fortify Software Security Center user administration | 153 |
| Global search functionality in Fortify Software Security Center | 158 |
| Placing Fortify Software Security Center in maintenance mode | 159 |
| Pausing and resuming job execution | 161 |
| About OpenText SAST Application Security Content | 162 |
| Enabling OpenText SAST and OpenText Application Security Tools upgrades from Fortify Audit Workbench | 166 |

About bug tracking system integration

Your team can submit bugs to your bug tracking system during issue auditing. Fortify Software Security Center 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" on page 346](#).

For information about how to set up and use bug tracking systems to manage the security vulnerabilities for your application versions, see ["Using bug tracking systems to help manage security vulnerabilities" on page 215](#).

Adding bug tracker plugins

As an Administrator, you can connect Fortify Software Security Center 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 Fortify Software Security Center-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 | <code><ssc_distribution_dir>/plugins/BugTrackerPluginAlm/com.fortify.BugTrackerPluginAlm-<version>.jar</code> |
| Bug Tracker Plugin for Azure DevOps | <code><ssc_distribution_dir>/plugins/BugTrackerPluginAzure/com.fortify.BugTrackerPluginAzure-<version>.jar</code> |
| Bug Tracker Plugin for Jira | <code><ssc_distribution_dir>/plugins/BugTrackerPluginJira/com.fortify.BugTrackerPluginJira-<version>.jar</code> |

6. Click **START UPLOAD**.

After the upload is completed, the Bug Tracking table lists the new plugin.

7. To enable the bug tracker plugin, click **ENABLE**.

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

See also

["Authoring bug tracker plugins" on page 346](#)

["Assigning a bug tracking system to an application version" on page 219](#)

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" on page 148](#)

["Adding and managing parser plugins" on the next page](#)

["Authoring bug tracker plugins" on page 346](#)

Securing logon credentials for bug tracking systems

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

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

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

If your application requires additional fields, you might need to modify the plugin before you use it. For instructions, see ["Authoring bug tracker plugins" on page 346](#) or contact Customer Support.

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 SAST scan with a build-label, which Fortify Software Security Center uses to map the scan with a source-control revision number. To do this, include the `-build-label <SVN_Revision_Number>` command option when you run OpenText 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.

Adding and managing parser plugins

As an Administrator, you can connect Fortify Software Security Center 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

["Adding bug tracker plugins" on page 149](#)

Preparing to display OpenText Core SCA (Debricked) results

You can view open source security data from OpenText Core SCA on the **AUDIT** or **OPEN SOURCE** pages in Fortify Software Security Center. 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 Fortify Software Security Center to display OpenText Core 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 Fortify Software Security Center 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.
10. In the **UPLOAD PLUGIN BUNDLE** dialog box, click **START UPLOAD**.
The **Parsers** page now lists the OpenText Core SCA parser plugin.

11. After the upload is complete, expand the row for the OpenText Core SCA parser plugin, and then click **ENABLE**.
12. To accept the enable plugin warning message, click **OK**.

See also

["Uploading scan artifacts" on page 261](#)

["Viewing open source data" on page 313](#)

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 Fortify Software Security Center. To do so, you must first download and install the required Sonatype Parser Plugin. After you do, the uploaded Sonatype analysis results are visible.

To prepare Fortify Software Security Center 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 Fortify Software Security Center 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" on page 261](#)

About Fortify Software Security Center user administration

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

Topics covered in this section:

| | |
|---|-----|
| Administrator accounts | 154 |
| User account types | 154 |
| About creating user accounts | 155 |
| Preventing destructive library and template uploads to Fortify Software Security Center | 156 |
| Viewing permissions for Fortify Software Security Center roles | 156 |
| About managing LDAP user roles | 156 |

Administrator accounts

Users who have Administrator accounts have complete access to all Fortify Software Security Center user and application version data and can manage the entire Fortify Software Security Center system. Only users who have Administrator accounts can create, edit, or delete other user accounts. To change a local user account, you must be a local Administrator.

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

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

See also

["Viewing permissions for Fortify Software Security Center roles" on page 156](#)

User account types

In addition to the administrator-level account used to administer user accounts, Fortify Software Security Center supports the following user account types, in descending order of level of authority:

- **Administrator**—An Administrator has access to all application versions and can perform all actions in the system.
- **Security Lead**—A Security Lead has access to all administrative operations except user account creation and editing. The Security Lead can create application versions and edit all aspects of the versions that they created or to which they are assigned.
- **Manager**—A Manager has read-only access to most administrative data. Managers can create and edit all data for the application versions to which they are assigned.
- **Developer**—A Developer has read-only access to some administrative data. Developers can create and edit a subset of data for the application versions to which they are assigned.
- **View-Only**—A View-Only user can view general information and issues for application versions to which 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 Fortify Software Security Center 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 Fortify Software Security Center using 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 Fortify ScanCentral SAST Controller. For instructions on using this role in the Fortify ScanCentral SAST configuration, see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

See also

[User accounts and access](#)

["About creating user accounts" below](#)

["Unlocking local user accounts" on page 192](#)

About creating user accounts

As an Administrator, you can edit, delete, or suspend local user accounts. OpenText recommends that after you sign in to Fortify Software Security Center for the first time, you create at least one non-default Administrator account, and then delete the default Administrator account.

After you create the non-default Administrator account, use the new account to create the user accounts.

Note: As an Administrator, you can delete or suspend all user accounts except for the last remaining administrator-level account. Fortify Software Security Center automatically disables the suspend and delete features for such an account.

For information about how to configure user account timeout and lockout settings, see ["Configuring core settings" on page 83](#). For more information about user account permissions, see ["Account administration" on page 188](#).

See also

["Creating local user accounts" on page 188](#)

["Viewing permissions for Fortify Software Security Center roles" on the next page](#)

["Unlocking local user accounts" on page 192](#)

Preventing destructive library and template uploads to Fortify Software Security Center

Caution! A malicious user might modify a report library or template so that it contains arbitrary and potentially destructive SQL queries and commands. Upload only libraries and templates that are written by trusted users and that have been reviewed for malicious queries and commands.

Only users who have permission to manage report definitions and libraries can upload custom report libraries and templates to Fortify Software Security Center. To prevent templates that execute arbitrary and potentially destructive commands from being uploaded to Fortify Software Security Center, 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 Fortify Software Security Center.

Viewing permissions for Fortify Software Security Center roles

To view detailed information about the actions that users assigned the different Fortify Software Security Center 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" on page 185](#)

["About creating user accounts" on the previous page](#)

["Preconfigured roles" on page 185](#)

["Unlocking local user accounts" on page 192](#)

About managing LDAP user roles

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

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

Group membership in Fortify Software Security Center

For Fortify Software Security Center to recognize a user as a member of a particular group, the user account must refer to a group object in the LDAP directory. When the user signs in, Fortify Software Security Center looks up the user in the LDAP directory. Fortify Software Security Center determines the user's group by the common name (CN) specified in the group membership attribute. If the user belongs to multiple groups, and those groups are mapped to different roles, Fortify Software Security Center assigns the user all roles.

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

Important! Use nested LDAP groups only if absolutely necessary. Enabling nested LDAP groups forces Fortify Software Security Center 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" below](#)

Handling failed LDAP user logins

If you configured nested LDAP groups for your Fortify Software Security Center server, and LDAP authentication fails during an attempted login because of incorrect credentials, then the 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 Fortify Software Security Center and assigned a role? Check with the LDAP administrator to determine whether the user is actually a member of the group to which they are assumed to belong.
- If user does belong to the LDAP group, check to see whether the group is registered with Fortify Software Security Center and assigned a role.
- Special case: If the user belongs to the LDAP group that is registered to Fortify Software Security Center, but was added to the group only within the last few hours, refresh the LDAP cache manually or wait a few hours for it to automatically refresh.

To manually request an LDAP cache refresh:

1. On the 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 Fortify Software Security Center" on the previous page](#)

About mapping Fortify Software Security Center roles to LDAP groups

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

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

Global search functionality in Fortify Software Security Center

Fortify Software Security Center provides global, category-based search functionality that applies search terms across application versions, issues, reports, comments, and users. Newly added documents (artifacts, application versions, users) are 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 attributes" on page 123](#).

To enable global searching on your Fortify Software Security Center server, you must provide Tomcat server with read and write access to the search index directory. 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 Fortify Software Security Center for the first time" on page 68](#)

["Configuring Fortify Software Security Center after an upgrade" on page 172](#)

["Troubleshooting search index issues" on the next page](#)

Troubleshooting search index issues

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

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

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 Fortify Software Security Center and then restart Fortify Software Security Center. For minimum and recommended values for Java heap size, see ["Hardware requirements" on page 32](#).

Placing Fortify Software Security Center in maintenance mode

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

To place Fortify Software Security Center in maintenance mode:

1. 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 Fortify Software Security Center 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 Fortify Software Security Center Setup wizard displays all of the current configuration settings. For information about server configuration, see ["Configuring Fortify Software Security Center for the first time" on page 68](#).

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 Fortify Software Security Center instance appears to be stuck in maintenance mode, try one of the possible solutions described in ["If Fortify Software Security Center is stuck in maintenance mode" below](#).

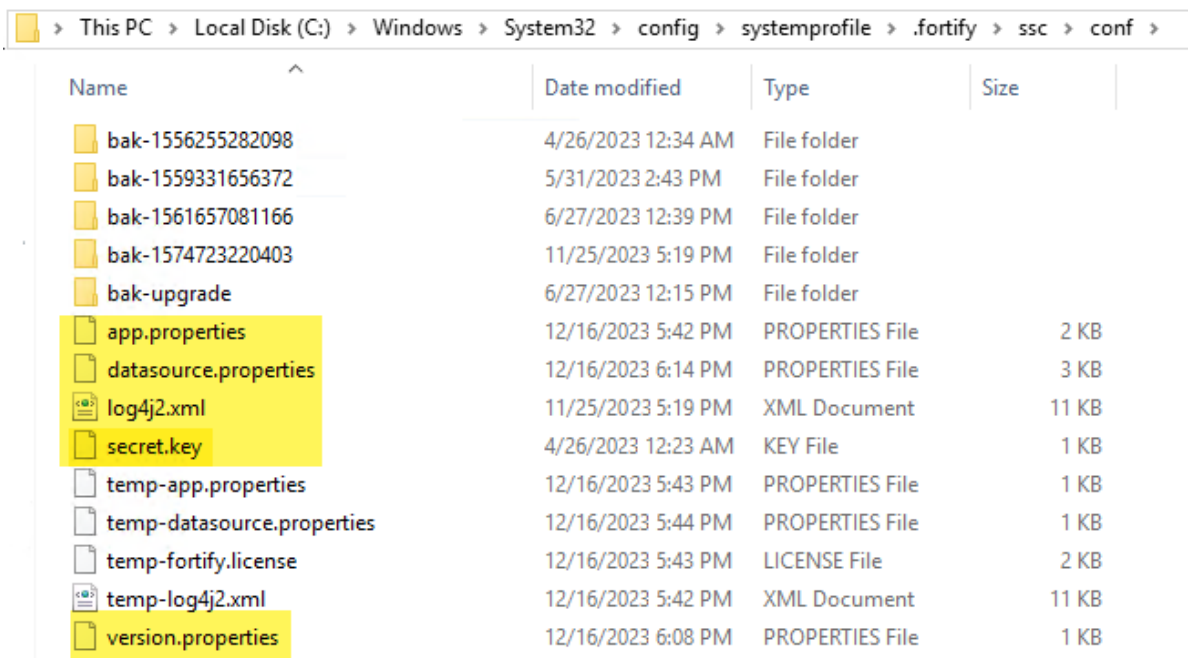
To facilitate server maintenance, you can pause job execution, which allows running jobs to finish but prevents new jobs from executing. For details, see ["Pausing and resuming job execution" on the next page](#).

If Fortify Software Security Center is stuck in maintenance mode

Fortify Software Security Center goes into maintenance mode when it is placed there by an Administrator (see ["Placing Fortify Software Security Center in maintenance mode" on the previous page](#)), or it cannot locate the `version.properties` in the `<fortify.home>/<app_context>/conf/` directory.

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

- Reconfigure Fortify Software Security Center. For instructions, see ["Configuring Fortify Software Security Center for the first time" on page 68](#).
- 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.



| Name | Date modified | Type | Size |
|----------------------------|--------------------|-----------------|-------|
| bak-1556255282098 | 4/26/2023 12:34 AM | File folder | |
| bak-1559331656372 | 5/31/2023 2:43 PM | File folder | |
| bak-1561657081166 | 6/27/2023 12:39 PM | File folder | |
| bak-1574723220403 | 11/25/2023 5:19 PM | File folder | |
| bak-upgrade | 6/27/2023 12:15 PM | File folder | |
| app.properties | 12/16/2023 5:42 PM | PROPERTIES File | 2 KB |
| datasource.properties | 12/16/2023 6:14 PM | PROPERTIES File | 3 KB |
| log4j2.xml | 11/25/2023 5:19 PM | XML Document | 11 KB |
| secret.key | 4/26/2023 12:23 AM | KEY File | 1 KB |
| temp-app.properties | 12/16/2023 5:43 PM | PROPERTIES File | 1 KB |
| temp-datasource.properties | 12/16/2023 5:44 PM | PROPERTIES File | 1 KB |
| temp-fortify.license | 12/16/2023 5:43 PM | LICENSE File | 2 KB |
| temp-log4j2.xml | 12/16/2023 5:42 PM | XML Document | 11 KB |
| version.properties | 12/16/2023 6:08 PM | PROPERTIES File | 1 KB |

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

Pausing and resuming job execution

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

To pause job execution on the server:

1. Sign in to Fortify Software Security Center 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.
 - Fortify Software Security Center displays a banner to notify users that job execution has been paused.
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 Fortify Software Security Center in maintenance mode" on page 159](#)

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 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" below](#)
- ["Importing OpenText SAST Application Security Content" on page 164](#)
- ["Deleting Rulepacks" on page 164](#)
- ["Exporting Rulepacks" on the next page](#)
- ["Seeding the database with report seed bundles in quarterly OpenText SAST Application Security Content releases" on page 174](#)
- 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 an existing mapping" on page 165](#)
- ["Creating a new mapping" on page 165](#)

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.

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 Fortify Software Security Center proxy to update Rulepacks, if the Rulepack update server is behind it. For information about how to set up a consolidated proxy for Fortify Software Security Center, see ["Configuring a proxy for integrations" on page 117](#).

To import the latest Rulepacks:

1. Sign in to Fortify Software Security Center 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**.
Fortify Software Security Center displays information about what the Rulepacks update involves.
5. To continue with the update, click **OK**.
After the update is complete, Fortify Software Security Center displays a list of imported rules.
6. Click **CLOSE**.

See also

["Deleting Rulepacks" on the next page](#)

["Seeding the database with report seed bundles in quarterly OpenText SAST Application Security Content releases" on page 174](#)

["Exporting Rulepacks" below](#)

["Importing OpenText SAST Application Security Content" on the next page](#)

Exporting Rulepacks

You can, if necessary, move Rulepacks from one Fortify Software Security Center instance to another, or between Fortify Software Security Center and Fortify Audit Workbench.

Export Rulepacks with the same file names used to import them, including the file extension (.bin or .xml).

To export a Rulepack:

1. 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" on the next page](#)

["Deleting Rulepacks" on the next page](#)

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 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, Fortify Software Security Center displays a processing warning.

See also

["Exporting Rulepacks" on the previous page](#)

["Deleting Rulepacks" below](#)

Deleting Rulepacks

You can remove old Rulepacks from Fortify Software Security Center.

To delete Rulepacks:

1. 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" on the previous page](#)

["Importing OpenText SAST Application Security Content" above](#)

["Updating Rulepacks from the Rulepack update server" on page 162](#)

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: Identifier Contains Dollar Symbol ($)
  </InternalCategory>
  <ExternalCategory>App100 CAT 1</ExternalCategory>
</Mapping>
</ExternalListExtension>
```

Important! After you extend your mapping file, you must upload it to Fortify Software Security Center. For instructions, see ["Importing OpenText SAST Application Security Content" on the previous page](#).

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

See also

["Creating a new mapping" below](#)

["About OpenText SAST Application Security Content" on page 162](#)

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 Fortify Software Security Center. For instructions, see ["Importing OpenText SAST Application Security Content" on page 164](#).

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

See also

["Extending an existing mapping" on the previous page](#)

["About OpenText SAST Application Security Content" on page 162](#)

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 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 Fortify Software Security Center host machine.

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

1. On the Fortify Software Security Center 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:
 - a. To enable OpenText SAST updates, create an update XML file (such as `update-sast.xml`) using the following example:

```
<installerInformation>  
  <versionId>2520</versionId> <!--The version of the installer file with periods  
removed-->  
  <version>25.2.0</version> <!--The version of the installer file-->  
  <platformFileList>  
    <platformFile>  
      <filename>OpenText_SAST_windows-x64_25.2.0.exe</filename>  
      <platform>windows-x64</platform>  
    </platformFile>  
    <platformFile>  
      <filename>OpenText_SAST_linux-x64_25.2.0.run</filename>  
      <platform>linux-x64</platform>  
    </platformFile>  
    <platformFile>  
      <filename>OpenText_SAST_osx-x64_25.2.0.app.zip</filename>  
      <platform>osx</platform>  
    </platformFile>  
  </platformFileList>  
  <downloadLocationList>  
    <downloadLocation>  
      <url>http://localhost:8080/update-site/installers/</url>  
    </downloadLocation>  
  </downloadLocationList>  
</installerInformation>
```

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

```
<installerInformation>  
  <versionId>2520</versionId> <!--The version of the installer file with periods  
removed-->  
  <version>25.2.0</version> <!--The version of the installer file-->
```

```
<platformFileList>
  <platformFile>
    <filename>OpenText_Application_Security_Tools_windows-x64_
25.2.0.exe</filename>
    <platform>windows-x64</platform>
  </platformFile>
  <platformFile>
    <filename>OpenText_Application_Security_Tools_linux-x64_
25.2.0.run</filename>
    <platform>linux-x64</platform>
  </platformFile>
  <platformFile>
    <filename>OpenText_Application_Security_Tools_osx-x64_
25.2.0.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 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*.

Chapter 8: Upgrading Fortify Software Security Center

To perform a direct upgrade to the latest Fortify Software Security Center version, you must have one of the last three versions already installed. The following are the valid upgrade paths for upgrading to version 25.2.0:

- 24.4.x to 25.2.x (direct)
- 24.2.x to 25.2.x (direct)
- 23.2.x to 25.2.x (direct)
- 23.1.x to 23.2.x to 25.2.x

If you cannot directly upgrade your current Fortify Software Security Center version to the latest version, see the version-specific documentation for instructions on how to upgrade.

This section contains the following topics:

| | |
|--|-----|
| Upgrade prerequisites | 169 |
| Preparing to upgrade the database | 170 |
| Upgrade tasks | 171 |
| Updating and deploying the WAR file | 172 |
| Configuring Fortify Software Security Center after an upgrade | 172 |
| Updating expired licenses | 174 |
| Seeding the database with report seed bundles in quarterly OpenText SAST Application Security Content releases | 174 |

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 Fortify ScanCentral SAST-related functionality in Fortify Software Security Center requires updated Controller and sensors. If you do not need sensor metrics, you can use existing sensors. You can use existing 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 Fortify Software Security Center 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" below](#)

Preparing to upgrade the database

The Fortify Software Security Center 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" below](#).

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" on page 54](#)

Preparing to run the database upgrade script

The Fortify Software Security Center 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 Fortify Software Security Center database using your database client tool.
- Acquire the database account information that was used to create the existing Fortify Software Security Center database. See ["Database user account permissions" on page 52](#).

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

Upgrade tasks

Upgrade to a new version of Fortify Software Security Center 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" on the next page). Note: <tomcat> represents the root directory of the Tomcat instance. |
| 3 | Start Tomcat server. |
| 4 | Open a browser and enter your Fortify Software Security Center web address to start the Setup wizard. |
| 5 | Use the Setup wizard to generate the migration SQL script (see "Configuring Fortify Software Security Center after an upgrade" on the next page). |
| 6 | Run the migration script on your database (see "Preparing to run the database upgrade script" on the previous page). Databases that contain over 1 TB of data might take five or more hours to migrate. Important! (SQL Server databases only) After you migrate Fortify Software Security Center 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 Fortify Software Security Center database. |
| 7 | Use the Setup wizard to reseed the database. |

| Task | Description |
|------|--|
| 8 | Restart Tomcat server. |
| 9 | Bug tracker plugins are not included in the <code>ssc.war</code> file. After you upgrade and start Fortify Software Security Center, remove old bug tracker plugins, and then install new plugins from the current installation package. For more information, see "About bug tracking system integration" on page 148 . |

Updating and deploying the WAR file

To update the Fortify Software Security Center WAR file:

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

After you deploy the new WAR file, complete the configuration tasks on the Setup wizard steps and in the **Administration** view. For information and instructions, see ["Configuring Fortify Software Security Center after an upgrade" below](#) and ["Additional Fortify Software Security Center configuration" on page 73](#).

Configuring Fortify Software Security Center after an upgrade

After you upgrade Fortify Software Security Center and enter your Fortify Software Security Center 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 Fortify Software Security Center, after an upgrade, or after the server is placed in maintenance mode (see ["Placing Fortify Software Security Center in maintenance mode" on page 159](#)).

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 Fortify Software Security Center 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 Fortify Software Security Center for the first time" on page 68.](#)

7. Click **NEXT** until you reach the **DATABASE SETUP** page.
8. On the **DATABASE SETUP** page, do the following:
 - a. In the **DATABASE TYPE** box, select the type that matches the Fortify Software Security Center database type.
 - b. In the **DATABASE USERNAME** box, type the username for your Fortify Software Security Center database.

For more information, see ["Database user account permissions" on page 52.](#)

- c. In the **DATABASE PASSWORD** box, type the password for your Fortify Software Security Center database.
 - d. In the **JDBC URL** box, type the URL for the Fortify Software Security Center database.

