HPE Security
Fortify Software Security Center

Software Version: 17.20

User Guide

IMPORTANT NOTICE
Certain versions of documents (“Material”) accessible here may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company. As of September 1, 2017, the Material is now offered by Micro Focus, a separately owned and operated company. Any reference to the HP and Hewlett Packard Enterprise/HPE marks is historical in nature, and the HP and Hewlett Packard Enterprise/HPE marks are the property of their respective owners.

Document Release Date: November 2017
Software Release Date: November 2017
Legal Notices

Warranty
The only warranties for Seattle SpinCo, Inc. and its subsidiaries’ (“Seattle”) products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Seattle shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend
Confidential computer software. Except as specifically indicated, valid license from Seattle required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor’s standard commercial license.

Copyright Notice
© Copyright 2008 - 2017 EntIT Software LLC, a Micro Focus company

Trademark Notices
Adobe™ is a trademark of Adobe Systems Incorporated.
Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.
UNIX® is a registered trademark of The Open Group.

Documentation Updates
The title page of this document contains the following identifying information:
- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software
To check for recent updates or to verify that you are using the most recent edition of a document, go to:
You will receive updated or new editions if you subscribe to the appropriate product support service. Contact your Micro Focus sales representative for details.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>15</td>
</tr>
<tr>
<td>Contacting HPE Security Fortify Support</td>
<td>15</td>
</tr>
<tr>
<td>For More Information</td>
<td>15</td>
</tr>
<tr>
<td>About the Documentation Set</td>
<td>15</td>
</tr>
<tr>
<td>Change Log</td>
<td>16</td>
</tr>
<tr>
<td>Chapter 1: Introduction</td>
<td>21</td>
</tr>
<tr>
<td>Intended Audience</td>
<td>21</td>
</tr>
<tr>
<td>Document Structure</td>
<td>22</td>
</tr>
<tr>
<td>What's New in Fortify Software Security Center 17.20</td>
<td>22</td>
</tr>
<tr>
<td>New Setup Wizard Replaces the Configuration Wizard</td>
<td>22</td>
</tr>
<tr>
<td>New Path for Fortify Software Security Center Configuration and Resources</td>
<td>22</td>
</tr>
<tr>
<td>New Software Distribution Bundles</td>
<td>22</td>
</tr>
<tr>
<td>View Issues Based on the Dates They Were Introduced to Your Code</td>
<td>23</td>
</tr>
<tr>
<td>Selecting the Prediction Policy for Audit Assistant</td>
<td>23</td>
</tr>
<tr>
<td>New Plugin Framework</td>
<td>23</td>
</tr>
<tr>
<td>Exporting Data to Comma-Separated Values Files</td>
<td>24</td>
</tr>
<tr>
<td>Switching Between the New User Interface and the Legacy User Interface</td>
<td>24</td>
</tr>
<tr>
<td>Accessing Legacy Documentation</td>
<td>24</td>
</tr>
<tr>
<td>Disabling the Legacy User Interface</td>
<td>25</td>
</tr>
<tr>
<td>Viewing Fortify Software Security Center Keyboard Shortcuts</td>
<td>25</td>
</tr>
<tr>
<td>Disabling Keyboard Shortcuts (Hotkeys)</td>
<td>26</td>
</tr>
<tr>
<td>Related Documents</td>
<td>26</td>
</tr>
<tr>
<td>All Products</td>
<td>27</td>
</tr>
<tr>
<td>HPE Security Fortify CloudScan</td>
<td>27</td>
</tr>
<tr>
<td>HPE Security Fortify Software Security Center</td>
<td>28</td>
</tr>
<tr>
<td>HPE Security Fortify Static Code Analyzer</td>
<td>28</td>
</tr>
<tr>
<td>HPE Security Fortify WebInspect</td>
<td>31</td>
</tr>
<tr>
<td>HPE Security Fortify WebInspect Enterprise</td>
<td>32</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Accessing the Software Security Center API Documentation</td>
<td>33</td>
</tr>
<tr>
<td><strong>Part I: Fortify Software Security Center Deployment</strong></td>
<td>34</td>
</tr>
<tr>
<td>Chapter 2: Providing for Secure Deployment</td>
<td>35</td>
</tr>
<tr>
<td>Securing Access to Facilities</td>
<td>35</td>
</tr>
<tr>
<td>Securing the Application Server</td>
<td>35</td>
</tr>
<tr>
<td>Setting Application Server Attributes to Protect Sensitive Data in Cookies</td>
<td>35</td>
</tr>
<tr>
<td>About Using HTTPS and SSL Communications</td>
<td>36</td>
</tr>
<tr>