Caution! The database name (including letter case) in the JDBC URL must exactly match your Fortify Software Security Center database name.

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>`.

- e. 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.

- f. After the Setup wizard indicates that the connection was successful, read the warning and instructions, and then click **DOWNLOAD SCRIPT**.
 - g. Save and run the `ssc-migration.sql` script.
For instructions, see ["About the Fortify Software Security Center database tables and schema" on page 58.](#)

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:
 - a. Click **BROWSE** to locate and select your process seed bundle ZIP file, and then click **SEED DATABASE**.
 - b. Click **BROWSE** to locate and select your report seed bundle ZIP file, and then click **SEED DATABASE**.
 - c. (Optional) Click **BROWSE** to locate and select your PCI SSF seed bundle ZIP file, and then click **SEED DATABASE**.

- d. (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 Fortify Software Security Center in maintenance mode, and then make any necessary changes. For instructions on how to place Fortify Software Security Center in maintenance mode, see ["Placing Fortify Software Security Center in maintenance mode" on page 159](#).

Updating expired licenses

For information about how to obtain a Fortify license file, see ["Downloading and unpacking Fortify Software Security Center files" on page 50](#).

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.

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 Fortify Software Security Center database" on page 58](#).

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:
 - a. Log in to the [Application Security Customer Portal](#).
 - b. In the navigation pane, select **PREMIUM CONTENT**.
 - c. Click the **FORTIFY EXCHANGE** link.
 - d. Select and download the latest report seed bundle.
2. Extract the contents of the seed bundle ZIP file.
3. Sign in to Fortify Software Security Center 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 Fortify Software Security Center database" on page 58](#)

["About OpenText SAST Application Security Content" on page 162](#)

["Updating Rulepacks from the Rulepack update server" on page 162](#)

Chapter 9: Using Fortify Software Security Center

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

Fortify Software Security Center correlates and tracks the 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 Fortify Software Security Center | 176 |
| Requesting access to Fortify Software Security Center | 178 |
| Changing your password | 178 |
| Setting preferences system-wide and across application versions | 178 |
| Viewing keyboard hotkeys | 179 |
| Accessing the API documentation | 179 |
| About the Fortify Software Security Center Dashboard | 180 |

Signing in to Fortify Software Security Center

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

To sign in to Fortify Software Security Center for the first time:

1. In a web browser, type the web address for your Fortify Software Security Center 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 Fortify Software Security Center prompts you to change your password, do so.

About session logout

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

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: Fortify Software Security Center 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" on page 141](#).

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

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

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

Inactive session timeout

If you have been inactive and your session is about to time out, Fortify Software Security Center 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, Fortify Software Security Center logs you out of the session and takes you to the logout screen.

- If you are logged on to Fortify Software Security Center through an SSO provider for which single logout is supported, you see a dialog box that lets you log out of your local user account, perform an SSO logout, or stay logged in.

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

If you click **SSO LOGOUT**, Fortify Software Security Center 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" on page 83](#).

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

Requesting access to Fortify Software Security Center

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 Fortify Software Security Center:

1. In a web browser, type the web address for your Fortify Software Security Center instance.
2. Click **Can't access or need an account?**
This button is available only if your Fortify Software Security Center Administrator has enabled email notification (see ["Configuring email alert notification settings" on page 90](#)).
3. Provide the required information and click **SEND**.

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 Fortify Software Security Center.
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**.

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:

- a. Select the check boxes for the features you want to enable and clear the check boxes for the features you want to turn off.
- b. To apply the YYYY/MMDD date format instead of the default MM/DD/YYYY format, select it from the **Date format** list.
- c. To apply the 24 Hour time format instead of the default 12 hour AM/PM format, select it from the **Time format** list.
- d. 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**.

- a. To include suppressed issues in the issues list on the **AUDIT** page, select the **Show suppressed issues** check box.
- b. To include removed issues on the **AUDIT** page, select the **Show removed issues** check box.
- c. To include hidden issues on the **AUDIT** page, select the **Show hidden issues** check box.
- d. To display short file names in the issues list on the **AUDIT** page, select the **Use short filenames** check box.

4. Click **SAVE**.

Viewing keyboard hotkeys

To view the keyboard hotkeys used to navigate the Fortify Software Security Center user interface:

1. Sign in to Fortify Software Security Center.
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" on the previous page](#)

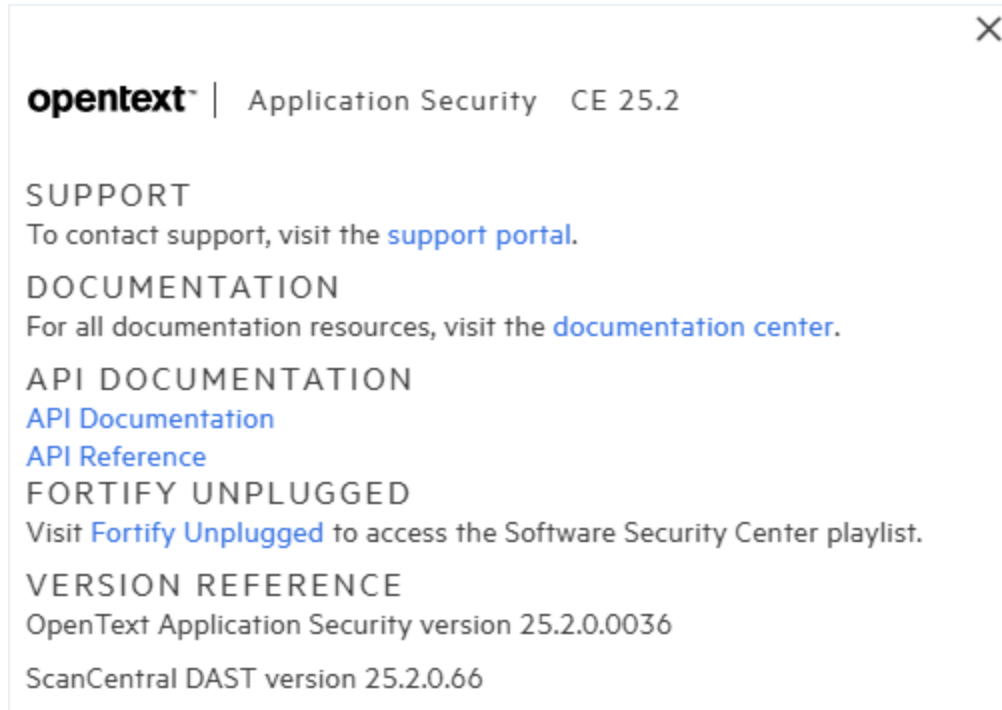
Accessing the API documentation

Important! Usage of Fortify Software Security Center API calls from external applications can have a negative impact on your Fortify Software Security Center 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 Fortify Software Security Center. Professional Services can assist you

with this.

To access the Fortify Software Security Center API documentation:

1. On the header, click the **Help** button .



2. Click the **API Documentation** link.

The Fortify Software Security Center API documentation webpage opens in the browser.

Tip: It is useful to leverage a proxy such as the Chrome DevTools to intercept Fortify Software Security Center traffic and determine the appropriate endpoint calls to make to perform user interface actions.

About the Fortify Software Security Center Dashboard

After you sign in to Fortify Software Security Center, 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:

| | |
|--|-----|
| Issue Stats | 181 |
| Viewing high-level summary metrics for your application versions | 182 |
| Viewing high-level summary metrics (graphical representation) for an application version | 183 |

| | |
|---|-----|
| Exporting the Dashboard summary table | 183 |
|---|-----|

Issue Stats

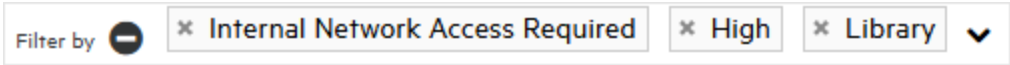
When you first sign in to Fortify Software Security Center, the first thing you see is the **ISSUE STATS** page in the **Dashboard** view. This page shows summary information about issues for the application versions that you can access, including the average number of days that it is taking to review 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**. A green bar indicates that issues are being managed quickly, a red bar indicates that issue management is too slow, and an orange bar indicates that issue management is somewhere between these two extremes.

Note: 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" on page 75](#).

If you click an application version listed in the table, Fortify Software Security Center takes you directly to the **AUDIT** page for that application version. No filters are applied to the data.

The **Dashboard** 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 | <p>Select an attribute from the Group by list. The default grouping attribute is the application version.</p> <p>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.</p> <p>Note: You can achieve finer control over the data displayed if your Group by list includes custom attributes (of the single-select type). For instructions on how to create custom attributes, see "Creating custom attributes" on page 198.</p> |
| Aggregate by an application attribute | <p>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.</p> <p>Note: You can achieve finer control over the data displayed if your Aggregate by list includes custom attributes (of the single-select type). For instructions on how to create custom attributes, see "Creating custom attributes" on page 198.</p> |

| Display setting | Description |
|--|--|
| Filter by one or more application attributes | <p>Select an attribute from the Filter by list. You can filter by multiple attributes, but you must select them one at a time.</p>  <p>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.</p> |

To clear your attribute selection from a list, click the **Clear all** button .

You can export Fortify Software Security Center data displayed on the **ISSUE STATS** and **AUDIT** pages to comma-separated values (CSV) files. For details, see ["Exporting selected data for an application version" on page 214](#).

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 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.

See also

["Viewing high-level summary metrics \(graphical representation\) for an application version" on the next page](#)

["Auditing analysis results" on page 282](#)

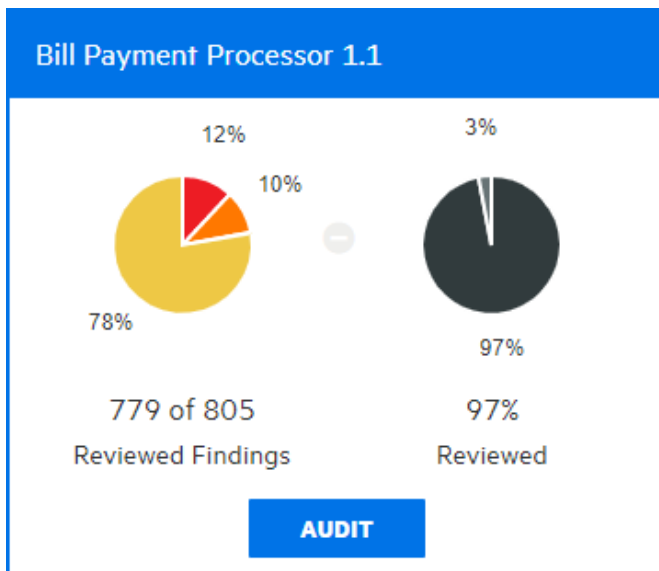
["Viewing high-level summary metrics for an application version" on page 271](#)

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**.
Fortify Software Security Center 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 high-level summary metrics for your application versions" on the previous page](#)

["Auditing analysis results" on page 282](#)

["Viewing high-level summary metrics for an application version" on page 271](#)


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 attributes" on page 123](#).

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:
 - a. On the header, select **Reports**.
 - b. Click **DATA EXPORTS**.
 - c. 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" on page 214](#)

Chapter 10: Managing user accounts

As described in the secure deployment guidelines, the primary system Administrator of a new Fortify Software Security Center installation creates a non-default administrator-level account, and then deletes the default Administrator account. Use the non-default Fortify Software Security Center administrator account to create additional Fortify Software Security Center user accounts.

This section contains information about Fortify Software Security Center roles, user account administration, how to register LDAP entities with Fortify Software Security Center, and how to configure an integration with Microsoft Entra ID.

This section contains the following topics:

| | |
|--|-----|
| About tracking teams | 185 |
| About roles | 185 |
| Account administration | 188 |

About tracking teams

As an Administrator or Security Lead, you need access to information that enables you to track and monitor your team's progress and ensure that good application security practices are in place and followed. Fortify Software Security Center provides a central point for guiding the adoption of good security practices. By understanding how information is tracked and reported, you can accurately measure development team progress based on application security standards.

About roles

Roles determine the actions a user can perform in Fortify Software Security Center.

For more fine-grained control over user access to Fortify Software Security Center functionality, you can create custom roles and assign them permissions from the Fortify Software Security Center interface. For instructions on how to create a role, see ["Creating custom roles" on page 187](#).

Preconfigured roles

The following table lists the preconfigured roles you can assign to users in Fortify Software Security Center. 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 permissions for Fortify Software Security Center roles" on page 156](#).

| 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: <ul style="list-style-type: none">• 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 Fortify Software Security Center and retrieve issue audit information. This role is intended for use only by a WebInspect Enterprise instance. |
| ScanCentral SAST Controller | Can upload scans from Fortify ScanCentral SAST to Fortify Software Security Center 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 <i>OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide</i> . |

See also

["About roles" on the previous page](#)

["Creating custom roles" on the next page](#)

Creating custom roles


You can define roles of your own and assign them permissions.

To define and configure permissions for a new role:

1. 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.

Fortify Software Security Center checks permissions to guard against states that are known to be incompatible. If the role and permissions you selected do not conflict, then you are returned to the **Roles** page, which displays detailed information about the new role.

Deleting custom roles

If a custom role listed on the **Roles** page is not assigned to any user account, you can delete that role.

To delete a role:

1. Sign in to Fortify Software Security Center 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" on the previous page](#)

Account administration

Only users who have Administrator accounts can create new user accounts and edit information for existing accounts. Use Administrator accounts to manage the Fortify Software Security Center system. OpenText recommends that you create only the administrator-level accounts necessary to create and edit local or LDAP Fortify Software Security Center user accounts. The Security Lead and lesser accounts can perform all other application-related activities.

Fortify Software Security Center permits the explicit addition of administrator-level accounts to application versions. This enables administrators to be assigned issues from the **AUDIT** page.

Topics covered in this section:

| | |
|---|-----|
| Creating local user accounts | 188 |
| Editing local user accounts | 190 |
| Unlocking local user accounts | 192 |
| Viewing externally managed users and groups | 193 |

Creating local user accounts

As an Administrator, you can add new local user accounts to Fortify Software Security Center.

Important! You cannot create externally managed users from Fortify Software Security Center. These can only be provisioned using the SCIM API.

To create a Fortify Software Security Center user account:

1. 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 Fortify Software Security Center. |
| Password never expires | Select this check box to allow the user to use the originally assigned password until he or she wants to change it. To require the user to change their password every thirty days, leave this check box cleared. |
| Suspended | Select this check box to suspend access to Fortify Software Security Center for this user account. |
| Roles | (Optional, but strongly recommended) Select the check boxes for all roles to assign to the user account. |

| Field | Description |
|--------|---|
| | Caution! Although this is optional, a user who has no assigned role cannot access Fortify Software Security Center unless that user belongs to a local group that does have an assigned role. |
| Access | <p>To specify the applications that the new user can access:</p> <p>Note: If you have assigned the user account the role of Administrator or Webinspect Enterprise System, the user has universal access to all Fortify Software Security Center applications.</p> <ol style="list-style-type: none">Click ADD.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.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.To add another application version or versions, repeat steps b and c.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" below](#)

["Unlocking local user accounts" on page 192](#)

Editing local user accounts

The following procedure describes how to edit the account for local user accounts created from Fortify Software Security Center, as well as user accounts provisioned using the SCIM API.

To edit a local user account:

1. On the 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**.

| User type SSO ▼ | | Filter by Active/Suspended ▼ | | DELETE | EXPORT | Search by user name | FIND | + ADD |
|--------------------------------------|-----------|-------------------------------------|-------------------------|--------|--------|---------------------|------|-------|
| Username | Last Name | First Name | Email | Roles | | Suspended | | |
| <input type="checkbox"/> scim-user-1 | Mary | Smith | mary.smith@fortify.com | | | | | |
| <input type="checkbox"/> scim-user-2 | James | Major | james.major@fortify.com | | | | | |
| <input type="checkbox"/> scim-user-3 | | | | | | | | |

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**.

| | | | | | |
|--|-------|--|-------|-------------------|-----------|
| <input type="checkbox"/> | susan | Richards | Susan | susan@fortify.com | Developer |
| First Name | | Email | | | |
| <input type="text" value="Susan"/> | | <input type="text" value="susan@fortify.com"/> | | | |
| Last Name | | | | | |
| <input type="text" value="Richards"/> | | <input type="checkbox"/> User must change password at next login | | | |
| | | <input checked="" type="checkbox"/> Password never expires | | | |
| | | <input type="checkbox"/> Suspended | | | |
| Roles | | Access | | ADD | DELETE |
| <input type="checkbox"/> Administrator | | <input type="checkbox"/> Bill Payment Processor - 1.1 | | | |
| <input type="checkbox"/> Application Security Tester | | <input type="checkbox"/> Logistics - 1.3 | | | |
| <input checked="" type="checkbox"/> Developer | | <input type="checkbox"/> Logistics - 2.5 | | | |
| <input type="checkbox"/> Manager | | <input type="checkbox"/> RWI - 1.0 | | | |
| <input type="checkbox"/> Security Lead | | <input type="checkbox"/> Web application - 1.0 | | | |
| <input type="checkbox"/> View-Only | | | | | |
| CHANGE PASSWORD | | CANCEL | | SAVE | |

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 Fortify Software Security Center, 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" below](#)

["Creating local user accounts" on page 188](#)

Unlocking local user accounts

After a local user tries unsuccessfully to sign in to three times in a row, Fortify Software Security Center 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 Fortify Software Security Center Administrator. As an Administrator, you can unlock the account for the user.

Note: The locking and unlocking of user accounts does not apply to users provisioned through the SCIM API.

After a user notifies you that they are locked out of their account, unlock the account as follows:

1. On the 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" on page 188](#)

["Editing local user accounts" on page 190](#)

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**.

Fortify Software Security Center 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 Fortify Software Security Center 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 Fortify Software Security Center unless the group has been assigned one or more roles, or the user is assigned a role individually from the **Local Users** page.

Important! From Fortify Software Security Center, the only changes you can make to externally-managed user and group accounts are role and application version assignments. 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" on page 112](#)

["Enabling SCIM to provision externally managed users and groups" on page 117](#)

["Using SCIM 2.0 and SAML 2.0 to configure a connection to Microsoft Entra ID for user provisioning" on page 115](#)

["Configuring SAML 2.0-compliant single sign-on" on page 137](#)

Chapter 11: Applications and application versions

To obtain consistent measurement results, you define an application for a single codebase. Fortify Software Security Center 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 Fortify Software Security Center application. Fortify Software Security Center automatically creates the first version of that application.
- An application version is an instance of the application or 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 SAST (Fortify Static Code Analyzer), OpenText 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 | 195 |
| About creating application versions | 196 |
| Viewing application versions | 211 |
| Searching applications and application versions from the Applications view | 212 |
| Recalculating application metrics | 214 |
| Editing application version details | 214 |

| | |
|--|---------------------|
| Exporting selected data for an application version | 214 |
| Using bug tracking systems to help manage security vulnerabilities | 215 |
| Changing the template associated with an application version | 223 |
| Setting analysis result processing rules for application versions | 223 |
| Configuring Fortify Audit Assistant options for an application version | 229 |
| Enabling auto-apply and auto-predict for an application version | 230 |
| About custom tags | 231 |
| About deleting application versions | 243 |

About tracking development teams

As an Administrator or Security Lead, you need access to information that enables you to track and monitor your team's progress and ensure that good application security practices are in place and followed. Fortify Software Security Center provides a central point for guiding the adoption of good security practices. By understanding how information is tracked and reported through applications and applications versions, you can accurately assess development team progress based on application security standards.

About the application creation process

After you sign in to Fortify Software Security Center 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" on page 197](#)

["Template selection" on page 203](#)

["Creating the first version of a new application" on page 204](#)

["Adding a new version to an application" on page 207](#)

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.

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" on page 244](#).

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).

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.

About annotating application versions for reporting

Fortify Software Security Center provides a set of application attributes that you can apply to individual application versions. You can use these attributes to group application versions for reporting, or to associate application versions with external systems.

Administrators can customize the base set of application attributes. Sample customizations can help organizations track onboarding progress by application ID, line of business, business unit, or regulatory compliance obligations.

About creating application versions

You can create a new Fortify Software Security Center 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" on the previous page](#)

["Creating the first version of a new application" on page 204](#)

["Adding a new version to an application" on page 207](#)

Application version attributes

Application versions have business attributes, technical attributes, and organization attributes. These attributes are metadata that Fortify Software Security Center uses to perform cross-application comparisons and reporting.

When you create a new application version, the **CREATE NEW APPLICATION VERSION** wizard guides you through the selection of required and optional technical, organization, business, and OpenText 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 Fortify Software Security Center provides, Administrators and Security Leads can create custom attributes to assign to application versions. Custom attributes are extremely useful when you need to focus on a highly specific subset of data. For instructions on how to create custom attributes, see ["Creating custom attributes" on the next page](#).

The following tables list the default set of attributes for Fortify Software Security Center applications. Note that this list does not include custom attributes that 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 ScanCentral DAST attribute | Description |
|-------------------------------------|---|
| Base URL | URL prefix that all pages in your application start with, which is useful in establishing relative pathways |

Creating custom attributes

Fortify Software Security Center comes with technical, organization, and business attributes that enable administrators and security leads to categorize applications and application versions. As an Administrator or a Security Lead, you can create your own custom attributes that can be set for application versions.

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 | <p>Type a descriptive name for the attribute.</p> <p>Important! If you delete an attribute that Fortify Software Security Center uses by default, and you then create a new attribute with the same name, database migration might fail.</p> |
| Description | <p>Type a brief description.</p> <p>The description is displayed under the attribute field in the CREATE NEW APPLICATION VERSION wizard.</p> |
| Category | <p>Select an attribute type.</p> <p>Depending on the category you select, the attribute is displayed on corresponding attribute tab of the CREATE NEW APPLICATION VERSION wizard.</p> |
| Type | <p>Select one of the following control types:</p> <ul style="list-style-type: none">• 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. <p>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.</p> <ul style="list-style-type: none">• 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. <p>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.</p> <ul style="list-style-type: none">• To create a check box for the attribute, select Boolean.• To create a field that accepts an integer value, select Integer. |

| Field | Description |
|----------|---|
| | <ul style="list-style-type: none">To create a calendar selection control for the attribute, select Date. <div>Note: This type is not available for a dynamic scan request attribute.</div> |
| 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. <div>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.</div> |

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" on page 202](#).

Note: By default, a custom attribute you create through the user interface is deletable. You can use the Fortify Software Security Center API to define a non-deletable attribute. For information about how to access the API, see ["Accessing the API documentation" on page 179](#).

See also

["Deleting attributes and attribute values" below](#)

["Application version attributes" on page 197](#)

Deleting attributes and attribute values

If an attribute or attribute value is no longer of use, you can often delete it from the Fortify Software Security Center database, 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 Fortify Software Security Center database:

- On the header, select **Administration**.
- 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**.
4. To confirm that you want to permanently remove the attribute from the system, click **OK**.

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.

☐ Application Type List of Values - Single Selection Technical

Name *

Application Type

Category *

Technical

Description

Codebase type

Type *

List of Values - Single Selection

☐ Required

☐ Hidden

| Value | Description | In Use | Hidden |
|-----------------------|--|--------|--------|
| Library | Application Programming Interface | | |
| Application Component | A module which performs a business function that is not a self contained application | | |
| Application | Codebase that defines the interface. May depend on many components and libraries | | |

DELETE

EDIT

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


Fortify Software Security Center 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" on page 198](#)

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.
Fortify Software Security Center 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" on page 198](#)

["Editing application version details" on page 214](#)

About issue templates

Applications are defined by *issue templates*, which determine how Fortify Software Security Center configures and prioritizes the issues uncovered in your application source code.

An issue template contains the following settings:

- Folder filters—Controls how issues are sorted into the folders
- Visibility filters—Controls which issues are shown and hidden
- Folder properties—Name, color, and which filter set it is active in
- Custom tags—Specifies which audit fields are displayed and the values for each

Fortify Software Security Center comes with 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 Fortify Software Security Center issue template into Fortify Audit Workbench, modify it, save it with a new name, and then import it into Fortify Software Security Center. You can also create a new issue template from scratch in Fortify Audit Workbench.

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 Fortify Software Security Center 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 Fortify Software Security Center and Fortify Audit Workbench. When there are multiple matched external categories, Fortify Software Security Center 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 Fortify Software Security Center, 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*.

Adding issue templates to the system

To add an issue template from Fortify Audit Workbench to Fortify Software Security Center:

1. Sign in to Fortify Software Security Center as an Administrator.
2. On the header, select **Administration**.
3. On the navigation pane, expand **Templates**, and then select **Issue Templates**.
Fortify Software Security Center 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**.

Template selection

Fortify Software Security Center 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.

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: <ol style="list-style-type: none">a. Click BROWSE.b. Locate and select the application that has the settings you want to use for the new application. |

| Field | Description |
|-------|--|
| | <p>You can type a string into the search box, and then click FIND to refine the list of applications.</p> <p>The VERSIONS pane lists the active versions of the selected application. To display inactive versions, select the Show inactive check box.</p> <p>c. From the VERSIONS list, select the check box for the version you want, and then click DONE.</p> <p>By default, Fortify Software Security Center includes all settings of the selected application version.</p> <p>d. To exclude one or more settings, clear the corresponding check boxes for the settings.</p> <p>e. To copy over all of the issues and audits associated with the selected application version, select the Application state check box.</p> <p>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" on page 214.</p> |

- To proceed to the **ATTRIBUTES** settings, click **NEXT**.
- 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. |

| Field | Description |
|-----------------------|---|
| 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 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" on page 130](#).

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 Fortify Software Security Center database:
 - i. Select **LOCAL**.
 - ii. 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:
 - i. Click **LDAP**, and then, from the **View By** list, select the attribute to use to display LDAP entities.
 - ii. 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" on page 261](#)

["Adding a new version to an application" below](#)

Adding a new version to an application

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 | <p>Type a name for the version.</p> <p>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.</p> |
| Version description | <p>(Optional) Type a description of this version of the application.</p> |
| Use existing application version | <p>To use the settings of an existing application version, select this check box and do the following:</p> <ol style="list-style-type: none">Click BROWSE.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.From the VERSIONS list, select the check box for the version you want, and then click DONE. By default, Fortify Software Security Center includes all settings of the selected application version.To exclude one or more settings, clear the corresponding check boxes for the settings.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" on page 214. |

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 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 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" on page 130](#).

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 Fortify Software Security Center database:
 - i. Select **LOCAL**.
 - ii. 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:
 - i. Click **LDAP**, and then, from the **View By** list, select the attribute to use to display LDAP entities.
 - ii. 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

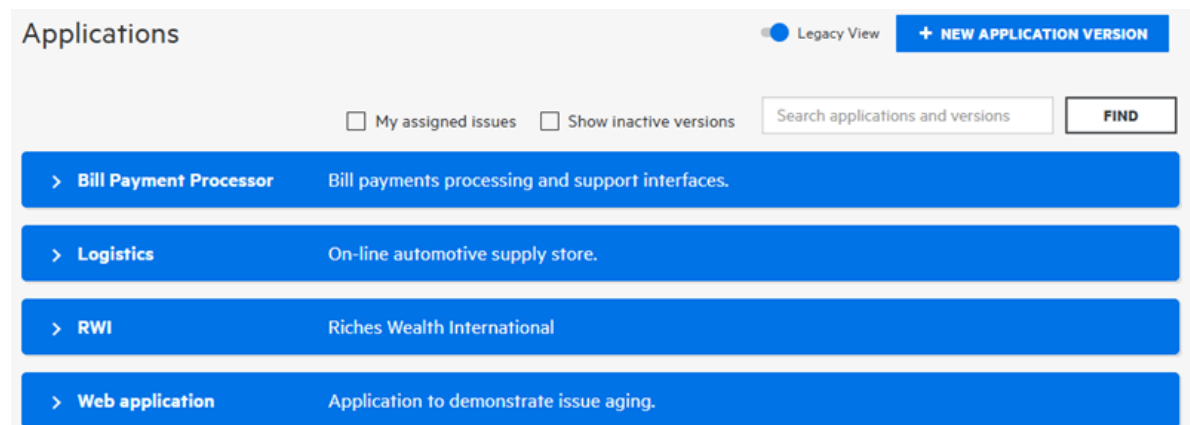
["Creating the first version of a new application" on page 204](#)

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.

| Name | Versions | Description |
|------------------------|----------|--|
| Bill Payment Processor | 1 | Bill payments processing and support interfaces. |
| Logistics | 2 | On-line automotive supply store. |
| RWI | 1 | Riches Wealth International |
| Web application | 1 | Application to demonstrate issue aging. |

Page Size: 20 1 to 4 of 4 Page 1 of 1

Filters Clear all

Search applications

General

☐ Include inactive versions

☐ My assigned issues

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), the number of issues in each priority group, and the date and time of the most recent scan.

| Name | Description | Application | Rating | Critical | High | Medium | Low | Most Recent |
|------|------------------|-------------|--------|----------|------|--------|-----|-------------|
| 1.3 | E-commerce web | Logistics | Fail | 31 | 31 | 1 | 158 | 06/13/2009 |
| 2.5 | Major updates to | Logistics | Fail | 8 | 24 | 1 | 138 | 04/02/2025 |

Page Size: 20 1 to 2 of 2 Page 1 of 1

Filters Clear all

Search versions

General

☐ Include inactive versions

☐ My assigned issues

See also

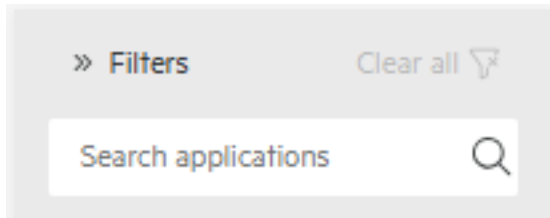
["Searching applications and application versions from the Applications view" below](#)

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.

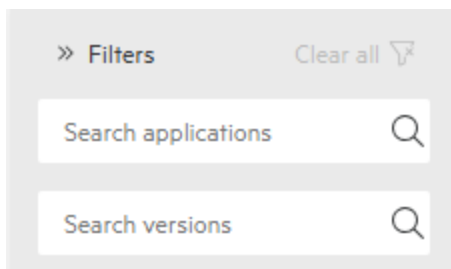


3. To return to the complete **Your Applications** page, clear the text in the search box.

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.

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 " on page 281](#)

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.

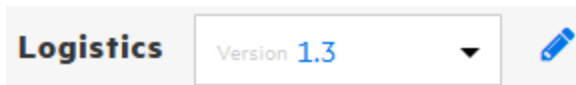
See also

["Downloading analysis results" on page 264](#)

Editing application version details

To edit the details of an application version:

- On the header, select **Applications**.
- Select the application version to edit.
- On the **AUDIT** page, click the **Edit** button .



- 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" on page 207](#).
- Click **SAVE**.

See also

["Changing the template associated with an application version" on page 223](#)

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 attributes" on page 123](#).

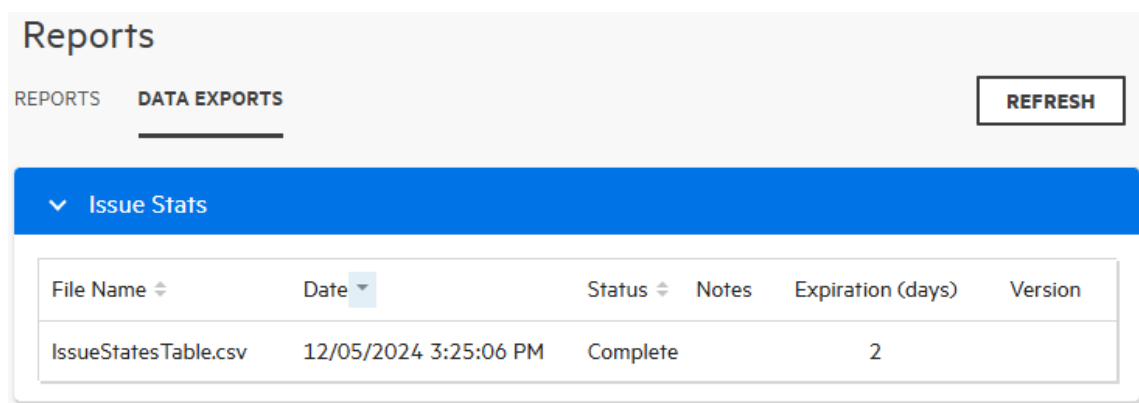
To export data for an application version:

- On the header, select **Dashboard** or **Applications**.
- 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:
 - a. On the header, select **Reports**.
 - b. Click **DATA EXPORTS**.



| Reports | | | | | |
|----------------------|-----------------------|--------------|-------|-------------------|---------|
| REPORTS | | DATA EXPORTS | | REFRESH | |
| Issue Stats | | | | | |
| File Name | Date | Status | Notes | Expiration (days) | Version |
| IssueStatesTable.csv | 12/05/2024 3:25:06 PM | Complete | | 2 | |

- c. 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" on page 183](#)

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 Fortify Software Security Center, you can map to any of several bug tracking systems, so that your development team can file bugs into the bug tracking system you already use.

When a developer files a bug, Fortify Software Security Center populates bug tickets with the following basic vulnerability information:

- Details that describe the type of issue uncovered
- Remediation guidance, with instructions on the action to take
- A link back to Fortify Software Security Center for complete issue details

Bug tracker configuration

To enable a team to access and use a bug tracking system from Fortify Software Security Center, a security lead or development manager must configure Fortify Software Security Center to connect to a bug tracker instance. Either the Developer or Security Lead can then submit bugs to address important security issues.

If you are a Security Lead or Manager, you can enable team access to your bug tracking system as follows:

1. Edit the application version details.
2. Configure the bug tracker.

See also

["Velocity templates for bug filing" below](#)

["Adding bug tracker plugins" on page 149](#)

["Authoring bug tracker plugins" on page 346](#)

Velocity templates for bug filing

Text-based fields for filing bugs in Fortify Software Security Center can be associated with Apache Velocity templates that reference issue data. When you submit a bug for one or more issues, the content for the mapped fields is generated using the corresponding template and data from the issues.

Fortify Software Security Center provides pre-defined templates for the summary and description fields of the supported bug tracker plugins that ship with Fortify Software Security Center. You can edit these pre-defined templates or add templates that map other text-based fields that the plugin provides.

This section contains the following topics:

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

["Customizing Velocity templates for bug tracker plugins" on page 218](#)

["Deleting Velocity templates" on page 219](#)

Adding Velocity Templates to Bug Tracker Plugins

Fortify Software Security Center provides pre-defined templates for the summary and description fields of the supported bug tracker plugins that ship with Fortify Software Security Center. You can edit these templates or add templates that map other text-based fields that the plugin provides.

Important! Before you add a new template or edit an existing one, 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**.
8. Click **APPLY**.
9. To add another template, repeat steps 5 through 8.
10. Click **SAVE**.

On the **Bug Filing** page, the details for the bug tracking plugin now include your new template.

See also

["Velocity templates for bug filing" on the previous page](#)


["Customizing Velocity templates for bug tracker plugins" on the next page](#)

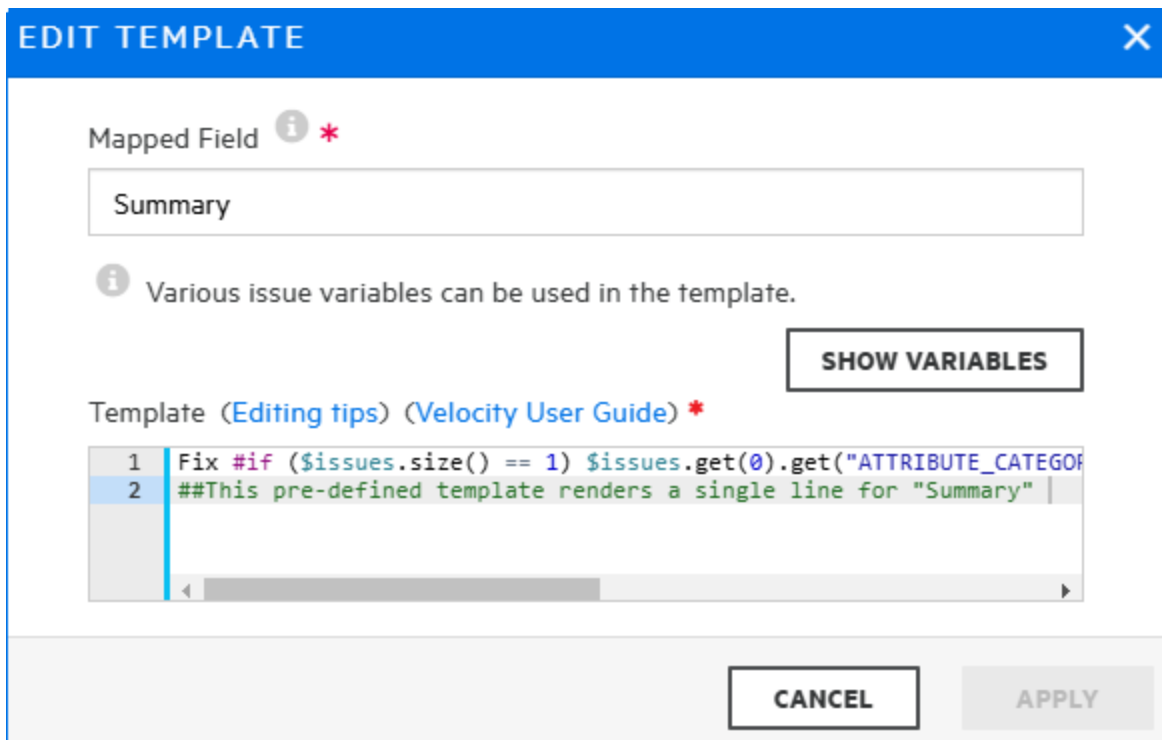
["Bug tracker configuration" on page 216](#)

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

Customizing Velocity templates for bug tracker plugins

To customize the Velocity template for a bug tracker plugin:

1. On the 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.



EDIT TEMPLATE

Mapped Field ⓘ *

Summary

ⓘ Various issue variables can be used in the template.

SHOW VARIABLES

Template (Editing tips) (Velocity User Guide) *

```
1 Fix #if ($issues.size() == 1) $issues.get(0).get("ATTRIBUTE_CATEGOR
2 ##This pre-defined template renders a single line for "Summary" |
```

CANCEL **APPLY**

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" below](#)

["Velocity templates for bug filing" on page 216](#)

["Adding Velocity Templates to Bug Tracker Plugins" on page 217](#)

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" on page 216](#)

["Adding Velocity Templates to Bug Tracker Plugins" on page 217](#)

["Customizing Velocity templates for bug tracker plugins" on the previous page](#)

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 Fortify Software Security Center verifies your connection to your bug tracker, it displays a message to indicate that the test was successful.
8. Click **OK**.
You can enable bug state management for the application version. With bug state management enabled, Fortify Software Security Center can update bugs as the states of the issues within those bugs change.
9. (Optional) To enable bug state management, select the **Bug state management** check box.
10. In the **Username** and **Password** boxes, provide the credentials for your bug tracker, and then click **APPLY**.
11. Click **OK**.
12. Click **CLOSE**.

See also

["About bug tracking system integration" on page 148](#)

["Adding bug tracker plugins" on page 149](#)

["Submitting a bug for multiple issues" on the next page](#)

["Authoring bug tracker plugins" on page 346](#)

Submitting a bug for a single issue

If a bug tracking plugin is specified for an application version (see ["Assigning a bug tracking system to an application version" on the previous page](#)), 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" on page 149](#) and ["Assigning a bug tracking system to an application version" on the previous page](#). Also, if a bug is already submitted for the issue, you cannot submit a new bug against it.

| Category | Primary Location | Previously Filed |
|----------------------------------|---------------------|------------------|
| Cross-Site Scripting: Persistent | BackDoors.java: 128 | |

3. In the **Login** area, provide the username and password for the bug tracker associated with this application version, and then click **LOGIN**.

Fortify Software Security Center retains your credentials for the duration of your work session so you do not have to provide them to file additional bugs during that session.

The **Login** 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" below](#)

["Viewing bugs submitted for issues" on page 295](#)

Submitting a bug for multiple issues


If a bug tracking plugin has been specified for an application version (see ["Assigning a bug tracking system to an application version" on page 219](#)), you can submit bugs that cover one or multiple issues. For information about how to file a bug for just one issue, see ["Submitting a bug for a single issue" on the previous page](#).

To submit a single bug that covers multiple issues:

1. From the **AUDIT** page for an application version, select the check boxes for all issues that you want to include in a bug, and then, above the issues table, click the **File Bug** 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" on page 219](#).

FILE ISSUES (3)

Login

Enter your username and password for logging into Bugzilla at . These are not your Fortify Software Security Center credentials.

Username:

Password:

LOGIN

Issues

Category ▾


Primary Location ▾

Previously Filed ▾

| | | |
|----------------------------------|---------------------|--|
| Cross-Site Scripting: Persistent | BackDoors.java: 128 | |
| Cross-Site Scripting: Persistent | BackDoors.java: 127 | |
| Cross-Site Scripting: Persistent | BackDoors.java: 125 | |

CANCEL

SUBMIT

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**.

Fortify Software Security Center retains your credentials for the duration of your work session so you do not have to provide them to file additional bugs during that session.

The **Login** section displays the fields for the bug tracker specified for the application version.

3. Provide input for all required fields, and then click **SUBMIT**.

After a successful submission, a bug icon is displayed for the selected issues in the **Bug submitted** column of the issues table.

See also

["Submitting a bug for a single issue" on page 220](#)

["Viewing bugs submitted for issues" on page 295](#)

Bug state management

Bug state management enables Fortify Software Security Center to make specific updates to bugs as the states of the issues within those bugs change. Fortify Software Security Center checks new security scans to determine whether filed bugs are to remain open, or can be closed.

If analysis results indicate that one of more security issues associated with a previously submitted bug persist (and match the selection criteria), Fortify Software Security Center checks the bug tracking system to ensure that the bug is in a valid open state and, if necessary, reopens the bug.

If all issues associated with a bug are removed (either because the issues were remediated or no longer match the selection criteria), Fortify Software Security Center updates the bug to indicate that stakeholders can resolve or close this ticket. To enable auditing and traceability, Fortify Software Security Center does not automatically resolve or close bugs.


For instructions on how to enable bug state management for an application version, see ["Assigning a bug tracking system to an application version" on page 219](#).

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, Fortify Software Security Center does not recalculate the issue metrics and metrics generated based on the previously assigned template are unavailable and cannot be deleted.

To change the template associated with an application version:

1. 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, Fortify Software Security Center 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.

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.