<td>Configuring Fortify Static Code Analyzer Tools to Communicate with Fortify Software Security Center Using HTTPS</td>
<td>36</td>
</tr>
<tr>
<td>Running Reports with WebSphere Application Server</td>
<td>37</td>
</tr>
<tr>
<td>About Securing Passwords and User Roles</td>
<td>37</td>
</tr>
<tr>
<td>Managing Computer Services and Accounts</td>
<td>38</td>
</tr>
<tr>
<td><strong>Chapter 3: Preparing for Fortify Software Security Center Deployment</strong></td>
<td>39</td>
</tr>
<tr>
<td>High-Level Deployment Tasks</td>
<td>39</td>
</tr>
<tr>
<td>Deployment Overview</td>
<td>41</td>
</tr>
<tr>
<td>The Fortify Software Security Center Installation Environment</td>
<td>41</td>
</tr>
<tr>
<td>Downloading Fortify Software Security Center Files</td>
<td>44</td>
</tr>
<tr>
<td>Unpacking and Deploying Fortify Software Security Center Software</td>
<td>44</td>
</tr>
<tr>
<td>About the Fortify Software Security Center Database</td>
<td>45</td>
</tr>
<tr>
<td>About JDBC Drivers</td>
<td>46</td>
</tr>
<tr>
<td>Adding the JDBC Driver to Fortify Software Security Center</td>
<td>46</td>
</tr>
<tr>
<td>About Fortify Software Security Center Database Character Set Support</td>
<td>47</td>
</tr>
<tr>
<td>Installing and Configuring the Database Server Software</td>
<td>47</td>
</tr>
<tr>
<td>Database User Account Privileges</td>
<td>47</td>
</tr>
<tr>
<td>Database-Specific Configuration Requirements</td>
<td>48</td>
</tr>
<tr>
<td>Configuring an IBM DB2 Database</td>
<td>48</td>
</tr>
<tr>
<td>Using a Microsoft SQL Server Database</td>
<td>49</td>
</tr>
<tr>
<td>Correcting a Case-Insensitive SQL Server Database Deployment</td>
<td>49</td>
</tr>
<tr>
<td>Configuring a MySQL Database</td>
<td>52</td>
</tr>
<tr>
<td>Correcting a Case-Insensitive MySQL Database Deployment</td>
<td>54</td>
</tr>
<tr>
<td>Configuring an Oracle Database</td>
<td>56</td>
</tr>
<tr>
<td>Preventing the “No more data to read from socket” Error</td>
<td>56</td>
</tr>
<tr>
<td>About the Fortify Software Security Center Database Tables and the Schema</td>
<td>56</td>
</tr>
<tr>
<td>About Seeding the Fortify Software Security Center Database</td>
<td>56</td>
</tr>
<tr>
<td>Permanently Deleting a Fortify Software Security Center Database</td>
<td>57</td>
</tr>
<tr>
<td>LDAP User Authentication</td>
<td>57</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>About Configuring a Proxy for Rulepack Updates</td>
<td>90</td>
</tr>
<tr>
<td>Configuring Email Alert Notification Settings</td>
<td>91</td>
</tr>
<tr>
<td>Setting the Strategy for Resolving Issue Audit Conflicts</td>
<td>92</td>
</tr>
<tr>
<td>Configuring Java Message Service Settings</td>
<td>93</td>
</tr>
<tr>
<td>Configuring LDAP Servers</td>
<td>94</td>
</tr>
<tr>
<td>Editing an LDAP Server Configuration</td>
<td>103</td>
</tr>
<tr>
<td>Importing an LDAP Server Configuration</td>
<td>103</td>
</tr>
<tr>
<td>Registering LDAP Entities</td>
<td>104</td>
</tr>
<tr>
<td>Refreshing LDAP Entities Manually</td>
<td>107</td>
</tr>
<tr>
<td>Deleting an LDAP Server Configuration</td>
<td>107</td>
</tr>
<tr>
<td>About the SAP NetWeaver Plugin for Fortify Software Security Center</td>
<td>108</td>
</tr>
<tr>
<td>Setting up the NetWeaver Plugin</td>
<td>108</td>
</tr>
<tr>
<td>Adding the SAP JCo Driver to Fortify Software Security Center</td>
<td>108</td>
</tr>
<tr>
<td>Connecting to SAP NetWeaver</td>
<td>109</td>
</tr>
<tr>
<td>Configuring Fortify Runtime Application Protection Communication Settings</td>
<td>110</td>
</tr>
<tr>
<td>Configuring Job Scheduler Settings</td>
<td>111</td>
</tr>
<tr>
<td>Setting Job Execution Priority</td>
<td>114</td>
</tr>
<tr>
<td>Canceling Scheduled Jobs</td>
<td>115</td>
</tr>
<tr>
<td>Configuring Browser Access Security for Fortify Software Security Center</td>
<td>115</td>
</tr>
<tr>
<td>Configuring Fortify Software Security Center to Work with Single Sign-On</td>
<td>117</td>
</tr>
<tr>
<td>Configuring Fortify Software Security Center to Work with a Central Authorization Server</td>
<td>118</td>
</tr>
<tr>
<td>Setting up Kerberos Authentication with Fortify Software Security Center</td>
<td>118</td>
</tr>
<tr>
<td>Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single Sign-On Solutions</td>
<td>119</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>121</td>
</tr>
<tr>
<td>Configuring Fortify Software Security Center to Work with Single Sign-On and Single Logout Solutions that use HTTP Headers</td>
<td>122</td>
</tr>
<tr>
<td>Configuring Fortify Software Security Center to use X.509 Certification-based SSO</td>
<td>123</td>
</tr>
<tr>
<td>Configuring Web Services to Require Token Authentication</td>
<td>124</td>
</tr>
<tr>
<td>Chapter 8: Additional Installation-Related Tasks</td>
<td>125</td>
</tr>
<tr>
<td>Disabling the Legacy User Interface</td>
<td>125</td>
</tr>
<tr>
<td>Setting the Legacy User Interface as the Default User Interface</td>
<td>126</td>
</tr>
<tr>
<td>Blocking Data Export to CSV Files</td>
<td>126</td>
</tr>
<tr>
<td>Configuring an Eclipse Plugin Update Site</td>
<td>127</td>
</tr>
<tr>
<td>About Bug Tracker Integration</td>
<td>127</td>
</tr>
<tr>
<td>Managing Bug Tracker Plugins</td>
<td>128</td>
</tr>
</tbody>
</table>
Adding Bug Tracker Plugins .............................................................. 128
Removing Bug Tracker Plugins ...................................................... 128
Securing Logon Credentials for Bug Tracking Systems .................. 129
Bug Tracker Parameters .................................................................. 129
HPE ALM Parameters ..................................................................... 130
Adding and Managing Parser Plugins ............................................ 130
About Fortify Software Security Center User Administration .......... 131
Administrator Accounts ................................................................. 131
Fortify Software Security Center User Accounts .......................... 132
About Creating User Accounts ....................................................... 132
Preventing Destructive Library and Template Uploads to Fortify Software Security Center ......................................................... 133
Viewing Permission Information for Fortify Software Security Center Roles .......................................................... 133
Unlocking User Accounts (Local Users Only) ................................. 134
About Managing LDAP User Roles ................................................. 135
Group Membership in Fortify Software Security Center .............. 135
Handling Failed LDAP User Logins ................................................. 135
About Mapping Fortify Software Security Center Roles to LDAP Groups .......................................................... 136
Creating Custom Application Attributes ...................................... 136
Global Search Functionality in Fortify Software Security Center .... 138
About Global Search Functionality ................................................. 138
Troubleshooting Search Index Issues .......................................... 139
Placing Fortify Software Security Center in Maintenance Mode .... 139
Chapter 9: Upgrading Fortify Software Security Center .................. 141
Fortify Software Security Center Database Upgrade Tasks .......... 141
Preparing to Upgrade the Fortify Software Security Center Database ......................................................... 142
 Setting the Innodb Buffer Pool Size when Upgrading a MySQL Server Database ......................................................... 143
Preparing to Run the Database Upgrade Script .............................. 143
Updating and Deploying the WAR File ........................................... 143
Configuring Fortify Software Security Center After an Upgrade ...... 144
Troubleshooting Database Migration Problems ............................ 147
Troubleshooting an Error Received While Seeding an IBM DB2 Database .......................................................... 147
Upgrading Fortify Static Code Analyzer from Fortify Audit Workbench .......................................................... 148
 Enabling Fortify Static Code Analyzer Suite Upgrades from Fortify Audit Workbench ......................................................... 148
Updating Expired Licenses ............................................................... 150
Seeding the Database with Seed Bundles Delivered with Quarterly Security Content Releases ......................................................... 151
Part II: Using Fortify Software Security Center .................................................. 153