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 | Fortify Software Security Center compares the Build Project for the scan and the scan that preceded it. If the Build Projects differ, management approval is required before the scan can be uploaded. |
| Check external metadata file versions in scan against versions on server | If a user attempts to upload an FPR file, Fortify Software Security Center compares the external metadata version for the file with the external metadata version on the Fortify Software Security Center server. If the external metadata version for the FPR file is later than the external metadata file version on the server, Fortify Software Security Center requires approval for the file upload. If the external metadata version for the FPR file is earlier than, or the same as, the external metadata file version on the server, then Fortify Software Security Center allows the FPR file upload. |
| Require approval if file count decreases by more than 10%. | Fortify Software Security Center 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 |

| Processing rule | Description |
|--|--|
| | is required before the scan can be uploaded. |
| Require approval if file count increases by more than 10%. | Fortify Software Security Center 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 | Fortify Software Security Center 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%. | Fortify Software Security Center 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%. | Fortify Software Security Center 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 | Fortify Software Security Center checks if any scan engine 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 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. |

| Processing rule | Description |
|---|---|
| | <p>To enable uploading speed dial and quick scan analysis results, clear this check box.</p> <p>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.</p> |
| Require approval if the Rulepacks used in the scan do not match the Rulepacks used in the previous scan | Fortify Software Security Center 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 | Fortify Software Security Center checks if an OpenText 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 | <p>Fortify Software Security Center checks if an OpenText SAST or OpenText DAST Agent scan contains analysis warnings. If it detects analysis warnings, the scan upload requires management approval.</p> <p>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</p> |

| Processing rule | Description |
|---|---|
| | <p>previously-uploaded FPR file that contains analysis warnings, Fortify Software Security Center does not require management approval when the changed artifact is again uploaded.</p> |
| Perform Force Instance ID migration on upload | <p>A newer version of OpenText 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 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 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" on the next page.</p> |
| Automatically perform Instance ID migration on upload | <p>A newer version of OpenText 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 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.</p> <p>For detailed information about how this rule works, see "About processing rules that affect instance ID migration" on the next page.</p> |
| Warn if audit information includes unknown | <p>If the audit information includes an unknown</p> |

| Processing rule | Description |
|---|--|
| custom tag | 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, Fortify Software Security Center blocks upload of the analysis results. |
| Disallow upload of analysis results if there is one pending approval | If an analysis result still requires approval, Fortify Software Security Center 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 <i>not</i> 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](#). An issue instance ID can mutate for any one of the following reasons:

- The IID-generation algorithm changes with a new OpenText 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 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 SAST version, or from a change in Rulepack version. For example, Fortify Software Security Center detects that the OpenText 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, Fortify Software Security Center runs the migration. If Fortify Software Security Center detects no changes in the OpenText 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. Fortify Software Security Center can easily determine whether the OpenText SAST version or Rulepack version has changed. If Fortify Software Security Center detects such a change, it performs the migration automatically. However, in other cases (duplicate code, scan settings), Fortify Software Security Center cannot make this determination. You can use this processing rule to force Fortify Software Security Center to perform 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" on page 261](#)

["Approving analysis results for an application version" on page 265](#)

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" on page 78](#)). Otherwise, the default settings are used for all application versions.

To configure Fortify Audit Assistant options for an application version:

1. Ensure that Fortify Software Security Center 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" on page 78](#)

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, 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, Fortify Software Security Center 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**.

The screenshot shows a dialog box titled "APPLICATION PROFILE - LOGISTICS 2.5". It has several tabs: "ADVANCED OPTIONS", "CUSTOM TAGS", "PROCESSING RULES", "BUG TRACKER", "APPLICATION SETTINGS", "AUDIT ASSISTANT TRAINING", and "AUDIT ASSISTANT OPTIONS". The "AUDIT ASSISTANT OPTIONS" tab is selected. Inside this tab, there is a section for "Default prediction policy" with a dropdown menu currently showing "Generic". Below this are two checkboxes: "Enable auto-predict" and "Enable auto-apply", both of which are unchecked. At the bottom right of the dialog, there are two buttons: "CLOSE" and "APPLY".

4. To have Fortify Audit Assistant automatically assess unaudited issues, select the **Enable auto-predict** check box.

For information on auto-prediction, see ["About Fortify Audit Assistant auto-prediction" on page 80](#).

5. Select the **Enable auto-apply** check box.

If your primary tag values are not mapped to Audit Assistant, Fortify Software Security Center displays a warning to that effect and advises you to contact your Administrator.

6. Click **APPLY**.

7. To save your settings, click **OK**.

8. Click **CLOSE**.

See also

["Configuring Fortify Audit Assistant" on page 78](#)

About custom tags

To audit code in Fortify Software Security Center, the security team examines analysis results and assigns values to “tags” that are associated with application issues. The development team can then use these tag values to determine which issues to address and in what order.

By default, Fortify Software Security Center 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 Practice**. 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 Fortify Software Security Center 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 Fortify Software Security Center.

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 page 275](#).

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" on page 178). |
| 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" on page 235](#).

See also

["Mapping Fortify Audit Assistant analysis tag values to Fortify Software Security Center custom tag values" on page 298](#)

["Globally hiding custom tags" on the next page](#)

["Deleting custom tags" on the next page](#)

["About custom tags" on page 231](#)

["Editing custom tags" on page 239](#)

["Associating custom tags with issue templates" on page 240](#)

["Managing custom tags through issue templates" on page 243](#)

["Managing custom tags through an issue template in an FPR file" on page 243](#)

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" on page 235](#)

["Adding custom tags to the system" on the previous page](#)

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.

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" on page 242](#). For information on how to remove a custom tag from an issue template, see ["Removing custom tags from issue templates" on page 241](#).

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

["About custom tags" on page 231](#)

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 \(Fortify Audit Assistant configured\)" below](#).

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" on page 238](#).
10. To add additional values, repeat steps 5 through 9.

See also

["Add a custom tag value \(Fortify Audit Assistant configured\)" below](#)

["Assigning custom tags to application versions" on page 241](#)

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.

ADD VALUE ✕

Name *

Not an Issue

Description

Value Description

AA Custom Tag Auto Assignment * i

☒ Not an Issue

☐ Indeterminate (Below Not An Issue threshold)

☐ Exploitable

☐ Indeterminate (Below Exploitable threshold)

☐ Not Predicted

AA Training Classification for the Custom Tag's Value * i

☐ Skip for training

☒ False positive

☐ Suspicious

☐ Exploitable

In order for Audit Assistant Training tags to function, the custom tag used as the Audit Assistant training tag must, minimally, have one of its list values mapped to 'Exploitable' and another list value mapped to 'False Positive'. You cannot map a single list value to both, so you will need to choose two different list values to map from the previous screen.

☐ Hidden

CANCEL

APPLY

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" below](#)).
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" on page 241](#).


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.

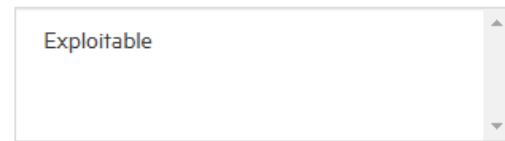
Issue State

Manage issue state assigned to Custom Tag values. Used only if the Custom Tag is a Primary Tag for an Application Version. Changes to Custom Tag value classification will apply only for audits made after the classification change.

Not an issue



Open issue



7. Repeat steps 5 and 6 until all values are in the appropriate Issue State list.
8. Click **SAVE**.

See also

["Editing custom tags" below](#)

["Deleting custom tag values" on the next page](#)

["Adding custom tags to the system" on page 232](#)

["Assigning custom tags to application versions" on page 241](#)

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" on page 232](#)

["Deleting custom tag values" on the next page](#)


["Assigning custom tags to application versions" on page 241](#)

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" on the previous page](#)

["Adding custom tags to the system" on page 232](#)

["Adding custom tag values" on page 235](#)

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" on the next page](#)

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

["About custom tags" on page 231](#)

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 Fortify Software Security Center, you must specify a value for the custom tag that is designated as the *primary tag*. By default, the **Analysis** tag is the primary tag.

During an audit, the primary tag is listed first. If list-type custom tags other than **Analysis** exist in your Fortify Software Security Center instance and are assigned to the application version, you can select one of these (instead of **Analysis**) as the primary tag.

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.

- a. Click **SELECT PRIMARY**.
- b. From the **Select Primary Tag** list, 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" on page 232](#). For information about how to edit a custom tag, see ["Editing custom tags" on page 239](#).

- c. 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" below](#)

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" on page 241](#)

["Adding custom tags to the system" on page 232](#)

["Assigning custom tags to application versions" on page 241](#)

Managing custom tags through issue templates

Custom tags defined in an issue template file are assigned to that specific issue template. You cannot update existing custom tags through direct issue template upload. If Fortify Software Security Center detects an updated custom tag, it displays a warning and prompts you to confirm that you want to continue.

You must update existing custom tags through the custom tag administration section of Fortify Software Security Center, as follows:

1. On the 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.

Managing custom tags through an issue template in an FPR file

FPR files typically contain an issue template. If an FPR file uploaded to Fortify Software Security Center contains an issue template with a custom tag that has been set as editable, you can add a value to the tag.

About deleting application versions

You cannot directly delete an application in Fortify Software Security Center. Fortify Software Security Center removes an application automatically after all of its versions are deleted.

If you are assigned the Administrator role in Fortify Software Security Center, you can delete any application version. If you are in the Security Lead or Manager role, then you can delete any application version to which you are assigned.

If you would rather not delete a version, but prefer instead to remove it from display on the **Dashboard** and **Applications** views, you can *deactivate* it.

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" below](#)

["Deleting an application version " on the next page](#)

Reactivating application versions

If a specific application version has been deactivated and is not listed on the **Dashboard** or 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.

APPLICATION PROFILE - RWI 2.0

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

Application Settings ?

Application Name
RWI

Application description
Riches Wealth International

Created by
admin

Version Settings

Version name: 2.0 [Pencil icon] [DELETE] [ACTIVATE]

Other Versions

Version name: 1.0 [Pencil icon] [DEACTIVATE]
Riches Wealth International.

[CLOSE] [APPLY]

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.

Deleting an application version

If you would rather not delete an application version, but prefer instead to remove it from display on the Fortify Software Security Center **Dashboard** and in the **Applications** view, see ["Deactivating application versions" on the previous page](#)

Important! If you delete all versions of an application, Fortify Software Security Center automatically deletes the application.

To delete a Fortify Software Security Center application version:

1. From the **Applications** view, select the 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**.
Fortify Software Security Center prompts you to confirm that you want to delete the version.
5. Click **OK**.

Fortify Software Security Center removes the version from the database.

Chapter 12: About webhooks

You can create webhooks to update external systems about events that occur in Fortify Software Security Center.

This section contains the following topics:

| | |
|---|-----|
| Webhooks permissions | 246 |
| Creating webhooks | 247 |
| Editing webhooks | 250 |
| Viewing webhook payloads | 250 |
| Redelivering webhook payloads | 251 |
| Deleting webhooks | 252 |

Webhooks permissions

The following table shows which Fortify Software Security Center roles have permission to perform which webhook-related tasks.

| Roles | Permissions |
|---------------|--|
| Administrator | User can create, view, and manage webhooks to monitor events. |
| Security Lead | <ul style="list-style-type: none">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. <p>A Security Lead cannot create or manage the following:</p> <ul style="list-style-type: none">Webhooks with the Send me everything! option selectedWebhooks with the Monitor All Application Versions option selectedWebhooks set to monitor any events that require universal access |

See also

["Viewing permissions for Fortify Software Security Center roles" on page 156](#)

Creating webhooks

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.

To create a new webhook:

1. Sign in to Fortify Software Security Center 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 Fortify Software Security Center integrations, you can select this check box to use it for webhooks. For information about how to configure a proxy for Fortify Software Security Center integrations, see "Configuring a proxy for integrations" on page 117 . |
| 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=. |

| Field | Description |
|--|---|
| Which events would you like to trigger this webhook? | <p>Do one of the following:</p> <ul style="list-style-type: none"> 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. <p>Global events (system-wide):</p> <p>USER_CREATED: A new local user, local group, or LDAP entity was added to Fortify Software Security Center.</p> <p>USER_DELETED: A local user, local group, or LDAP entity was deleted from Fortify Software Security Center.</p> <p>USER_UPDATED: A local user, local group, or LDAP entity was updated.</p> <p>LOCAL_USER_ACCOUNT_LOCKED: A local user was locked out of Fortify Software Security Center as a result of too many sign-in attempts with invalid credentials.</p> <p>APP_VERSION_CREATED: A new application version was created in Fortify Software Security Center.</p> <p>APP_VERSION_DELETED: An application version was deleted from Fortify Software Security Center.</p> <p>REPORT_GENERATION_COMPLETE: A new requested report is available for viewing and download.</p> <p>REPORT_GENERATION_REQUESTED: A new report was requested.</p> |

| Field | Description |
|---|---|
| | <p>Application version events (application version-specific):</p> <p>ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS: An uploaded artifact was successfully processed, and its data is available.</p> <p>ANALYSIS_RESULT_UPLOAD_FAILURE: An uploaded artifact was not successfully processed.</p> <p>ANALYSIS_RESULT_UPLOAD_REQUIRES_APPROVAL: An uploaded scan artifact requires approval before it can be processed.</p> <p>ANALYSIS_RESULT_INDEXING_COMPLETED: Indexing of data for global searches after Fortify Software Security Center finished processing an uploaded artifact was completed.</p> <p>ANALYSIS_RESULT_UPLOAD_APPROVE: An artifact was approved for uploading.</p> <p>APP_VERSION_UPDATED: An application version was updated.</p> |
| Which application versions would you like to monitor? | <p>Do one of the following:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> i. Click ADD. ii. From the APPLICATION list, select an application to monitor. iii. To select all versions, select the Select all check box. Otherwise select the check boxes for the versions. iv. To add more application versions, repeat steps ii through iii. v. 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

["Viewing webhook payloads" below](#)

["Deleting webhooks" on page 252](#)

Editing webhooks

To edit a webhook:

1. Sign in to Fortify Software Security Center 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" on page 247](#).
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" below](#)

["Creating webhooks" on page 247](#)

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 Fortify Software Security Center 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 |

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" on page 363](#)

["Deleting webhooks" on the next page](#)

["Creating webhooks" on page 247](#)

["Editing webhooks" on the previous page](#)

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" on page 247](#)

["Editing webhooks" on page 250](#)

["Viewing webhook payloads" on page 250](#)

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" on page 247](#)

["Editing webhooks" on page 250](#)

Chapter 13: Variables, performance indicators, and alerts

Fortify Software Security Center lets you store measured values and event conditions for application versions as variables. A 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. Fortify Software Security Center can also email alert notifications to members of an application version team.

This section contains the following topics:

| | |
|---|-----|
| Creating variables | 253 |
| Creating performance indicators | 255 |
| Creating alerts | 256 |
| Viewing and marking alerts | 259 |

Creating variables

As an Administrator or a Security Lead, you can define variables for your applications.

To create a Fortify Software Security Center 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 Fortify Software Security Center variable search string. For information about how to construct search strings, select the Syntax Guide link or see "Variable syntax" below. |
| 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.

Variable syntax

The Fortify Software Security Center 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. | (2,4] Indicates a range of greater than two and less than or equal to four |

| Relational operator | Description | Example |
|---------------------|---|--|
| | Use a parenthesis to specify that the range excludes (is greater than or less than) the adjoining number. | |
| ! (not equal) | Negate a search string with an exclamation character (!). | file:!Main.java Returns all issues that are not in Main.java. |

Creating performance indicators

Fortify Software Security Center performance indicators enable you to combine variables into metrics that are normalized across application version boundaries, and that can represent complex, high-level abstractions such as monetary costs. This topic provides information about performance indicator syntax and instructions on how to create performance indicators.

To create a Fortify Software Security Center performance indicator:

1. Sign in to Fortify Software Security Center as a Security Lead or Administrator, and then click the **Administration** tab.

Note: Users who are assigned the Manager or Developer role cannot create Fortify Software Security Center performance indicators.

2. 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. |

| Field | Description |
|-------------|--|
| | The format for a performance indicator is as follows: <i><variable><operator><variable></i> where <i><operator></i> is a standard mathematical operator (+, -, *, /), a comparator (==, >, <), or the ternary operator (?) and <i><variable></i> is an existing Fortify Software Security Center 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.

Creating alerts

Alert definitions can include variables or performance indicators to determine when Fortify Software Security Center is to generate an alert notification in the **Todo List** pane of the Dashboard.

Note: This functionality is available only if a Fortify Software Security Center Administrator has enabled email notifications.

You can configure alert notifications to send email messages about one or more alert notifications to users assigned to a given application version.

You can define alerts for any application versions to which you have been granted access.

To create a Fortify Software Security Center alert:

1. Sign in to Fortify Software Security Center 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 Fortify Software Security Center 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 | <ol style="list-style-type: none"> From the Alert when list, select a performance indicator. From the list of operators, select an operator. 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. To have your alert reset after each new artifact upload, select the Reset after triggering check box. |
| Variable | <ol style="list-style-type: none"> From the Alert when list, select a variable. From the list of operators, select an operator. 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. To have your alert reset after each new artifact upload, select the Reset after triggering check box. |
| System event | <ul style="list-style-type: none"> From the Alert when list, select the system event to trigger the alert. |
| Scheduled alert (Administrators only) | <ol style="list-style-type: none"> From the Alert when date box, click to open a calendar and specify the date on which Fortify Software Security Center is to send the alert. Type the hour and minute (hh:mm) at which to send the alert. |

| Alert type | Instructions |
|------------|---|
| | <ul style="list-style-type: none"> c. Click to toggle between AM and PM to set whether the alert is sent in the morning or afternoon. d. From the list of countries and regions, select the country or region to which your date and time settings apply. e. 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:
 - a. Click **ADD**.
 - b. 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.
 - c. To include inactive versions of the application in the **VERSIONS** list, select the **Show inactive** check box.
 - d. To use the alert for all application versions, select the **Select all** check box. Otherwise, in the **VERSIONS** list, select the check boxes for the versions to use for the alert.
 - e. To select versions of another application, repeat steps b through d.
 - f. 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" on the next page](#)

["Configuring email alert notification settings" on page 90](#)

["Configuring whether to receive email alerts" on page 92](#)

Editing alerts

To edit a Fortify Software Security Center alert:

1. Sign in to Fortify Software Security Center 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**.

Deleting alerts

To delete a Fortify Software Security Center alert:

1. Sign in to Fortify Software Security Center 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**.

Viewing and marking alerts

Fortify Software Security Center flags any unread alerts that either you or another user has set up for you to receive. These 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.

Chapter 14: Working with scan artifacts

The following sections describe the aspects of working with scan artifacts.

This section contains the following topics:

| | |
|---|-----|
| Uploading scan artifacts | 261 |
| Viewing scan artifact details | 263 |
| Downloading analysis results | 264 |
| Approving analysis results for an application version | 265 |
| Viewing issue metadata | 267 |
| Mapping analysis results to external lists | 268 |
| Purging scan artifacts | 268 |
| Deleting artifacts | 269 |

Uploading scan artifacts

The following procedure describes how to upload your scan artifacts to the Fortify Software Security Center database. For information about how to submit training metadata to Fortify Audit Assistant, see ["Submitting training data to Fortify Audit Assistant" on page 305](#).

Note: As it adds data to the database, Fortify Software Security Center truncates HTTP responses that contain more than 100,000 characters. Such responses are either cut off at the end, or contain `\n\n . . . \n\n` elsewhere in the response. This does not affect downloaded scans. It affects only the data displayed on the Fortify Software Security Center **AUDIT** page.

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

Important! To upload third-party artifacts, you must have the correct parser configured. For information, see ["Adding and managing parser plugins" on page 151](#).

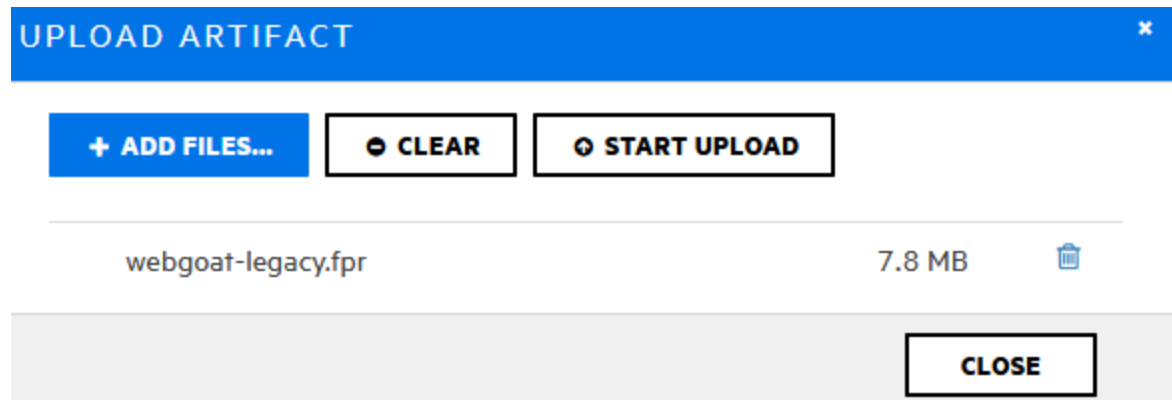
To upload a scan artifact to the Fortify Software Security Center database:


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 Core 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" on page 265](#).