Chapter 10: Using Fortify Software Security Center ........................................ 154
  About the Central Role of Fortify Software Security Center .......................... 154
  Security Management Workflow ................................................................. 155
  User Accounts and Access ........................................................................... 155
    Active Directory/LDAP Integration ............................................................ 156
    Logging in to Fortify Software Security Center for the First Time ............. 156
    Requesting Access to Fortify Software Security Center ......................... 157
    Changing Your Password ......................................................................... 158
    Enabling and Disabling Receipt of Email Alerts ........................................ 159
  About the Fortify Software Security Center Dashboard ............................... 160
    Issue Stats Page ....................................................................................... 160
    Exporting Data to Comma-Separated Values Files .................................... 163
    Deactivating Application Versions ........................................................... 164
    Reactivating Application Versions ........................................................... 164

Chapter 11: Managing User Accounts ............................................................... 166
  Fortify Software Security Center User Account Management .................... 166
  Modifying Your User Account ..................................................................... 166
  About Tracking Teams ................................................................................ 167
  About Roles .................................................................................................. 167
    Pre-configured Roles ................................................................................ 167
    Role-Based Permissions for Fortify Software Security Center .................. 168
    Creating Custom Roles ............................................................................ 173
    Deleting Custom Roles ............................................................................ 174
  Fortify Software Security Center Account Administration ......................... 175
    Creating Local User Accounts .................................................................. 175
    Registering LDAP Entities ....................................................................... 176
    Unlocking User Accounts (Local Users Only) ........................................... 179

Chapter 12: Applications and Application Versions ........................................ 180
  About Tracking Development Teams ......................................................... 181
    About the Application Creation Process ............................................... 181
    Strategies for Creating Application Versions ........................................... 182
      Strategies for Packaged Software ......................................................... 182
      Strategies for Continuous Deployment ................................................ 182
    About Annotating Application Versions for Reporting ............................. 182
    Viewing a List of Fortify Software Security Center Applications ................ 182
  About Creating Application Versions ......................................................... 183
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Version Attributes</td>
<td>183</td>
</tr>
<tr>
<td>Creating Custom Attributes</td>
<td>184</td>
</tr>
<tr>
<td>Specifying New Custom Attributes in Existing Application Versions</td>
<td>187</td>
</tr>
<tr>
<td>About Issue Templates</td>
<td>187</td>
</tr>
<tr>
<td>Adding Issue Templates to the System</td>
<td>188</td>
</tr>
<tr>
<td>Template Selection</td>
<td>188</td>
</tr>
<tr>
<td>Creating the First Version of a New Application</td>
<td>189</td>
</tr>
<tr>
<td>Adding a New Version to an Application</td>
<td>192</td>
</tr>
<tr>
<td>Searching Applications and Application Versions from the Applications View</td>
<td>195</td>
</tr>
<tr>
<td>Updating the Application Overview Page</td>
<td>195</td>
</tr>
<tr>
<td>Editing Application Version Details</td>
<td>195</td>
</tr>
<tr>
<td>About Deleting Application Versions</td>
<td>196</td>
</tr>
<tr>
<td>Deactivating Application Versions</td>
<td>196</td>
</tr>
<tr>
<td>Reactivating Application Versions</td>
<td>197</td>
</tr>
<tr>
<td>Deleting an Application Version</td>
<td>198</td>
</tr>
<tr>
<td>Using Bug Tracking Systems to Help Manage Security Vulnerabilities</td>
<td>198</td>
</tr>
<tr>
<td>Bug Tracker Configuration</td>
<td>199</td>
</tr>
<tr>
<td>Velocity Templates for Bug Filing</td>
<td>199</td>
</tr>
<tr>
<td>Adding Velocity Templates to Bug Tracker Plugins</td>
<td>200</td>
</tr>
<tr>
<td>Editing Velocity Templates for Bug Tracker Plugins</td>
<td>202</td>
</tr>
<tr>
<td>Deleting Velocity Templates</td>
<td>202</td>
</tr>
<tr>
<td>Submitting a Bug for One or More Issues</td>
<td>203</td>
</tr>
<tr>
<td>Bug State Management</td>
<td>204</td>
</tr>
<tr>
<td>Changing the Template Associated with an Application Version</td>
<td>205</td>
</tr>
<tr>
<td>Setting Analysis Result Processing Rules for Application Versions</td>
<td>206</td>
</tr>
<tr>
<td>Custom Tags</td>
<td>209</td>
</tr>
<tr>
<td>Adding Custom Tags to the System</td>
<td>210</td>
</tr>
<tr>
<td>Modifying Custom Tag Attributes</td>
<td>212</td>
</tr>
<tr>
<td>Globally Hiding Custom Tags</td>
<td>213</td>
</tr>
<tr>
<td>Deleting Custom Tags</td>
<td>213</td>
</tr>
<tr>
<td>Adding Custom Tag Values</td>
<td>213</td>
</tr>
<tr>
<td>Editing Custom Tags</td>
<td>214</td>
</tr>
<tr>
<td>Deleting Custom Tag Values</td>
<td>214</td>
</tr>
<tr>
<td>Deleting Custom Tag Values</td>
<td>214</td>
</tr>
<tr>
<td>Associating Custom Tags with Issue Templates</td>
<td>215</td>
</tr>
<tr>
<td>Viewing the Custom Tags Associated with an Issue Template</td>
<td>216</td>
</tr>
<tr>
<td>Removing Custom Tags from Issue Templates</td>
<td>216</td>
</tr>
<tr>
<td>Assigning Custom Tags to Application Versions</td>
<td>217</td>
</tr>
<tr>
<td>Disassociating a Custom Tag from an Application Version</td>
<td>218</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Managing Custom Tags Through Issue Templates</td>
<td>219</td>
</tr>
<tr>
<td>Managing Custom Tags Through an Issue Template in an FPR File</td>
<td>219</td>
</tr>
<tr>
<td>Chapter 13: Variables, Performance Indicators, and Alerts</td>
<td>220</td>
</tr>
<tr>
<td>Working with Variables</td>
<td>220</td>
</tr>
<tr>
<td>Creating Variables</td>
<td>220</td>
</tr>
<tr>
<td>Variable Syntax</td>
<td>221</td>
</tr>
<tr>
<td>Performance Indicators</td>
<td>222</td>
</tr>
<tr>
<td>Creating Performance Indicators</td>
<td>222</td>
</tr>
<tr>
<td>Alert Definitions</td>
<td>223</td>
</tr>
<tr>
<td>Creating Alerts</td>
<td>223</td>
</tr>
<tr>
<td>Editing Alerts</td>
<td>226</td>
</tr>
<tr>
<td>Deleting Alerts</td>
<td>226</td>
</tr>
<tr>
<td>Viewing and Marking Alerts</td>
<td>227</td>
</tr>
<tr>
<td>Chapter 14: About Working with Scan Artifacts</td>
<td>229</td>
</tr>
<tr>
<td>Uploading Scan Artifacts</td>
<td>229</td>
</tr>
<tr>
<td>Viewing File Processing Errors</td>
<td>231</td>
</tr>
<tr>
<td>Uploading SAP NetWeaver Data to an Application Version</td>
<td>231</td>
</tr>
<tr>
<td>Viewing Scan Errors</td>
<td>233</td>
</tr>
<tr>
<td>Downloading Scan Artifacts</td>
<td>234</td>
</tr>
<tr>
<td>Downloading the Merged FPR File for an Application Version</td>
<td>234</td>
</tr>
<tr>
<td>Downloading Individual Scan Results</td>
<td>235</td>
</tr>
<tr>
<td>Approving Scan Artifacts</td>
<td>235</td>
</tr>
<tr>
<td>Viewing High-Level Summary Results</td>
<td>235</td>
</tr>
<tr>
<td>Viewing Summary Metrics on the Issue Stats Page</td>
<td>236</td>
</tr>
<tr>
<td>Viewing Summary Metrics on the Chart Page</td>
<td>236</td>
</tr>
<tr>
<td>Viewing Summary Metrics on the Overview Page</td>
<td>237</td>
</tr>
<tr>
<td>Displaying Additional Application Versions on the Dashboard</td>
<td>238</td>
</tr>
<tr>
<td>Viewing Issue Metadata</td>
<td>239</td>
</tr>
<tr>
<td>Mapping Scan Results to External Lists</td>
<td>239</td>
</tr>
<tr>
<td>Purging Scan Artifacts</td>
<td>240</td>
</tr>
<tr>
<td>Deleting Artifacts</td>
<td>241</td>
</tr>
<tr>
<td>Chapter 15: Collaborative Auditing</td>
<td>242</td>
</tr>
<tr>
<td>About Auditing</td>
<td>242</td>
</tr>
<tr>
<td>About Current Issues State</td>
<td>242</td>
</tr>
<tr>
<td>Setting the Strategy for Resolving Issue Audit Conflicts</td>
<td>243</td>
</tr>
<tr>
<td>Auditing Issues</td>
<td>244</td>
</tr>
<tr>
<td>Accessing the Audit Page from the Issue Stats Page of the Dashboard</td>
<td>244</td>
</tr>
</tbody>
</table>
Creating CloudScan Sensor Pools ................................................................. 282
Deleting CloudScan Pools ................................................................. 284