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 analysis results" on page 264](#)

["Setting analysis result processing rules for application versions" on page 223](#)

["Uploading FPR files" on page 344](#)

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.

| ARTIFACT HISTORY | | | | | | |
|---|----------|-------------|------|--------|---------------|--|
| <div><div>ARTIFACT</div><div>APPLICATION FILE</div><div>APPLICATION & SOURCES</div><div>REFRESH</div></div> | | | | | | |
| Upload Date | Status | Uploaded by | Type | Audits | Scan Artifact | |
| 01/26/2025 10:47:13 PM | Complete | susan | SAST | | webgoat_5.fpr | |
| 01/26/2025 10:47:06 PM | Complete | susan | SAST | | webgoat_4.fpr | |
| 01/26/2025 10:46:59 PM | Complete | susan | SAST | | webgoat_3.fpr | |
| 01/26/2025 10:46:53 PM | Complete | lisa | SAST | | webgoat_2.fpr | |
| 01/26/2025 10:46:48 PM | Complete | susan | SAST | | webgoat_1.fpr | |

3. To view details for an artifact, click the corresponding row.

| | | | | | | | |
|--|---------------------------|---------------------|------------------------|------|------------------|-------------------------|--|
| 01/26/2025 10:46:48 PM | | Complete | susan | SAST | | webgoat_1.fpr | |
| Upload IP | Not Available | File Name | webgoat_1.fpr | | File Size | 857.6 KB | |
| Analysis Type | SAST | Analysis Date | 02/23/2009 11:48:12 AM | | Certification | VALID | |
| Engine Version | 5.7.0.0025 | Scan Elapsed Time | 01:59 | | Hostname | mobile-16 ... gular.net | |
| Number of Files | 168 | Total Lines of Code | 25913 | | Executable Lines | 8250 | |
| Build ID | webgoat | | | | | | |
| Rulepacks | 2009.4.0.0006, 5.1.0.0031 | | | | | | |
| <div><div>DOWNLOAD </div><div>DOWNLOAD WITH SOURCES </div><div>APPROVE </div><div>DENY </div><div>PURGE </div><div>DELETE </div></div> | | | | | | | |

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.

| RULEPACK DETAILS | |
|---|--|
| 2009.4.0.0006 | |
| <ul style="list-style-type: none">• Fortify Secure Coding Rules, Extended, JSP• Fortify Secure Coding Rules, Core, Java• Fortify Secure Coding Rules, Core, Annotations• Fortify Secure Coding Rules, Core, Classic ASP, VBScript, and VB6• Fortify Secure Coding Rules, Core, PHP• Fortify Secure Coding Rules, Extended, SQL• Fortify Secure Coding Rules, Extended, .NET• Fortify Secure Coding Rules, Core, SQL• Fortify Secure Coding Rules, Core, C/C++ | <ul style="list-style-type: none">• Fortify Secure Coding Rules, Extended, Content• Fortify Secure Coding Rules, Extended, Java• Fortify Secure Coding Rules, Core, JavaScript• Fortify Secure Coding Rules, Extended, C/C++• Fortify Secure Coding Rules, Extended, Configuration• Fortify Secure Coding Rules, Core, .NET• Fortify Secure Coding Rules, Core, ColdFusion• Fortify Secure Coding Rules, Core, Python |
| 5.1.0.0031 | |
| <ul style="list-style-type: none">• Fortify Secure Coding Rules, Core, COBOL | |

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" on the next page.](#)

See also

["Uploading scan artifacts" on page 261](#)

["Downloading analysis results" below](#)

["Purging scan artifacts" on page 268](#)

["Setting analysis result processing rules for application versions" on page 223](#)

["Uploading FPR files" on page 344](#)

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" on page 261](#)

["Deleting artifacts" on page 269](#)

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 result processing rules for application versions" on page 223](#).) 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.

The screenshot displays the OpenText Application Security interface. On the left, the 'Applications' view shows a list of applications. The 'Bill Payment Processor' application is selected, showing its version '1.1' with an alert icon (ⓘ) next to it. A red arrow points to this alert icon. On the right, the 'ARTIFACT HISTORY' table is shown. The table has columns for 'Upload Date' and 'Status'. The first row shows an upload date of '04/09/2021 10:39:58 AM' and a status of 'Requires Approval'. A red arrow points to the 'Requires Approval' status. Above the table, there are buttons for 'ARTIFACT', 'APPLICATION FILE', and 'APPLICATION & SOURCES'. The 'APPLICATION FILE' button is highlighted.

Note: If an artifact was uploaded by mistake or you do not want Fortify Software Security Center to process the artifact, see ["Denying processing approval"](#) below.

To approve analysis results for an application version so that Fortify Software Security Center 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**.

Fortify Software Security Center proceeds to process the artifact.

Denying processing approval

If an artifact was uploaded by mistake or, for some other reason, you do not want Fortify Software Security Center to process the artifact, you can either delete it, or, if you want to retain a record of the artifact upload, you can deny approval.

To deny approval of an artifact:

1. 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 Fortify Software Security Center 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**.


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**.

METADATA 

Instance ID:
3BC31286F68156D8BF9A7F34BA37635B

Primary Rule ID:
94B3FB0E-4AED-4006-9CDD-B2B1C13747EE

Fortify Priority:
Critical

Bug URL:

Priority Metadata Values:
Impact: 5
Likelihood: 5

Legacy Priority Metadata Values:
Severity: 4
Confidence: 5

[Fortify Taxonomy: Software Security errors](#)

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.

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 Fortify Software Security Center.

To import a new or modified external metadata document into Fortify Software Security Center:

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 Fortify Software Security Center and Fortify Audit Workbench, you can import the changed mapping document to Fortify Software Security Center, and then open the FPR file in Fortify Audit Workbench to see how the mapping works with the analysis results.

Purging scan artifacts

Purging an artifact recovers space from the Fortify Software Security Center database by removing the uploaded artifact, the temporary results of artifact processing, and the cross-reference information for source files.

Before you purge artifacts for an application version, consider the following:

- After the purge, you cannot delete the purged artifacts, or the earliest artifact not purged.
- Purging does not affect any issue-base metrics in the system.
- If you have custom reports, consult 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 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 Fortify Software Security Center 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.
4. Click **PURGE**.
5. To confirm purging the artifact, click **OK**.

See also

["Deleting artifacts" below](#)

Deleting artifacts

Deleting an artifact removes all traces of the artifact.

Note: You cannot delete an artifact that is being processed or one that has already been purged.

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

1. 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" on the previous page](#)

Chapter 15: Collaborative auditing

When an analysis engine (analyzer such as OpenText 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 Fortify Software Security Center, 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

Fortify Software Security Center 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" on page 194](#).


This section contains the following topics:

| | |
|---|-----|
| Viewing high-level summary metrics for an application version | 271 |
| About current issues state | 271 |
| Viewing information about issues to audit | 272 |
| Filtering issues for display | 275 |
| Searching issues | 276 |
| Searching globally | 281 |
| Auditing analysis results | 282 |
| Using Fortify Audit Assistant with Fortify Software Security Center | 297 |
| Exporting open source data | 306 |
| Integrating Fortify Software Security Center with Fortify WebInspect Enterprise | 306 |
| Viewing open source data | 313 |
| Downloading an OpenText Core SCA (Debricked) software bill of materials | 315 |

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.

| Version Progress | |
|--|--------------------------|
| Last measured on | Apr 28, 2021, 8:03:15 AM |
| Total Issues | 805 ↑ |
| Total Issues Audited % | 96.77% ↑ |
| Critical Priority Issues | 101 |
| Critical Priority Issues Audited % | 92.08% |
| Fortify Security Rating  | 1 |

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.

See also

["Viewing high-level summary metrics for your application versions" on page 182](#)

About current issues state

Fortify Software Security Center 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, Fortify Software Security Center merges that information into any existing audit information for a given issue. Fortify Software Security Center also marks an issue as *removed* after the analysis engine no longer finds the issue.

Whenever new analysis results are uploaded, Fortify Software Security Center checks every issue to determine if it was uncovered in a previous scan.

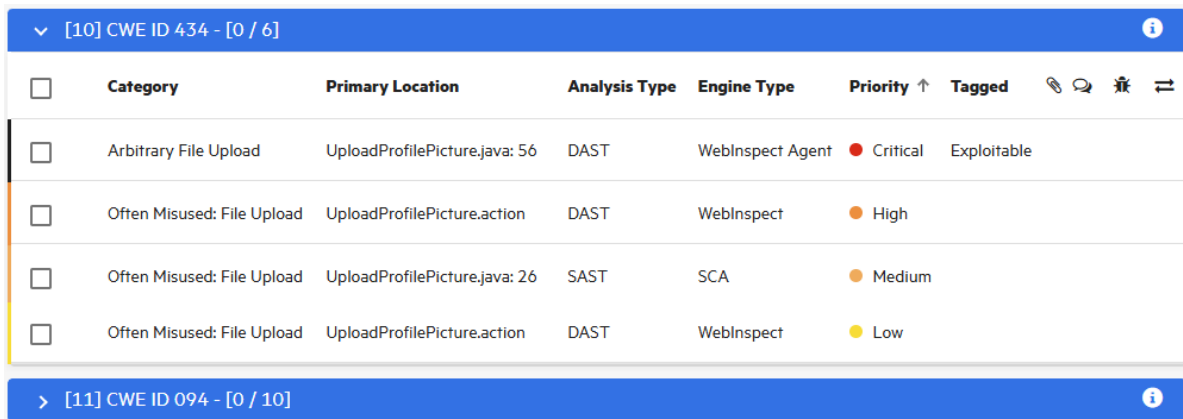
Viewing information about issues to audit

To display the issues you want to audit:

1. Upload analysis results for the application version you want to audit (see ["Uploading scan artifacts" on page 261](#)).
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" on page 275](#) and ["Viewing issues based on folders" on the next page](#).




4. In the issues table, if you have selected a grouping, expand a group to view the issues it contains.



| [10] CWE ID 434 - [0 / 6] | | | | | | | |
|------------------------------|----------------------------|-------------------------------|---------------|------------------|--|-------------|--|
| <input type="checkbox"/> | Category | Primary Location | Analysis Type | Engine Type | Priority ↑ | Tagged | |
| <input type="checkbox"/> | Arbitrary File Upload | UploadProfilePicture.java: 56 | DAST | WebInspect Agent | ● Critical | Exploitable | |
| <input type="checkbox"/> | Often Misused: File Upload | UploadProfilePicture.action | DAST | WebInspect | ● High | | |
| <input type="checkbox"/> | Often Misused: File Upload | UploadProfilePicture.java: 26 | SAST | SCA | ● Medium | | |
| <input type="checkbox"/> | Often Misused: File Upload | UploadProfilePicture.action | DAST | WebInspect | ● Low | | |
| > [11] CWE ID 094 - [0 / 10] | | | | | | | |

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 |
| | Indicates whether any attachments are associated with the issue |

| Column | Description |
|--|---|
| Contains attachment | |
|  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 | <p>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.</p> <p>If either a subsequent static scan or dynamic scan shows an issue was fixed, the correlation icon is removed.</p> <p>(Sort displays correlated issues first or last.)</p> |

See also

["Auditing analysis results" on page 282](#)

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*).

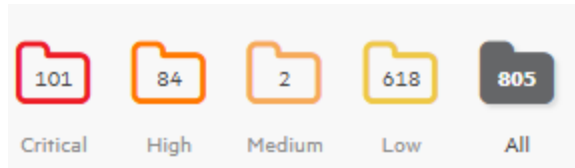
Note: When you edit or create filter sets and folders in Fortify Audit Workbench, be aware that the search modifiers used by Fortify Audit Workbench and Fortify Software Security Center might not match. Not all searches, filters, or folders based on search expressions produce the same results. In addition, if your search expression contains external metadata categories such as OWASP or CWE, your results might not match because the expressions might differ on Fortify Software Security Center and Fortify Audit Workbench. When there are multiple matched external categories, Fortify Software Security Center 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 Fortify Software Security Center, 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.

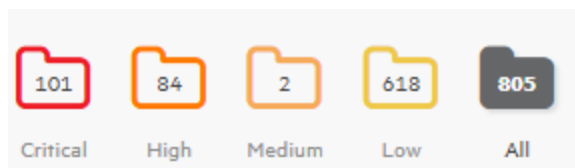
2. To see the number of issues in a folder that have been reviewed, point to the folder.



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 next page](#)

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" on page 290](#)

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" on page 291](#).

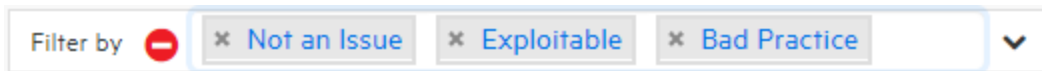
To filter issues for display on the **OVERVIEW** or **AUDIT** page:


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 .

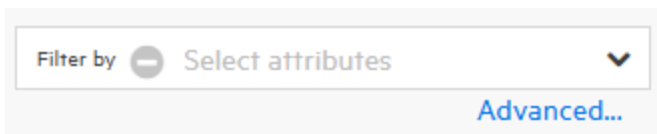
2. From the **Filter by** list, select the attributes to use to filter the issues for display in the issues table.

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:
 - a. Click the **Advanced** link.



- b. 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.


- c. To refine the **Select filters** list further, type a text string in the **Filter options** box, and then click **FIND**.

The **Select filters** list displays the filters that contain the matching text.

To see the complete list of filters again, click the **x** in the **Filter options** box.

- d. 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.
- e. To add filters for another filter category, repeat steps b through d.
- f. 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" on page 288](#)

["Searching issues" below](#)

["Viewing issues based on folders" on page 273](#)

["Searching globally " on page 281](#)

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, Fortify Software Security Center returns only issues that match all of the modified search terms. For example, `file:ApplicationContext.java category:SQL Injection` returns only SQL injection issues found in `ApplicationContext.java`.

If you use the same modifier more than once in a search string, then the search terms qualified by those modifiers are treated as an OR comparison. For example,

`file:ApplicationContext.java category:SQL Injection category:Cross-Site Scripting` returns SQL injection issues and cross-site scripting issues found in `ApplicationContext.java`.

For complex searches, you can also insert the AND or the OR keyword between your search queries. Note that AND and OR operations have the same priority in searches.

3. Click **Find**.
4. To return to the complete issues list, clear the text in the search box.

See also

["Search modifiers" below](#)

["Filtering issues for display" on page 275](#)

["Search query examples" on page 280](#)

["Searching globally " on page 281](#)

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 <code>exploitable</code> , <code>not an issue</code> , and so on. |

| Modifier | Description |
|----------------------------|---|
| [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 | <p>Searches for issues by intended audience. Valid values are targeted, medium, and broad.</p> <p>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.</p> |
| 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 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> | <p>Searches for issues based on the value of the specified custom tag.</p> <p>To search for a specific date in a date-type custom tag, specify the date in the format: yyyy-mm-dd.</p> <p>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:</p> <p>[Target Date]:<none></p> |
| [engine priority] | Searches for issues based on the original priority value |

| Modifier | Description |
|--------------------------|---|
| | 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 <i>critical</i> , <i>high</i> , <i>medium</i> , and <i>low</i> . |
| historyuser | Searches for issues that have audit data modified by the specified user. |
| [issue age] | Searches for the issue age, which is <i>new</i> , <i>updated</i> , <i>reintroduced</i> , or <i>removed</i> . |
| 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] . |

| Modifier | Description |
|------------------|--|
| [source context] | Searches for dataflow issues that have the source function call contained in the specified code context Also see source and [primary context] . |
| sourcefile | Searches for dataflow issues with the source function call that the specified file contains. Also see file . |
| status | Searches issues that have the status reviewed, not reviewed, or under review. |
| suppressed | Searches for suppressed issues. |
| taint | Searches for issues that have the specified taint flag. |

For examples of search queries that use modifiers, see ["Search query examples" below](#).

See also

["Searching issues" on page 276](#)

Search query examples

The following table contains search query examples.

| 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 |

| Search target | Query |
|---|-----------------------|
| 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" on page 276](#)

["Search modifiers" on page 277](#)

Searching globally

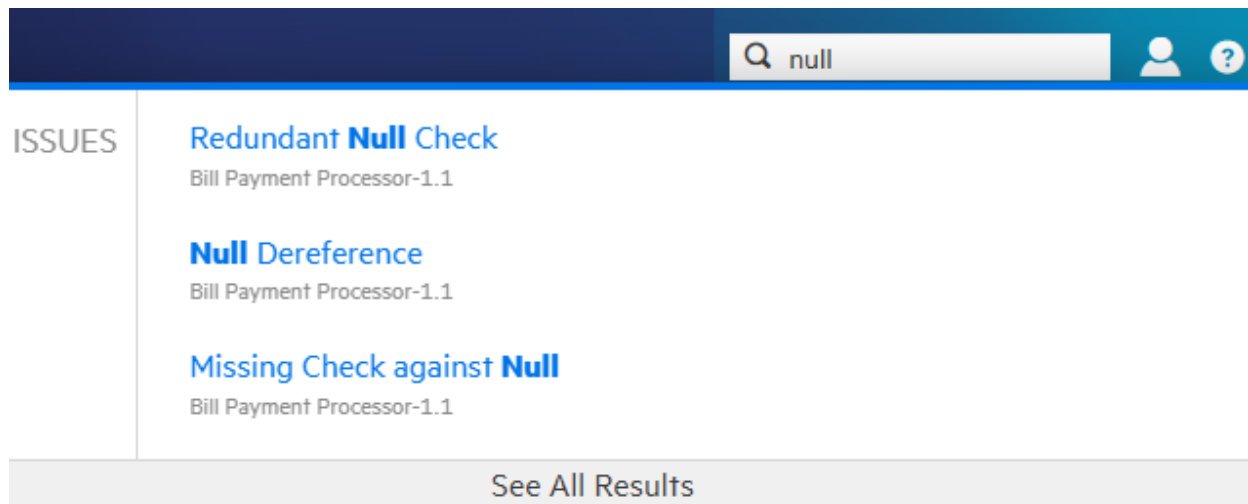
Regardless of the view you have open, you have access to the global **Search** box on the header. Any search string you type here is applied across all application versions, issues, reports, comments, and users.

Note: The search box is visible only if **Enable global search** was selected during Fortify Software Security Center setup. For more information, see ["Configuring Fortify Software Security Center for the first time" on page 68](#).


To use the global **Search** box:

1. From any view, type a search string into the **Search** box.
Fortify Software Security Center displays the first several items that match your search string, grouped by category. The application version is also displayed.
2. To go to a specific item listed, click the item.
3. To see a list of all search results, below the listed items, click **See All Results**.

Example: Finding issues



After you select an issue from the listed results, Fortify Software Security Center takes you to the corresponding version page with the issue expanded to full view.

If you select **See All Results**, Fortify Software Security Center takes you to the **Search Results** page. From here, you can open the first match with the issue expanded to full view. From there, you can use the next and previous buttons  to page through all of the 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" on page 290](#).

See also

["Searching applications and application versions from the Applications view" on page 212](#)

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" on page 261](#).
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" on page 275](#) and ["Viewing issues based on folders" on page 273](#).

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:

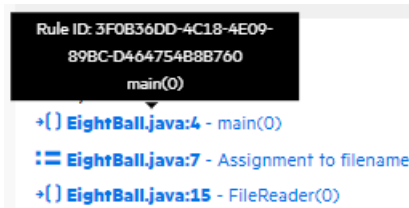
1. To expand an issue and view its details, click its row in the table.

For information about viewing OpenText DAST results, see ["Viewing OpenText DAST analysis results in Fortify Software Security Center" on page 307](#).

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.

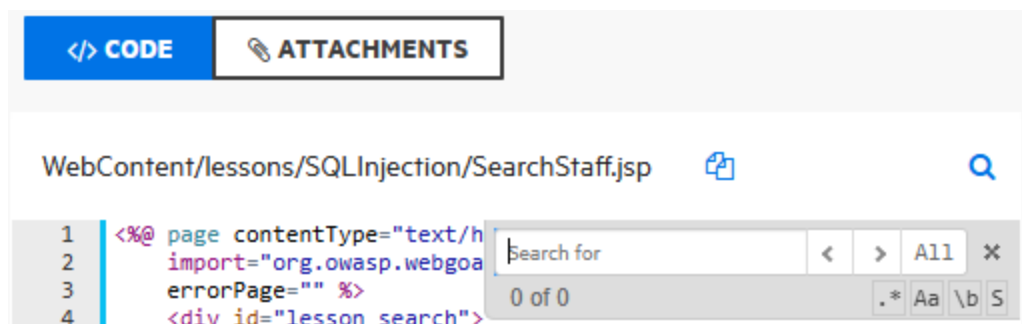
2. To view summary details about a step along the course that tainted data has taken, under **Analysis Trace**, point to that step.





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:
 - a. On the **CODE** tab, click the search button .
 - b. 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.

AUDIT **HISTORY** INFO ISSUE HISTORY

Detected on: 08/10/2024 3:09:48 AM

09/26/2024 2:17:38 PM

Changed SUPPRESSED to true

09/26/2024 2:16:25 PM

Changed User to alaya

09/26/2024 2:16:25 PM

Changed Analysis to Reliability Issue

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.

AUDIT HISTORY **INFO** ISSUE HISTORY

OVERVIEW



DETAILS



RECOMMENDATIONS



METADATA



ADDITIONAL REFERENCES



IMPLICATIONS



7. To expand a row and view a category of information, click the corresponding arrow (➤).

AUDIT HISTORY **INFO** ISSUE HISTORY

OVERVIEW

Hardcoded passwords can compromise system security in a way that cannot be easily remedied.

DETAILS

8. To view attribute changes for an issue, select the **ISSUE HISTORY** tab.

Click **ARTIFACT DETAILS** to view the list of artifacts from the scan history. For more information, see ["About audit issue history" on page 145](#).

AUDIT HISTORY INFO **ISSUE HISTORY**

CHANGED ON 09/26/2024 1:49:29 PM

ARTIFACT DETAILS

SEVERITY changed from 1.0 to 2.0

CONFIDENCE changed from 1.0 to 2.0

LIKELIHOOD changed from 0.16 to 0.32

CHANGED ON 09/26/2024 1:49:23 PM

ARTIFACT DETAILS

SEVERITY changed from 3.0 to 1.0

CONFIDENCE changed from 5.0 to 1.0

LINE changed from 12 to 15

CODESNIPPET changed from

DAC70D056E8A1305D44B055B9B76C154#Eight

Ball.java:12:12 to

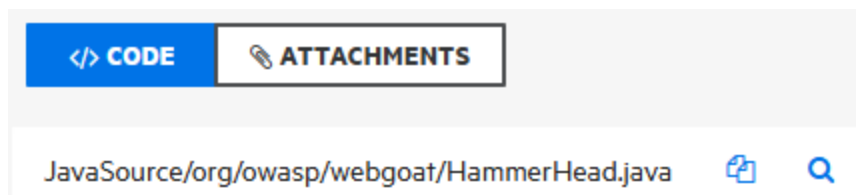
B5E2AAD84E148E1C439D0BFF1A3E75E4#Eight

Ball.java:15:15

LIKELIHOOD changed from 0.8 to 0.16

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. 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:
- Click **ATTACHMENTS**.



- Click **CLICK HERE TO ADD**.
- In the **UPLOAD ATTACHMENT** dialog box, click **BROWSE**, and then select the file you want to upload.