Chapter 17: BIRT Reports ................................................................. 285
Issue Reports ................................................................. 285
CWE/SANS Top 25 Reports ................................................................. 285
Developer Workbook Report ................................................................. 286
DISA STIG Reports ................................................................. 286
FISMA Compliance: FIPS - 200 Report ................................................................. 286
OWASP Mobile Top 10 Reports ................................................................. 286
OWASP Top 10 Reports ................................................................. 286
PCI DSS Compliance: Application Security Report ................................................................. 286
Penetration Testing Correlation Report ................................................................. 287
Seven Pernicious Kingdoms Report ................................................................. 287
Vulnerability Report ................................................................. 287
Portfolio Reports ................................................................. 287
Hierarchical Summary Report ................................................................. 287
Issue Trending Report ................................................................. 287
Key Performance Indicators Report ................................................................. 288
Security at a Glance Report ................................................................. 288
Application Summary Report ................................................................. 288
Generating and Viewing Reports ................................................................. 288
Preventing Destructive Libraries and Templates from Being Uploaded ................................................................. 291
BIRT Libraries ................................................................. 291
Importing Report Libraries ................................................................. 291
Customizing Fortify Software Security Center BIRT Reports ................................................................. 292
Acquiring the BIRT Report Designer ................................................................. 292
Downloading Report Definitions ................................................................. 293
Importing Report Definitions ................................................................. 293

Chapter 18: Authentication Tokens ................................................................. 295
Generating Authentication Tokens ................................................................. 295

Appendix A: LDAP Configuration Property Descriptions ................................................................. 297

Appendix B: Using the fortifyclient Utility ................................................................. 299
fortifyclient Requirements ................................................................. 299
About Specifying the Fortify Software Security Center URL ................................................................. 300
fortifyclient Authentication Tokens ................................................................. 300
Preface

Contacting HPE Security Fortify Support

If you have questions or comments about using this product, contact HPE Security Fortify Technical Support using one of the following options.

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

https://support.fortify.com

To Email Support

fortifytechsupport@hpe.com

To Call Support

1.844.260.7219

For More Information

For more information about HPE Security software products:

http://www.hpe.com/software/fortify

About the Documentation Set

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


You will need to register for an account.
# Change Log

The following table lists changes made to this document.

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

<table>
<thead>
<tr>
<th>Software Release / Document Revision</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.20</td>
<td>All references to the Configuration Wizard were removed. Settings that existed in the configuration wizard in earlier versions are now accessed through the Fortify Software Security Center Administration view.</td>
</tr>
</tbody>
</table>

**New topics:**

- "What's New in Fortify Software Security Center 17.20" on page 22
- "Adding the JDBC Driver to Fortify Software Security Center" on page 46
- "About the fortify.home Directory" on page 61
- "Configuring Fortify Software Security Center for the First Time" on page 70
- "Blocking Data Export to CSV Files" on page 126
- "Managing Bug Tracker Plugins" on page 128
- "Adding and Managing Parser Plugins" on page 130
- "Placing Fortify Software Security Center in Maintenance Mode" on page 139
- "Configuring Fortify Software Security Center After an Upgrade" on page 144
- "Seeding the Database with Seed Bundles Delivered with Quarterly Security Content Releases" on page 151
- "Exporting Data to Comma-Separated Values Files" on page 163
- "Debugging a Bug Tracker Plugin" on page 320

**Modified topics:**

- "Switching Between the New User Interface and the Legacy User Guide"
<table>
<thead>
<tr>
<th>Software Release / Document Revision</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Interface &quot; on page 24</td>
</tr>
<tr>
<td></td>
<td>• &quot;Preparing for Fortify Software Security Center Deployment&quot; on page 39</td>
</tr>
<tr>
<td></td>
<td>• &quot;About JDBC Drivers&quot; on page 46</td>
</tr>
<tr>
<td></td>
<td>• &quot;Configuration Options Available in the Administration View&quot; on page 78</td>
</tr>
<tr>
<td></td>
<td>• The procedure described in &quot;Configuring Audit Assistant&quot; on page 83 was changed to reflect the addition of the <strong>Prediction policy name</strong> list to the Audit Assistant page.</td>
</tr>
<tr>
<td></td>
<td>• &quot;Configuring Core Settings&quot; on page 87</td>
</tr>
<tr>
<td></td>
<td>• &quot;Adding the SAP JCo Driver to Fortify Software Security Center&quot; on page 108</td>
</tr>
<tr>
<td></td>
<td>• &quot;About Bug Tracker Integration&quot; on page 127</td>
</tr>
<tr>
<td></td>
<td>• &quot;Global Search Functionality in Fortify Software Security Center&quot; on page 138</td>
</tr>
<tr>
<td></td>
<td>• &quot;Upgrading Fortify Software Security Center&quot; on page 141</td>
</tr>
<tr>
<td></td>
<td>• &quot;Preparing to Upgrade the Fortify Software Security Center Database&quot; on page 142</td>
</tr>
<tr>
<td></td>
<td>• &quot;Updating Expired Licenses&quot; on page 150</td>
</tr>
</tbody>
</table>