Note: The file size must not exceed 3 MB.



- (Optional) In the **Description** box, type a description of the file.
 - Click **SAVE**.
- If you attached an image file, Fortify Software Security Center 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:

- a. Under **USER**, click the **Edit assigned user** button .
- b. To locate a user to assign to the issue from the **SELECT USER** dialog box, in the **Find user** box, type part or all of a user's name, and then click **FIND**.
- c. In the list of returned names, click the name of the user to assign to the issue.
- d. Click **DONE**.

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, Fortify Software Security Center 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.

ABC 

Add a comment about this custom tag value change

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" on page 302](#).

17. In the **COMMENTS** box, type a comment about this issue audit.

18. Click **SAVE**.

See also

["Auditing correlated issues" on the next page](#)

["Auditing a batch of issues" on page 296](#)

["About Fortify Audit Assistant" on page 78](#)


["About audit issue history" on page 145](#)










["Configuring application security training" on page 77](#)

Auditing correlated issues

If the artifacts uploaded for the application version include results from both static (OpenText SAST) and dynamic (OpenText 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 .

| <input type="checkbox"/> Category | Primary Location | Analysis Type | Engine Type | Priority | Tagged |  |  |  |  |  |
|--|-------------------------|---------------|-------------|--|--------|---|---|---|---|---|
| <input type="checkbox"/> Cross-Site Scripting: Reflected | xss | DAST | WebInspect | ● Critical | | | | |  | |
| <input type="checkbox"/> Cross-Site Scripting: Reflected | xss | DAST | WebInspect | ● Critical | | | | |  | |
| <input type="checkbox"/> Cross-Site Scripting: Poor Validation | FindOwnersForm.java: 84 | SAST | SCA | ● Medium | | | | |  | |
| <input type="checkbox"/> 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.

|  This list of correlated issues is either targeting or originated from the highlighted issue. | | | | | | | | | | |
|--|------------------------|---------------|-------------------|--|--------|---|---|---|---|---|
| <input type="checkbox"/> Category | Primary Location | Analysis Type | Engine Type | Priority | Tagged |  |  |  |  |  |
| <input type="checkbox"/> <i>Cross-Site Scripting: Reflected</i> | <i>xss</i> | <i>DAST</i> | <i>WebInspect</i> | ● <i>Critical</i> | | | | |  | |
| <input type="checkbox"/> Cross-Site Scripting: Reflected | XssController.java: 24 | SAST | SCA | ● Critical | | | | |  | |

You can audit the listed issues as described in ["Auditing analysis results" on page 282](#).

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**.


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 analysis results" on page 282](#).

| <input type="checkbox"/> Category | Primary Location |
|--|--|
| <input type="checkbox"/> J2EE Bad Practices: Leftover Debug Code | EightBall.java: 4 |
| <input type="checkbox"/> 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 Fortify Software Security Center 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*.

| <input type="checkbox"/> Category ⇅ | Primary Location ⇅ |
|---|--|
| <input type="checkbox"/> Cross-Site Scripting: Persistent |  CSRF.java: 193 |

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.

| <input type="checkbox"/> Category ⇅ | Primary Location ⇅ |
|--|--|
| <input type="checkbox"/> Insecure Randomness |  WeakSessionID.java: 77 |

See also

["Setting issue viewing preferences" below](#)

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.
Fortify Software Security Center 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 suppressed issues. Each suppressed issue is tagged with an **S** in the **Primary Location** column.

Viewing removed issues

When Fortify Software Security Center 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.
Fortify Software Security Center 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 Fortify Software Security Center, hidden issues are the issues that are not shown because of the filter set rules currently in effect.

To reveal any hidden issues associated with an application version:

1. From the Dashboard or Applications view, select the version for the application version you are interested in.

Fortify Software Security Center opens the **AUDIT** page for the selected version.

2. On the 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.

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.

Fortify Software Security Center 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.

Overriding assigned issue priority

When analysis results are parsed and loaded into Fortify Software Security Center, the scan parser for each supported engine type assigns a priority value to each issue. However, this priority value does not reflect the full context of the affected code or application. Other factors that concern the use of the affected code 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, Fortify Software Security Center provides the capability for trusted users to change the priority originally assigned to an issue. Such priority changes are reflected in generated reports.

Caution! 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 Fortify Software Security Center 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" on page 187](#).

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**.

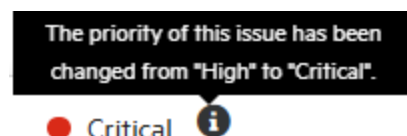
Viewing issues that have changed priority values

To view issues that have priority values that you and others have manually assigned, from the **Group by** list, select **Priority Override**.

| Critical - [2 / 2] | | | | | | | |
|--|--------------------|---------------|-------------|---------------------------|--------------|--|--|
| <input type="checkbox"/> Category ↑ | Primary Location | Analysis Type | Engine Type | Priority ? | Tagged | | |
| <input type="checkbox"/> Header Manipulation | config.jsp: 12 | SAST | SCA | ● Critical ⓘ | Suspicious | | |
| <input type="checkbox"/> Password Management: Hardcoded Password | DOS_Login.java: 64 | SAST | SCA | ● Critical ⓘ | Not an Issue | | |

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:

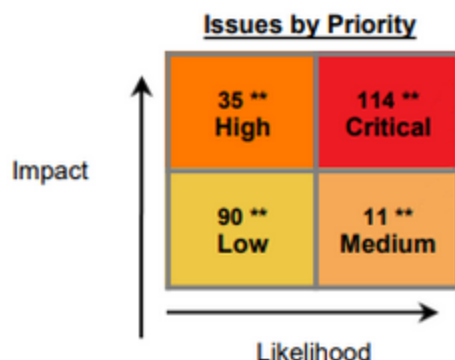
Fortify Software Security Center

OWASP Top 10 2021

RWI - 1.0

Note: This report calculates counts based on issue priority. Issue priority is initially set based on the raw scan information. However, reviewers are able to modify the original issue priority based on additional contextual information. If the issue details section is included in the report, it will indicate the issues where the original value has been changed.

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.spic | | |
| Location | Analysis Info | Analyzer |
| WEB-INF/src/java/com/order/spic/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.spic.ConnFactory.ConnFactory() In WEB-INF/src/java/com/order/spic/ConnFactory.java:16 | SCA |
| WEB-INF/src/java/com/order/spic/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.spic.ConnectionFactory.ConnectionFactory() In WEB-INF/src/java/com/order/spic/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.

Viewing bugs submitted for issues

The issues table on the **AUDIT** page includes a **Bug submitted** column  that shows whether a bug has been submitted against a listed issue.

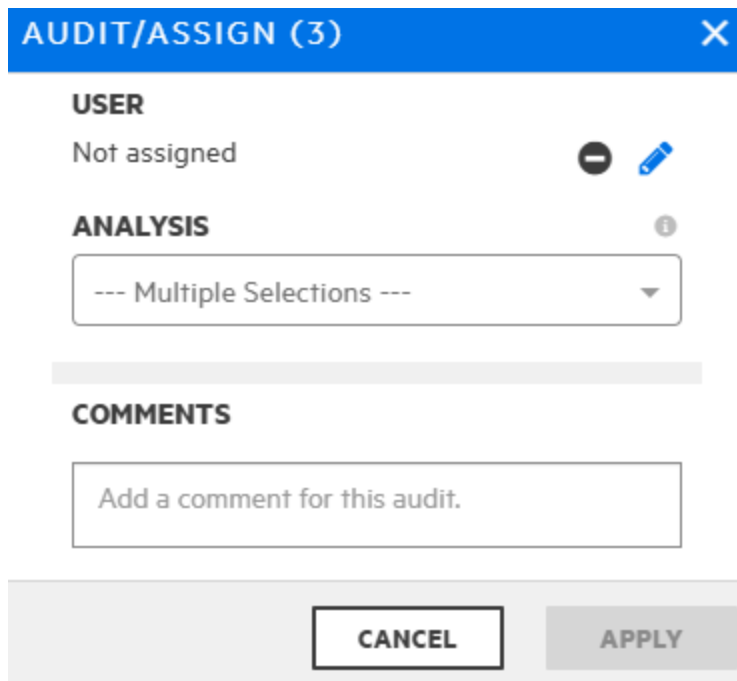
To view the bug, click the **VIEW BUG** icon , and log in to the assigned bug tracking application.


Tip: To view a bug, you must use a browser supported by the bug tracker application.

Auditing a batch of issues

To audit multiple issues at a time for an application version:

1. 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:
 - a. Select the **Edit assigned user** button .
 - b. To find a user account, in the **Find user** box, type part or all of a user's name, and then click **FIND**.
 - c. In the list of returned names, click the name of the user to assign.
 - d. Click **DONE**.

The **USER** section now displays the selected user name and avatar (if available).

5. From the **ANALYSIS** list (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" on page 302](#).

7. (Optional) In the **COMMENTS** box, type a comment about this issue audit.
8. Click **APPLY**.

See also

["Auditing analysis results" on page 282](#)

Using Fortify Audit Assistant with Fortify Software Security Center

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 Fortify Software Security Center 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 Fortify Software Security Center version 23.2.0 or later.

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 Core Application Security 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 Fortify Software Security Center custom tag values" on the next page.](#)


Mapping Fortify Audit Assistant analysis tag values to Fortify Software Security Center custom tag values

To use Fortify Audit Assistant with Fortify Software Security Center, you must map Fortify Audit Assistant analysis tag values to Fortify Software Security Center list-type custom tag values. You can map the Fortify Audit Assistant analysis tag values to the **Analysis** custom tag that is installed with Fortify Software Security Center 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" on page 235](#) 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 Fortify Software Security Center 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.

ADD VALUE ✕

Name *

Not an Issue

Description

Value Description

AA Custom Tag Auto Assignment * i

☒ Not an Issue

☐ Indeterminate (Below Not An Issue threshold)

☐ Exploitable

☐ Indeterminate (Below Exploitable threshold)

☐ Not Predicted

AA Training Classification for the Custom Tag's Value * i

☐ Skip for training

☒ False positive

☐ Suspicious

☐ Exploitable

In order for Audit Assistant Training tags to function, the custom tag used as the Audit Assistant training tag must, minimally, have one of its list values mapped to 'Exploitable' and another list value mapped to 'False Positive'. You cannot map a single list value to both, so you will need to choose two different list values to map from the previous screen.

☐ Hidden

CANCEL

APPLY

If Fortify Software Security Center 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

["Configuring Fortify Audit Assistant" on page 78](#)

["Adding custom tag values" on page 235](#)

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" on page 229](#)

["Configuring Fortify Audit Assistant" on page 78](#)

["About Fortify Audit Assistant auto-prediction" on page 80](#)

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 [Updating the Fortify Audit Assistant configuration](#).
2. Obtain a Fortify Audit Assistant account.
 - a. Go to <https://analytics.fortify.com>.
 - b. Click the **Need an Account?** link.

The **Request a Fortify Audit Assistant Tenant** window opens.
 - c. 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 Fortify Software Security Center:
 - 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 Fortify Software Security Center 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" on page 78](#).

6. From Fortify Software Security Center, 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 Fortify Audit Assistant" on page 305](#).

7. From Fortify Software Security Center, open an application version and submit its OpenText 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 setting prediction policies" on page 300](#)

["Configuring Fortify Audit Assistant" on page 78](#)

["Configuring Fortify Audit Assistant options for an application version" on page 229](#)

["Enabling auto-apply and auto-predict for an application version" on page 230](#)

["Submitting training data to Fortify Audit Assistant" on page 305](#)

["Reviewing Fortify Audit Assistant results" below](#)

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" on page 273](#) and ["Filtering issues for display" on page 275](#).

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.

Criticality ▲ Tagged ◆

High Exploitable ✎

SUPPRESS

GET TRAINING

< > ↗ ↘

AUDIT

DETAILS

RECOMMENDATIONS

USER

Not assigned

✎

ANALYSIS ✎

i

Exploitable ▼

AA_PREDICTION

i

Exploitable ▼

AA_CONFIDENCE

i

0.994

COMMENTS

Type here...

SAVE

UNDO

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" on page 78](#)

["Auditing analysis results" on page 282](#)

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 Fortify Software Security Center 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 Fortify Software Security Center custom tag values" on page 298](#)

["Submitting training data to Fortify Audit Assistant" on the next page](#)

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 EXPLOITABLE and FALSE POSITIVE results. All languages might not reach this threshold at the same time.

For more information, see ["About Fortify Audit Assistant training" above](#).

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 ASSISTANT 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.

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" on page 302](#)

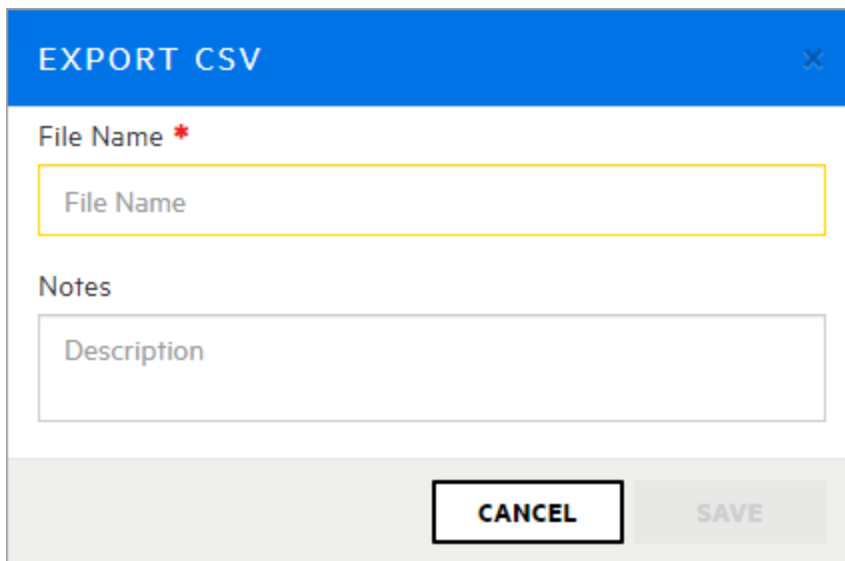
["About Fortify Audit Assistant" on page 78](#)


["Enabling auto-apply and auto-predict for an application version" on page 230](#)

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**.

A screenshot of the 'EXPORT CSV' dialog box. The dialog has a blue header bar with the title 'EXPORT CSV' and a close button (X). Below the header, there is a 'File Name' field with a red asterisk indicating it is required. The field contains the placeholder text 'File Name'. Below this is a 'Notes' section with a text area containing the placeholder text 'Description'. At the bottom of the dialog, there are two buttons: 'CANCEL' and 'SAVE'.

3. In the **File Name** box, type the name for the CSV file to generate.
4. (Optional) In the **Notes** box, type any notes to associate with the generated file.
5. Click **SAVE**.
6. To view the exported result:
 - a. On the header, select **Reports**.
 - b. Click the **DATA EXPORTS** tab.
 - c. 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" on page 123](#). The default expiration period for these reports is two days.

Integrating Fortify Software Security Center with Fortify WebInspect Enterprise

Fortify Software Security Center and Fortify WebInspect Enterprise are closely integrated and can share analysis results. Administrators can also submit requests for dynamic scans from the user

interface. This section describes how to view OpenText DAST results in Fortify Software Security Center and provides instructions for Fortify Software Security Center users on how to request dynamic scans.

Viewing OpenText DAST analysis results in Fortify Software Security Center

OpenText DAST saves analysis results (results data and audit data) in FPR format, which you can upload to Fortify Software Security Center. See ["Uploading scan artifacts" on page 261](#). OpenText DAST issue details differ from those shown for issues uncovered by other analyzers, such as OpenText SAST.

Important! To successfully integrate OpenText DAST with Fortify Software Security Center, you must install a trusted CA certificate on the Java™ Runtime Environment on both the Fortify Software Security Center and OpenText 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**.

Cross-Site Scripting hidden_AdminControl.jsp WEBSPECT Critical

CODE **COMMENTS & HISTORY** **ATTACHMENTS** **SUPPRESS** **GET TRAINING**

Overview

Cross-Site Scripting vulnerabilities were verified as executing code on the web application. Cross-Site Scripting occurs when dynamically generated web pages display user input, such as login information, that is not properly validated, allowing an attacker to...

Implication

XSS can generally be subdivided into two categories: stored and reflected attacks. The main difference between the two is in how the payload arrives at the server. Stored attacks are just that...in some form stored on the target server, such as in a database, or via a submission to a bulletin board or visitor log. The victim will retrieve and execute the attack code in his browser when a request is made for the stored information. Reflected attacks, on the other hand, come from somewhere else. This happens when user input from a web client is immediately included via server-side scripts in a dynamically generated...

Additional References

HP Cross-Site Scripting Whitepaper
http://download.hpsmartupdate.com/asclabs/cross-site_scripting.pdf

OWASP Cross-Site Scripting Information
<http://www.owasp.org/documentation/toplen/a4.html>

Microsoft
<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q252985>

Microsoft Anti-Cross Site Scripting Library V1.0
<http://www.microsoft.com/downloads/details.aspx?familyid=9a2b9c92-7ad2-408d-b3cf-50036>

URL: http://tomcatss.spidynamics.com:80/riches/pages/common/hidden_AdminControl.jsp

Method: GET

Vulnerable Parameter: users

Attack Payload: users: 12345%3csCriPt%3ealert(64872)%3c%2fsCriPt%3e

Request

```
GET /riches/pages/common/hidden_AdminControl.jsp?actions=12345&message=1974&users=12345%3csCriPt%3ealert(64872)%3c%2fsCriPt%3e HTTP/1.1
Referer: http://tomcatss.spidynamics.com:80/riches/pages/common/hidden_AdminControl.jsp
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Accept: */*
Pragma: no-cache
Host: tomcatss.spidynamics.com
X-Scan-Memo: Category="Audit"; Function="createStateRequestFromAttackDefinition"; SID="D
Connection: Keep-Alive
Cookie: CustomCookie=WebInspect745672X283F9C295F5541D79D520A8090293A15YA029;JSESSIONID=C...
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 15 Sep 2011 16:45:10 GMT
X-WIPP-Version: java / 1.0 / tomcatss_5575
X-WIPP-RequestID: fcd7ba7f-5c93-484b-807f-67f11698778b
Content-Type: text/html; charset=ISO-8859-1
Content-Length: 901
Vary: Accept-Encoding
Keep-Alive: timeout=15, max=1
Connection: Keep-Alive

<form method=get action="hidden_AdminControl.jsp">
  Shell Command<br />
  <input name="actions" type=text size="80"><br />
  <input type=submit value="Execute"><br />
  Automated shutdown message (sent to everyone by default)<br />
  <input name="message" type=text size="80"><br />
  <input type=submit value="Send to Specific Users (semicolon separated list)"><br />
  <input name="users" type=text size="80"><br />
  <input type=submit value="Broadcast Alert">

  <div>Emergency Broadcast sent to users:</div><pre>12345<scripT>alert(64872)</scripT>
</pre>

  <div>Transactions reported from database for account <div>12345</div></div>

  <br /><br /><div>Debug Code</div><br />
  <div>Note: This code should be removed once debugging is complete for bug 192203 (inspec
  Account Number <input name="acctno" type=text size="15"><br />
  <input type=submit value="Retrieve">
</form>
```

AUDIT

USER
Not Assigned



ANALYSIS
Not Set

COMMENTS
Type Here...

SAVE **UNDO**

The **Steps** tab is available only if the steps are included in the OpenText 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 analysis results" on page 282](#).

OpenText DAST audit data

In addition to screen shots, the following types of audit data are transferred from OpenText DAST to Fortify Software Security Center:

- **Vulnerability Notes**—Vulnerability notes in OpenText DAST are transferred to Fortify Software Security Center as issue comments.
- **Ignored Vulnerabilities**—Vulnerabilities marked as “Ignored” in OpenText DAST are marked “Suppressed” after transfer to Fortify Software Security Center.
- **False Positives**

False positives

Fortify Software Security Center does not have a direct equivalent of the OpenText DAST “false positive” status. If an OpenText 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 Fortify Software Security Center, you can use the default **Analysis** custom tag. An OpenText DAST false positive is assigned the **Analysis** value “Not an Issue” in Fortify Software Security Center. To emulate the OpenText DAST behavior of hiding the issue from lists and counts, the issue is marked as **Suppressed**.

| <input type="checkbox"/> | Category | Primary Location |
|--------------------------|--|--------------------------|
| <input type="checkbox"/> | Poor Error Handling: Unhandled Exception | S index.jsp |

Note: If the selected value for **Analysis** has changed from “Not an Issue” or is missing, or if the **Analysis** list has been removed from your application version, then the false positive status of the issue is lost. The issue is marked as “Suppressed.”

See also

["Setting issue viewing preferences" on page 290](#)

Submitting dynamic scan requests to Fortify WebInspect Enterprise

If OpenText DAST is installed in your environment, and you are assigned to one of the following roles, you can request scans from Fortify Software Security Center:

- 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 Fortify Software Security Center 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 |

| Dynamic scan attribute | Description |
|------------------------|---|
| | 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 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**.

Fortify Software Security Center displays a message to verify that the request submission was successful.

Next, the OpenText DAST tester who monitors and responds to scan requests runs the scan during the hours you specified, and then uploads the results to Fortify Software Security Center.

5. If you are a Fortify Software Security Center Administrator or Application Security Tester, you can run the requested dynamic scan immediately from Fortify WebInspect Enterprise.

See also

["Viewing OpenText DAST analysis results in Fortify Software Security Center" on page 307](#)

["Processing dynamic scan requests from Fortify WebInspect Enterprise" below](#)

Processing dynamic scan requests from Fortify WebInspect Enterprise

If you are in the role of Administrator or Application Security Tester, you can start Fortify WebInspect Enterprise, where you can view and process dynamic scan requests submitted by Fortify Software Security Center users.

To process dynamic scan requests in Fortify WebInspect Enterprise:

1. From Fortify WebInspect Enterprise, initialize Fortify Software Security Center, and then use the WebInspect Enterprise Console to synchronize Fortify Software Security Center application versions with WebInspect projects (see the *OpenText™ Fortify WebInspect Enterprise User Guide*).
2. From the Fortify Software Security Center **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 Fortify Software Security Center to Fortify WebInspect Enterprise.

5. Select the pending request.
6. In the lower pane, on the **Details** tab, from the **Status** list, select **In Progress**, and then click **Change Status**. In Fortify Software Security Center, users assigned to the application version can now see that the scan request is no longer pending.
7. At the top of the view, click **Create a Web Site Scan** and complete the steps in the Scan Wizard to run the scan and upload the results to Fortify Software Security Center. For detailed instructions, see the *OpenText™ Fortify WebInspect Enterprise User Guide*.

See also

["Submitting dynamic scan requests to Fortify WebInspect Enterprise" on page 310](#)

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**.

Fortify Software Security Center displays the date and time the scan request was submitted, and request status information.

Dynamic scan request states

After you submit a dynamic scan request, (see ["Submitting dynamic scan requests to Fortify WebInspect Enterprise" on page 310](#)) 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**.
Fortify Software Security Center prompts you to confirm that you want to cancel the last dynamic scan request.
3. Click **Yes**.

Viewing open source data

After you download, install, and enable the OpenText Core SCA or Sonatype parser plugin for Fortify Software Security Center, 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 Core 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" on page 282](#).

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 screenshot shows a table with the following data:

| org.apache.struts/struts2-core | | CVE-2018-11776 | | 2.5.10 | Critical | maven | No Source License |
|--------------------------------|-------------------------|---------------------|---------------------------------|--------|---|--------------------------|-------------------|
| File Name | struts2-core-2.5.10.jar | Category | Vulnerable OSS : CVE-2018-11776 | | Analysis | Not Set | |
| Priority | Critical | CVE | CVE-2018-11776 | | Comments | Add a comment | |
| Evidence | View | CWE | CWE-20 | | Suppress | <input type="checkbox"/> | |
| Invoked | Yes | Controllable | Yes | | <input type="button" value="CANCEL"/> <input type="button" value="SAVE"/> | | |

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" on page 288. |
| 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 Core 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 OpenText Core SCA \(Debricked\) results" on page 152](#)

["Preparing to display Sonatype results" on page 153](#)

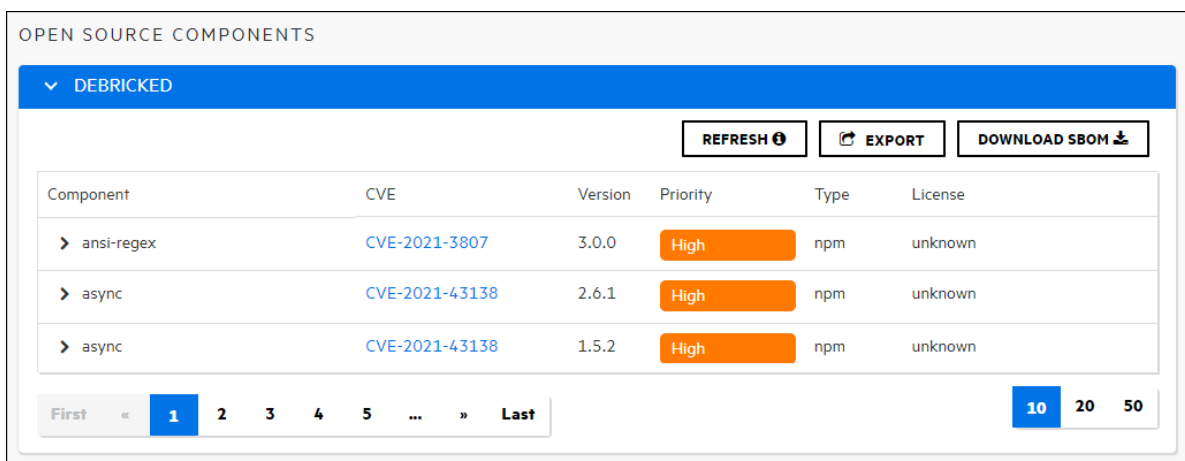
Downloading an OpenText Core SCA (Debricked) software bill of materials

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.



| OPEN SOURCE COMPONENTS | | | | | |
|------------------------|--------------------------------|---------|----------|------|---------|
| ▼ DEBRICKED | | | | | |
| | | | | | |
| | | | | | |
| Component | CVE | Version | Priority | Type | License |
| ansi-regex | CVE-2021-3807 | 3.0.0 | High | npm | unknown |
| async | CVE-2021-43138 | 2.6.1 | High | npm | unknown |
| async | CVE-2021-43138 | 1.5.2 | High | npm | unknown |

5. Click **Download SBOM**.
6. Open the downloaded JSON file in a text editor to view the SBOM.

Chapter 16: Working with OpenText ScanCentral DAST

If Fortify Software Security Center is configured to communicate with OpenText ScanCentral DAST to request and manage dynamic scans, then the **DAST** tab in the **ScanCentral** view includes the **Scans**, **Sensors**, **Sensor Pools**, **Settings List**, and **Scan Schedules** pages. For information about how to configure the connection between Fortify Software Security Center and OpenText ScanCentral DAST, see ["Enabling the running and management of OpenText ScanCentral DAST scans" on page 119](#).

This section contains the following topics:

| | |
|--|---------------------|
| OpenText ScanCentral DAST permissions | 316 |
| Submitting requests for dynamic scans to OpenText ScanCentral DAST | 317 |
| Synchronizing audit history changes in OpenText ScanCentral DAST using Kafka | 318 |

OpenText ScanCentral DAST permissions

The following table shows which Fortify Software Security Center roles have permission to perform which OpenText ScanCentral DAST-related tasks.

| Role | Permissions |
|---------------|---|
| View-Only | <ul style="list-style-type: none">View OpenText ScanCentral DAST data, except for jobs not assigned to any application version <p>Restrictions:</p> <ul style="list-style-type: none">Users see only the scans for application to which they are assignedUsers see only sensor pool assignment for the applications to which they are assigned |
| Security Lead | <ul style="list-style-type: none">View OpenText ScanCentral DAST dataCreate, run, change, and delete scans, schedules, and settingsManage pools and sensorsDownload artifactsRun scans from existing templates and base settingsManage deny intervals, application priority level, and retention policyManage global restrictions, restricted scan settings, and private data |

| | |
|-----------------------------|--|
| | <p>settings</p> <ul style="list-style-type: none">• Manage key stores and artifacts repositories <p>Restrictions:</p> <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• View OpenText ScanCentral DAST data• Manage pools and sensors <p>Restrictions:</p> <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• View OpenText ScanCentral DAST data• Run scans from existing templates and base settings• Download artifacts |
| Application Security Tester | <ul style="list-style-type: none">• View OpenText 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 permissions for Fortify Software Security Center roles" on page 156](#)

Submitting requests for dynamic scans to OpenText ScanCentral DAST

If Fortify Software Security Center is integrated with OpenText ScanCentral DAST, and you are assigned to one of the following roles, you can request dynamic scans from Fortify Software Security Center:

- Administrator
- Application Security Tester
- Security Lead
- Developer

For information about how to configure OpenText ScanCentral DAST scans and work with scans, sensors, sensor pools, settings, and scan schedules, see the *OpenText™ ScanCentral DAST Configuration and Usage Guide*.

See also

["Enabling the running and management of OpenText ScanCentral DAST scans" on page 119](#)

["OpenText ScanCentral DAST permissions" on page 316](#)

Synchronizing audit history changes in OpenText ScanCentral DAST using Kafka

Issues in Fortify Software Security Center that are managed in the **AUDIT** page and published to OpenText ScanCentral DAST are referred to as Findings.

Configure Kafka in Fortify Software Security Center to synchronize audit history changes for suppressed issues, priority override, and analysis tag settings to OpenText ScanCentral DAST. For more information on how to set up Kafka in Fortify Software Security Center, see ["Configuring a Kafka Stream to use with OpenText ScanCentral DAST" on page 120](#).

When you audit an issue in Fortify Software Security Center, a background process requests the audits to be published to the Kafka topic. OpenText ScanCentral DAST processes the audits and reflects any suppressed issues, priority override, and analysis tag settings in the Scans view and scan visualization.

Chapter 17: Working with Fortify ScanCentral SAST

If Fortify Software Security Center is configured to communicate with Fortify ScanCentral SAST, then the **SAST** tab is enabled in the **ScanCentral** view. The **SAST** tab displays the **Scan Requests**, **Sensors**, **Controller**, and **Sensor Pools** pages. For information about how to configure the connection between Fortify Software Security Center and Fortify ScanCentral SAST, see ["Enabling integration with Fortify ScanCentral SAST" on page 122](#).

This section contains the following topics:

| | |
|---|-----|
| Fortify ScanCentral SAST permissions | 319 |
| Viewing Fortify ScanCentral SAST scan request details | 320 |
| Prioritizing a Fortify ScanCentral SAST scan request | 321 |
| Canceling Fortify ScanCentral SAST scan requests | 322 |
| Viewing Fortify ScanCentral SAST sensor information | 322 |
| Viewing Fortify ScanCentral SAST Controller information | 323 |
| About Fortify ScanCentral SAST sensor pools | 325 |

Fortify ScanCentral SAST permissions

The following table shows which Fortify Software Security Center roles have permission to perform which Fortify ScanCentral SAST-related tasks.

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

| Roles | Permissions |
|-----------|--|
| View-Only | <ul style="list-style-type: none">View Fortify ScanCentral SAST data, except for jobs not assigned to any application version. <p>Restrictions:</p> <ul style="list-style-type: none">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 | <ul style="list-style-type: none">• View, download, and manage Fortify ScanCentral SAST data• Perform all tasks that involve changes to sensor pools• Cancel scan requests• Assign sensors and application versions to sensor pools <p>Restrictions:</p> <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• View, download, and manage Fortify ScanCentral SAST data, except for jobs not assigned to any application version <p>Restrictions:</p> <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• View Fortify ScanCentral SAST data, except for jobs not assigned to any application version |

See also

["Viewing permissions for Fortify Software Security Center roles" on page 156](#)



Viewing Fortify ScanCentral SAST scan request details

For information about how to install, configure, and use 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.

- (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.
To clear any applied filtering, click **RESET**.
- (Optional) To modify the display such as clearing sorting, or selecting the columns to display, click the **Display options** button .
- To expand a row and see more details about a scan, click the **Show scan details** button .



Header: Pending | c58... | 3 | HelloWo... | Default ... | 24.4.0.0... | 12/15/2... | Os | Os | **PRIORITIZE SCAN** ↑

Submitter IP address: 129.231.223.93

Scan arguments: -scan

Sensor Detail

UUID: 24.4.0.0063

SCA version: 24.4.0.0063

Sensor IP address: 24.4.0.0063

Sensors JVM: 24.4.0.0063

Pool: Default Pool

CANCEL SCAN | **EXPORT** ▼

- 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.
- To update the data displayed, click **REFRESH**.

See also

["Prioritizing a Fortify ScanCentral SAST scan request" below](#)

["Canceling Fortify ScanCentral SAST scan requests" on the next page](#)

["Viewing Fortify ScanCentral SAST sensor information" on the next page](#)

["Viewing Fortify ScanCentral SAST Controller information" on page 323](#)

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:

- On the header, select **ScanCentral**, and then select **SAST**.
- 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.
- Click **PRIORITIZE SCAN** in the row for the scan you want to run first.

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**.

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**.

| Filter by All States ▼ | Filter by All Pools ▼ | Search by hostname | FIND | | | | |
|---|--|--------------------|-------------|---------------------------|--------------|-----------------------|-----------------------|
| <div><div>● Active</div><div>● Stale</div><div>● Shutdown scheduled</div><div>● Inactive</div></div> | <table><thead><tr><th>Last Controller Contact ↕</th><th>Start Time ↕</th></tr></thead><tbody><tr><td>12/16/2024 2:08:35 PM</td><td>12/15/2024 7:38:49 PM</td></tr></tbody></table> | | | Last Controller Contact ↕ | Start Time ↕ | 12/16/2024 2:08:35 PM | 12/15/2024 7:38:49 PM |
| Last Controller Contact ↕ | Start Time ↕ | | | | | | |
| 12/16/2024 2:08:35 PM | 12/15/2024 7:38:49 PM | | | | | | |

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 Fortify ScanCentral SAST scan requests" above](#)

["Viewing Fortify ScanCentral SAST scan request details" on page 320](#)

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 Fortify ScanCentral SAST scan request details" on page 320](#)

["Canceling Fortify ScanCentral SAST scan requests" on the previous page](#)

["Viewing Fortify ScanCentral SAST sensor information" on the previous page](#)

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
```

2. 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" below](#)

Placing the Controller in maintenance mode

An abrupt shutdown of the 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 Fortify Software Security Center and, if any sensors are running scans, the Controller mode changes from **ACTIVE** to **WAITING_FOR_JOB_COMPLETED**. If no job is being processed, the mode changes directly from **ACTIVE** to **MAINTENANCE**. At this point, you can safely shut down the Controller.

Safely shutting down 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" on the previous page](#)), you cannot shut down sensors from the Fortify Software Security Center 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**.

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" on page 323](#)

["Stopping the Controller" on page 323](#)

About Fortify ScanCentral SAST sensor pools

If your Fortify Software Security Center server is integrated with Fortify ScanCentral SAST, and you are an Administrator, Manager, or Security Lead, you can create groups of sensors, or *sensor pools* based on any criteria, which you can then target for scan requests.

Sensor pools give you more control over 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 Fortify Software Security Center for available sensor pools. If the scan request is not associated with an application version, 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

Fortify Software Security Center provides two pre-defined sensor pools: the *unassigned sensor pool* and the *default pool*. The unassigned sensor pool, which contains all newly-registered sensors, serves as a shared sensor pool for other pools. If 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 Fortify ScanCentral SAST sensor pools" on the next page](#)

["Fortify ScanCentral SAST permissions" on page 319](#)

["Deleting Fortify ScanCentral SAST sensor pools" on page 328](#)

Creating Fortify ScanCentral SAST sensor pools

If your Fortify Software Security Center server is integrated with 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 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, Fortify Software Security Center is not connected to the Controller. Check your Fortify ScanCentral SAST configuration (see ["Enabling integration with Fortify ScanCentral SAST" on page 122](#)).

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.

The screenshot shows the 'Sensors' section of the Fortify ScanCentral SAST interface. On the left, there is a search box labeled 'Search by hostname' with a magnifying glass icon and a 'FIND' button. Below the search box, a list of sensors is displayed. The first sensor, 'sc-s15-wrk61', is selected, indicated by a blue checkmark and a red lock icon. To the right of the sensor list, the 'Sensor information' panel is visible, showing the following details:

| Sensor information | |
|--------------------|--------------|
| Sensor state | Active |
| Assigned to | DOTNET |
| Hostname | sc-s15-wrk61 |
| IP address | 10.94.154.31 |
| Total memory | 7.9 GB |
| SCA version | 25.2.0.0040 |

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:
 - a. Under **Versions**, click **ADD**.
 - b. 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.
 - c. To list any inactive versions of the selected application, select the **Show inactive** check box.
 - d. To assign all of the listed versions to the new pool, select the **Select all** check box. Otherwise, to assign only a subset of the application versions, select the check boxes next to the version names.
The **SELECTED VERSIONS** pane lists your selections.
 - e. To assign versions of another application to this pool, repeat steps b through d.
 - f. To remove an application version from the **SELECTED VERSIONS** list, click the **Delete** button  next to its name.
 - g. Click **DONE**.
10. In the **CREATE NEW POOL** dialog box, click **SAVE**.
The **Sensor Pools** table now lists your new pool.

You can edit or delete the pool at any time.

See also

["Deleting Fortify ScanCentral SAST sensor pools" on the next page](#)

["Viewing Fortify ScanCentral SAST sensor information" on page 322](#)

Moving sensors between pools

To move 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 Fortify ScanCentral SAST sensor pools" on page 326](#) to assign the now unassigned sensors.


See also


["About Fortify ScanCentral SAST sensor pools" on page 325](#)

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.

3. Click the **Delete Pool** button  that corresponds to the pool you want to delete.

Fortify Software Security Center removes the pool from the list and adds all sensors assigned to the deleted pool to the **Unassigned Sensors** tab.

See also

["Viewing Fortify ScanCentral SAST sensor information" on page 322](#)

["Creating Fortify ScanCentral SAST sensor pools" on page 326](#)

Chapter 18: BIRT reports

Fortify Software Security Center reports are based on the Business Intelligence and Reporting Technology (BIRT) system. BIRT is an open source reporting system based on Eclipse. For information about BIRT, 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 | 329 |
| Importing report libraries | 330 |
| Generating and downloading reports | 330 |
| Generating and downloading customized BIRT reports in XLSX | 332 |
| Customizing BIRT reports | 333 |
| Acquiring the BIRT Report Designer | 333 |
| Downloading report templates | 333 |
| Importing report definitions | 334 |

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" on page 333](#).

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.

Importing report libraries

An Administrator can add report libraries to the Fortify Software Security Center 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 Fortify Software Security Center" on page 156](#)

["Generating and downloading reports" below](#)

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:
 - a. Under **Application version**, click **BROWSE**.
 - b. 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.

SELECT APPLICATION VERSION [X]

APPLICATION

Q log [X] **FIND**

Logistics

VERSIONS ☐ Show inactive

Q Filter versions **FIND**

☐ 1.3

☐ 2.5


CANCEL **DONE**

The active versions of the selected application are listed under **VERSIONS**.

- c. Select the check box for the version to include in the report. (You can select only one.)
For Portfolio Reports, you can select multiple application versions to include in the report.
 - d. 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**.

Fortify Software Security Center 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 attributes" on page 123](#).

See also

["Generating and downloading customized BIRT reports in XLSX" on the next page](#)

["Downloading report templates" on page 333](#)

["Importing report definitions" on page 334](#)

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 <code>enableXlsxGeneration</code> 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**.

Fortify Software Security Center 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 .

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 Fortify Software Security Center 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" below](#).
2. Load a Fortify Software Security Center report definition into Report Designer.
You typically first export a report definition from Fortify Software Security Center, and then upload that report definition into Report Designer. For information about how to export a Fortify Software Security Center report definition, see ["Downloading report templates" below](#).
3. Connect Report Designer to a running instance of the Fortify Software Security Center database.
Connecting Report Designer to the Fortify Software Security Center database enables you to load and verify the database queries you add to a BIRT report.
4. Use the Report Designer to add report design elements to the report definition, and add database queries to those design elements.
5. Use a local instance of Fortify Software Security Center to test the operation of a customized BIRT report.
6. Import the customized report definition into Fortify Software Security Center.

See also

["Importing report definitions" on the next page](#)

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 ["BIRT report requirements" on page 38](#).

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.

Downloading report templates

You can download a Fortify Software Security Center 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 Fortify Software Security Center 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 Fortify Software Security Center. 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 Fortify Software Security Center, see ["Importing report definitions" below](#).

See also

["Generating and downloading reports" on page 330](#)

Importing report definitions

A BIRT report definition provides the Fortify Software Security Center report engine the information it needs to generate a report. This includes information such as the report name, report parameters, and the name of the report template file.

BIRT enables you to import report definitions files to Fortify Software Security Center. To do this, you need a Fortify Software Security Center BIRT definition 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 Fortify Software Security Center.

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 Fortify Software Security Center BIRT definition file (with the .rptdesign extension). |

5. (Optional) Add one or more parameters to the report definition, as follows:
- Click **ADD PARAMETER**.
 - 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. |

- Click **APPLY**.
- Click **SAVE**.

See also

["Generating and downloading reports" on page 330](#)

Chapter 19: Authentication tokens

Authentication tokens are unique keys that allow users to automate actions in Fortify Software Security Center, 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, Fortify Software Security Center logs the operation under the account name used to create the token.

This section contains the following topics:

| | |
|--|-----|
| Authentication token types | 336 |
| Generating authentication tokens | 338 |
| Editing authentication tokens | 339 |
| Deleting authentication tokens | 339 |

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 Fortify Software Security Center 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 |

| Token type | Description |
|--------------------------|---|
| | <p>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.</p> |
| CIToken | Allows integration of Fortify Software Security Center 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 | <p>Enables users to:</p> <ul style="list-style-type: none"> • 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 Fortify ScanCentral SAST client. |
| ToolsConnectToken | For use with OpenText Application Security Tools (Fortify Audit Workbench and Secure Code Plugins) that connect to Fortify Software Security Center for collaborative auditing, remediation, and uploading of analysis results. |
| UnifiedLoginToken | Gives access to most of the REST API. It is intended for short-run automations that last less than a day. |

Generating authentication tokens

You can generate authentication tokens from either the **Administration** view in Fortify Software Security Center, or from the command line using the `fortifyclient` utility. Only you can see the details of your tokens. A Fortify Software Security Center Administrator can extend the life of a token you create, but not beyond the maximum days to live for that token.

Note: 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" on page 336](#).

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.

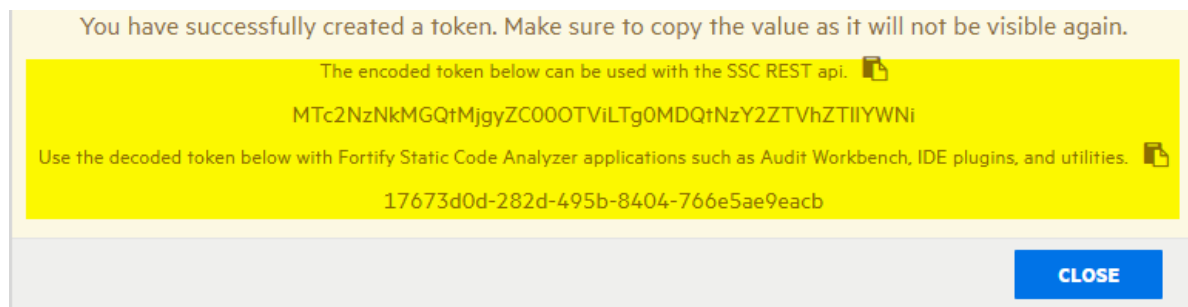
The expiration time is set to the current time on the specified date. By default, the expiration date value is set to the maximum number of days to live for the selected token type. You can set this to an earlier date to give the token a shorter life.

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" on page 341](#)

["Specifying the number of days before a token expires" on page 342](#)

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" on the previous page](#)

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" on the previous page](#)

Appendix A: Using the fortifyclient utility

You can use the fortifyclient utility to generate authentication tokens, securely transfer objects to and from Fortify Software Security Center, and purge application version artifacts from the command line.

This section contains the following topics:

| | |
|--|-----|
| Preparing to use fortifyclient | 340 |
| Listing fortifyclient commands and options | 341 |
| Generating an authentication token from the command line | 341 |
| Listing authentication tokens | 342 |
| Invalidating tokens | 343 |
| Listing application versions | 343 |
| Uploading FPR files | 344 |
| Downloading FPR files | 344 |
| Purging application version artifacts | 345 |
| Importing content bundles | 345 |
| Downloading audit attachment files | 345 |

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 Fortify Software Security Center URL. See “host.url” in ["Application configuration options" on page 360](#).
- The commands to generate tokens and list existing tokens require the credentials for a Fortify Software Security Center 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, Fortify Software Security Center logs the operation under the account name used to create the token.

See also

Unpacking and deploying Fortify Software Security Center software

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 | <p>Specifies the HTTP connection timeout in seconds in which the client should establish a connection.</p> <p>The default value is 10 seconds.</p> |
| FORTIFYCLIENT_READ_TIMEOUT_SEC | <p>Specifies the HTTP read timeout in seconds in which the client should receive a response.</p> <p>The default value is 600 seconds.</p> |
| FORTIFYCLIENT_WRITE_TIMEOUT_SEC | <p>Specifies the HTTP write timeout in seconds in which the client should deliver a request body.</p> <p>The default value is 60 seconds.</p> |

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.

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 Fortify Software Security Center 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 Fortify Software Security Center:

```
fortifyclient token -url <host.url> -gettoken AnalysisUploadToken -user  
Developer1 -password <password>
```

See also

["Authentication token types" on page 336](#)

["Generating authentication tokens" on page 338](#)

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" on the previous page](#)

Listing authentication tokens

Fortify Software Security Center administrators can use `fortifyclient` to list all existing authentication tokens for all Fortify Software Security Center user accounts. The `fortifyclient` utility does not support filtering the list of tokens by Fortify Software Security Center account name or account privilege level.

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 Fortify Software Security Center created automatically.

Invalidating tokens

You can invalidate an existing authentication token by deleting it from the Fortify Software Security Center 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" on the previous page](#)

["Deleting authentication tokens" on page 339](#)

Listing application versions

You can use `fortifyclient` to list the Fortify Software Security Center application versions accessible by the account that was used to create a particular 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" on page 341.](#))

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" on page 341](#)

Uploading FPR files

Users periodically upload application analysis results files (in FPR format) to Fortify Software Security Center. 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.

Examples

Upload an FPR file to Fortify Software Security Center using an application version identifier:

```
fortifyclient uploadFPR -url <host.url> -authtoken <token> -file MyScan.fpr -  
applicationVersionID <id>
```

Upload an FPR file to Fortify Software Security Center 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" on page 341](#)

["Listing application versions" on the previous page](#)

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 Fortify Software Security Center using an application version identifier:

```
fortifyclient downloadFPR -url <host.url> -authtoken <token> -file MyScan.fpr -  
applicationVersionID <id>
```

Download an FPR file from Fortify Software Security Center 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" on page 341](#)

["Listing application versions" on the previous page](#)

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 May 28, 2025:

```
fortifyclient purgeApplicationVersion -url <host.url> -authtoken <token> -  
application MyApp -applicationVersion 1.0 -scanDate 05282025
```

You can also specify the application version using an application version identifier.

See also

["Generating an authentication token from the command line" on page 341](#)

["Listing application versions" on page 343](#)

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 Fortify Software Security Center:

```
fortifyclient import -url <host.url> -authtoken <token> -bundle bundle.zip
```

Downloading audit attachment files

The following example command downloads an audit attachment file from Fortify Software Security Center:

```
fortifyclient downloadAttachment -url <host.url> -authtoken <token> -file  
xyz.png -attachmentId <attachment_id>
```

Appendix B: Authoring bug tracker plugins

Fortify Software Security Center 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 ["Supported service integrations" on page 38](#). 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 guide and in the Fortify Software Security Center 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 | 346 |
| Component setup | 347 |
| Implementation | 347 |
| Plugin methods and method calls | 348 |
| Plugin helper | 353 |
| Error handling | 353 |
| Almost stateless | 354 |
| Debugging a bug tracker plugin | 354 |
| Deploying a customized bug tracker plugin | 354 |

Use case

As a Fortify Software Security Center Administrator, you can configure an external bug tracking system to use with a given application version, as described in ["About bug tracking system integration" on page 148](#). Fortify Software Security Center displays the required configuration parameter fields for the bug tracker you select, and you set the values for these just one time for the application version. After you test the bug tracker configuration parameter values for validity (optional), you save them to the database for use whenever a user logs a defect for the application version.

A user who submits a bug against an application version logs on to the bug tracker, and then completes the required fields that the bug tracker supplies for the bug parameters. Required

parameter information can include such items as summary, description, severity level, component, and so on.

The plugin framework supports a dynamic aspect to bug-tracking parameters. Whenever a user changes a parameter value, the plugin detects the change and an updated list of bug parameters with new list selections becomes available.

When a bug is filed, the bug ID is saved in the database against the issue. The user can then 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.

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.

Implementation

Fortify Software Security Center 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, UserAuthenticationStore credentials);
    public String getBugDeepLink(String bugId);
}

```

Plugin methods and method calls

The following table lists the methods and calls to use with your plugin.

| Method or call | Description |
|------------------------|---|
| requiresAuthentication | <p>This method is expected to return true if it requires the framework to request credentials from the user for any bug-tracking operation.</p> <p>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</p> |

| Method or call | Description |
|---------------------------------------|---|
| | false, the system passes null for all the <code>UserAuthenticationStore</code> parameters of the plugin methods. |
| <code>getBatchBugParameters</code> | 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 <code>BugTrackerPlugin.setConfiguration (java.util.Map)</code> 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. |
| <code>getConfiguration</code> | 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 <code>BugTrackerConfig</code> 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. |
| <code>setConfiguration (call)</code> | 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 <code>setConfiguration</code> call, which sets the configuration for the plugin using which operations are to be carried out. |
| <code>testConfiguration (call)</code> | The plugin framework uses the <code>testConfiguration</code> call to test the configuration previously set using the <code>setConfiguration</code> call. This method is expected to hit the bug-tracking system using the configuration details set and validate them to the fullest extent possible. The user credentials are fetched from the user if this plugin declared that it requires authentication. |
| <code>getShortDisplayName</code> | <p>The <code>getShortDisplayName</code> method returns a short display name for the plugin. This string populates the list of available bug tracker plugins.</p> <p>Important! If you customize the sample bug-trackers code that Fortify Software Security Center provides, but you use</p> |

| Method or call | Description |
|---------------------------|---|
| | <p>the same plugin classname, do not change the short display name of the plugin. (For consistency, also avoid changing the long display name.) If you <i>do</i> change the name of the main implementation class, then you must also change the display name(s) for the plugin.</p> |
| getLongDisplayName | <p>The <code>getLongDisplayName</code> 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.</p> <p>Important! If you customize the sample bug-trackers code that Fortify Software Security Center provides, but you use the same plugin classname, do not change the short display name of the plugin. (For consistency, also avoid changing the long display name.) If you <i>do</i> change the name of the main implementation class, then you must also change the display name(s) for the plugin.</p> |
| getBugParameters | <p>The <code>getBugParameters</code> method returns metadata about the bug parameters to present to users. Fortify Software Security Center supports the following three bug parameter types:</p> <ul style="list-style-type: none"> • <code>BugParamText</code> translates to a text box. • <code>BugParamTextArea</code> translates to a multiple-line text box and is typically used for bug descriptions. • <code>BugParamChoice</code> translates to a list. • The <code>issueDetail</code> 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 <code>pluginHelper</code> protected member has a helper method to build a suggested default bug description. (See "Plugin helper" on page 353.) |
| onBatchBugParameterChange | <p>If a user changes the value of a parameter in the user interface, this method fetches the updated choice list for other batch bug</p> |

| Method or call | Description |
|-------------------|--|
| | <p>parameters. The <code>BugTrackerPlugin.setConfiguration</code> (<code>Map</code>) method is called on the plugin instance before this method is invoked. If the</p> <p><code>BugParamChoice.getHasDependentParams()</code> attribute for a plugin bug parameter is set to <code>true</code>, then this method is called whenever the parameter value changes in the user interface layer.</p> <p>Recommendations:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Modify the <code>currentValues</code> parameter and return it. • Construct the return value from the raw parameters maintained. Set the values and choice lists before returning. |
| onParameterChange | <p>The plugin framework calls the <code>onParameterChange</code> method whenever the value for a bug parameter marked as <code>hasDependentParams</code> (see <code>BugParamChoice</code> class javadoc) changes. This method can take action and return a new list of bug parameters to display.</p> <p>Keep the following guidelines in mind:</p> <ul style="list-style-type: none"> • 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 |

| Method or call | Description |
|--------------------------------|--|
| | <p>ensure that it does not already include the parameter.</p> <ul style="list-style-type: none"> • Return null if there is no change. • Use one of the following strategies: <ul style="list-style-type: none"> • Modify the <code>currentValues</code> parameter and return it. • Construct the return value from raw parameters maintained. Set values and choice lists before returning. |
| <code>fileBug</code> | <p>This method files a bug on the external bug-tracking system. The <code>BugSubmission</code> object passed encompasses all bug details.</p> <p>Ensure that you correctly differentiate between the <code>bug.getIssueDetail()</code> object and the <code>bug.getParams()</code> object. The <code>bug.getIssueDetail()</code> object returns details of the issue, whereas the <code>bug.getParams()</code> object returns the bug parameter values that the user provides.</p> <p>If you added Bug Description as a user-editable bug parameter, then fetch the bug description from the <code>bug.getParams()</code> object instead of from the <code>bug.getIssueDetail()</code> object. The return value of the <code>fileBug</code> object must be a <code>bugId</code>, which can be used to fetch the bug with the <code>fetchBug</code> method and formulate the deep link with the <code>getBugDeepLink</code> method.</p> <p>Use fields in <code>BugSubmission.getIssueDetail()</code>, namely <code>getLastBuildWithoutIssue()</code>, <code>getDetectedInBuild()</code>, and <code>getFileName()</code> to perform changeset discovery if you have access to your repository.</p> |
| <code>fileMultiIssueBug</code> | <p>File bugs that contain multiple issues on the bug tracking system. The <code>BugTrackerPlugin.setConfiguration(Map)</code> method is called on the plugin instance before this method is invoked.</p> <p>Recommendations:</p> <ul style="list-style-type: none"> • Fortify Software Security Center provides the summary and description obtained using <code>MultiIssueBugSubmission.getIssueDetails()</code>. The user does not supply these values. If you added the summary |

| Method or call | Description |
|-----------------------------|---|
| | <p>and description as bug parameters, use <code>bug.getParams()</code> to retrieve the user-supplied values.</p> <ul style="list-style-type: none">• If you have access to your repository, use the <code>getLastBuildWithoutIssue()</code>, <code>getDetectedInBuild()</code>, and <code>getFileName()</code> fields in <code>MultiIssueBugSubmission.getIssueDetails()</code> to perform changeset discovery. |
| <code>fetchBug</code> | This method fetches the current bug status. |
| <code>getBugDeepLink</code> | 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.

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.

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.

Almost stateless

With every top-level request that Fortify Software Security Center sends to the plugin framework bug tracker (and that needs to communicate with the bug tracker provider), the `setConfiguration` call is made. The only states that should be saved within the plugin are the configuration values that this method provides. The configuration values can be used during bug tracker plugin internal processing. From this point on, all plugin calls are expected to be stateless.

Plugin instances must not maintain any state, leave open connections, or try to use connections opened in the previous call. Fortify Software Security Center does not cache or reuse plugin instances across plugin operations. New states must be opened on each call and cleaned up before method exit.

Debugging a bug tracker plugin

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.

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 Fortify Software Security Center, 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" on page 346](#)

Chapter C: Advanced configuration

This section covers advanced configuration topics for Administrators.

This section contains the following topics:

| | |
|---|-----|
| Automating Fortify Software Security Center configuration | 356 |
| Application configuration options | 360 |

Automating Fortify Software Security Center configuration

You can automate Fortify Software Security Center configuration before deployment using the autoconfig file. This file includes sections for each configurable aspect of Fortify Software Security Center. The autoconfig file enables automated deployment by providing settings and seed bundles for silent Fortify Software Security Center update and installation. You can use the autoconfig file to automate all Setup wizard tasks. The Setup wizard picks 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 Fortify Software Security Center instance from one computer to another, you must also move the `secret.key` file (not just your properties file).

To automate Fortify Software Security Center configuration:

Important! To automate the configuration in a root context, see ["Automating configuration in a root context" on page 358](#).

1. Open a text editor and create a file named `<app_context>.autoconfig`, where `<app_context>` is the application server context in which Fortify Software Security Center is deployed (the name of the directory created under `<fortify.home>`).
2. Add the following to the `<app_context>.autoconfig` file in the YAML format shown.

Note: 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.

```
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

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

  # SQL Server database
  # jdbc.url: 'jdbc:sqlserver://mssql-host:1433;database=ssc_
  db;sendStringParametersAsUnicode=false'
  # SQL 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, Fortify Software Security Center computes the effective configuration checksum and saves it in the `version.properties` file as the value for the `autoconfig.checksum` property.

When Fortify Software Security Center starts with the `autoconfig` file present, it computes an effective configuration checksum and compares it to the checksum stored in the `version.properties` file. If the checksums do not match, Fortify Software Security Center runs a lightweight auto-configuration, and updates the `autoconfig.checksum` value.

If the auto-configuration fails for any reason, Fortify Software Security Center 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.

Fortify Software Security Center performs the complete automatic configuration only if it is not fully configured. Fortify Software Security Center performs lightweight auto-configuration only if the checksums do not match but it is otherwise already configured.

Lightweight auto-configuration skips database migration (regardless of 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.

Automating configuration in a root context

To automate Fortify Software Security Center 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: Copy only the database properties for the database engine you use, and ensure that you remove the hash symbol (`#`) before each property.

```
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

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'
```

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 Fortify Software Security Center configuration" on page 356](#)

Application configuration options

Administrators can update Fortify Software Security Center configuration settings in the `<fortify.home>/<app_context>/conf/app.properties` file or the `appProperties` section of an autoconfig file used to automate the Fortify Software Security Center configuration.

| Property name | Description |
|---|---|
| Fortify Software Security Center URL | |
| <code>host.url</code> | Specifies the web address for accessing Fortify Software Security Center ("Automating Fortify Software Security Center configuration" on page 356) |
| <code>host.validation</code> | If set to <code>true</code> , enables HTTP host validation against the <code>host.url</code> value ("Automating Fortify Software Security Center configuration" on page 356). The default is <code>false</code> . |
| Global search | |
| <code>searchIndex.location</code> | Specifies the absolute path to the full text index directory on local file system ("Automating Fortify Software Security Center configuration" on page 356) |
| Background job execution | |
| <code>jobs.threadCount</code> | Specifies the size of the job processing thread pool ("Partitioning an Oracle database for improved performance" on page 57). The default value is 10. |
| <code>job.exclusiveJobOverheadPercentage</code> | Specifies a percentage by which to reduce the <code>jobs.threadCount</code> 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. |
| <code>job.numberOfDedicatedDataExports</code> | Specifies the number of job processing threads reserved for data exports. The default value is 2. |

| Property name | Description |
|-------------------------------------|--|
| 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. |
| Passwords | |
| password.strength.min.score | Specifies the minimum acceptable strength score for saving a new password (" Setting the required password strength for Fortify Software Security Center sign in " on page 145). The default value is 3. |
| sso.localAuthenticationEnabled | If set to true, allows local password authentication for use with X.509 SSO (" About configuring Fortify Software Security Center to work with single sign-on " on page 136). The default is false. |
| LDAP cache | |
| ldap.cache.persistence.enabled | If set to true, Fortify Software Security Center stores the ldap cache in the database for faster startup (" Enabling persistence of the LDAP cache " on page 112). The default is true. |
| ldap.cache.refresh.interval.hours | Specifies the cache refresh interval (in hours) (" Enabling persistence of the LDAP cache " on page 112). 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 " on page 147). The default is false. |

Configuring background job execution strategy

The following table describes how to replicate the background job execution strategies that existed prior to Fortify Software Security Center version 25.2.0.

| Legacy job execution strategy | Description | Configuration instructions |
|-------------------------------|---|--|
| Conservative | Balances job concurrency, throughput, and job stability. | No changes required. |
| Aggressive | <p>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.</p> <p>OpenText does not recommend using this job execution strategy.</p> | <ul style="list-style-type: none"> Set <code>job.exclusiveJobOverheadPercentage</code> to 0. Set <code>job.numberOfConcurrentReports</code> to the same value as the <code>jobs.threadCount</code> value. OpenText recommends using a smaller value than the <code>jobs.threadCount</code> value or the default value of 2 to increase scan processing throughput and reduce peak memory that report generation can consume. Set <code>job.numberOfConcurrentExclusiveJobs</code> to the same value as the <code>jobs.threadCount</code> 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 | <p>Enables jobs to run in sequence and one at a time.</p> <p>OpenText does not recommend using this job execution strategy.</p> | <ul style="list-style-type: none"> Set <code>jobs.threadCount</code> to 1. Set <code>job.numberOfDedicatedDataExports</code> to 0. |

Appendix D: Webhook payloads

Every webhook payload contains the following fields:

- events—Webhook event list (information about events triggered)
- sscUrl—URL address of the server
- webhookId—Associated webhook ID
- triggeredAt—Date on which the payload was created in (created and stored in the database)

Example:

```
{
  "events": [
    {
      "event": "ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS",
      "artifactId": 1,
      "projectVersionId": 1,
      "filename": "file.fpr",
      "username": "testUser1"
    }
  ],
  "triggeredAt": "2020-08-21T12:19:24.502+0000",
  "sscUrl": "http://localhost:8180/ssc",
  "webhookId": 1
}
```

This section contains the following topics:

| | |
|---|-----|
| Event payloads | 364 |
| Artifact upload payload | 364 |
| Project version payload | 365 |
| Report generation payload | 367 |
| User payload | 368 |

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.

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": 1,
  "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"
}
```

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": "v1"
}
```

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
- **projectId**—(child) Application version ID
- **projectVersionName**—Application version name
- **previousProjectId**—ID of the (parent) application
- **previousProjectName**—Name of the (parent) application
- **previousProjectVersionId**—ID of the (parent) application version
- **previousProjectVersionName**—Name of the (parent) application version
- **event**—APP_VERSION_CREATED

Example:

```
{
  "event": "APP_VERSION_CREATED",
  "projectId": 1,
  "projectName": "Test application",
  "projectVersionId": 2,
  "projectVersionName": "v2",
  "previousProjectId": 1,
  "previousProjectName": "Test application",
  "previousProjectVersionId": 1,
  "previousProjectVersionName": "v1"
}
```

Report generation payload

Payloads generated for report events.

Fields:

- **reportId**—ID of the requested report
- **reportName**—Name specified for report generation
- **renderingEngine**—Report rendering engine
- **reportType**—Report type
- **event**—Type of the report generation event

Available values:

- REPORT_GENERATION_COMPLETE
- REPORT_GENERATION_REQUESTED

Example:

```
{
  "event": "REPORT_GENERATION_COMPLETE",
  "reportId": 1,
  "reportName": "Test report",
  "renderingEngine": "BIRT",
  "reportType": "PROJECT"
}
```

User payload

Payloads generated for user lifecycle events.

Fields:

- id—User id
- username—User's username
- event—User event
 - USER_CREATED - Authentication entity (LOCAL_USER, LOCAL_GROUP, LDAP_USER, LDAP_GROUP, or LDAP_ORGANIZATIONAL_UNIT) was created in Fortify Software Security Center.
 - USER_DELETED - Authentication entity (LOCAL_USER, LOCAL_GROUP, LDAP_USER, LDAP_GROUP, or LDAP_ORGANIZATIONAL_UNIT) was deleted from Fortify Software Security Center.
 - USER_UPDATED - Authentication entity (LOCAL_USER, LOCAL_GROUP, LDAP_USER, LDAP_GROUP, or LDAP_ORGANIZATIONAL_UNIT) was updated in Fortify Software Security Center.
 - LOCAL_USER_ACCOUNT_LOCKED
- userType—Type of user

Available types:

- LOCAL_USER
- LOCAL_GROUP
- LDAP_USER
- LDAP_GROUP
- LDAP_ORGANIZATIONAL_UNIT

Example:

```
{  
  "id":1,  
  "username":"testUser",  
  "event":"USER_CREATED",  
  "userType":"LOCAL_USER"  
}
```

Send documentation feedback

If you have comments about this document, you can [contact the documentation team](#) by email.

Note: If you are experiencing a technical issue with our product, do not email the documentation team. Instead, contact Customer Support at <https://www.microfocus.com/support> so they can assist you.

If an email client is configured on this computer, click the link above to contact the documentation team and an email window opens with the following information in the subject line:

Feedback on User Guide (Application Security 25.2.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to fortifydocteam@opentext.com.

We appreciate your feedback!