**Removed topics:**

- Starting the HPE Security Fortify Software Security Center Configuration Wizard
- Running the Configuration Wizard from the Command Line
- Setting Properties Using the Configuration Wizard
- Configuring the Core Parameters
- Saving the Configuration Wizard Settings
- About Database Setup
- Seeding a New Fortify Software Security Center Database
- Reseeding the Upgraded Database
<table>
<thead>
<tr>
<th>Software Release / Document Revision</th>
<th>Changes</th>
</tr>
</thead>
</table>
|                                    | - Configuring the Database Connection Parameters  
|                                    | - About Configuring Connectivity to an Upgraded Database  
|                                    | - Migrating from a Previous Version of Fortify Software Security Center  
|                                    | - Generating and Running the Database Migration Script  
|                                    | - Testing the JDBC Connection  
|                                    | - Configuring the Defect Tracker Plugins  
|                                    | - Additional Bug Tracker Configuration Information  
| 17.10                              | - This document now includes all content from the *HPE Security Fortify Software Security Center Installation and Configuration Guide*, which is no longer published, as of this release.  
|                                    | - Removed all references to the Solaris operating system, which is no longer supported.  
|                                    | **New topics:**  
|                                    | - "What's New in Fortify Software Security Center 17.20 " on page 22  
|                                    | - "Getting a Fortify Scan Analytics Authentication Token" on page 82  
|                                    | - "Refreshing LDAP Entities Manually" on page 107  
|                                    | - "Configuring Browser Access Security for Fortify Software Security Center" on page 115  
|                                    | - "Setting the Strategy for Resolving Issue Audit Conflicts" on page 243  
|                                    | - "Viewing Issues Assigned to You" on page 251  
|                                    | - "Submitting Training Data to Audit Assistant" on page 266  
|                                    | **Modified topics:**  
|                                    | - The topic "Configuring LDAP Servers" on page 94 includes more information about the Base Distinguished Name for LDAP directory structure searches and about Relative Search DNs.  
|                                    | - "Configuring Fortify Software Security Center to Work with Single Sign-On and Single Logout Solutions that use HTTP Headers" on page 122 now contains information about how to configure single logout.
<table>
<thead>
<tr>
<th>Software Release / Document Revision</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• The task for validating the database was removed from the table of tasks in the topic About Database Setup.</td>
</tr>
<tr>
<td></td>
<td>• &quot;Registering LDAP Entities&quot; on page 176 now includes a step that describes how to refresh the LDAP cache manually.</td>
</tr>
<tr>
<td></td>
<td>• The procedure described in &quot;Creating Alerts&quot; on page 223 includes a new step to reset performance indicator and variable alerts after each artifact upload. It also includes new steps to create a scheduled alert.</td>
</tr>
<tr>
<td></td>
<td>• &quot;Auditing Issues&quot; on page 244 now includes information on how to attach an image file to an issue during an audit.</td>
</tr>
<tr>
<td></td>
<td>• The ruleid and dynamic modifiers were removed from the table of modifiers in &quot;Search Modifiers&quot; on page 253.</td>
</tr>
<tr>
<td></td>
<td>• The topic &quot;About Audit Assistant&quot; on page 258 now includes information about how to request a Fortify Scan Analytics account.</td>
</tr>
<tr>
<td>16.20</td>
<td>Removed all information related to the Red Hat JBoss application server, which is no longer supported.</td>
</tr>
<tr>
<td></td>
<td><strong>New topics:</strong></td>
</tr>
<tr>
<td></td>
<td>• What's New in the HPE Fortify Software Security Center 16.20 User Interface</td>
</tr>
<tr>
<td></td>
<td>• &quot;Accessing the Software Security Center API Documentation&quot; on page 33</td>
</tr>
<tr>
<td></td>
<td>• &quot;Configuring Issue Stats Thresholds&quot; on page 77</td>
</tr>
<tr>
<td></td>
<td>• &quot;Configuring Audit Assistant&quot; on page 83</td>
</tr>
<tr>
<td></td>
<td>• &quot;Unlocking User Accounts (Local Users Only)&quot; on page 179</td>
</tr>
<tr>
<td></td>
<td>• &quot;Setting Job Execution Priority&quot; on page 114</td>
</tr>
<tr>
<td></td>
<td>• &quot;Canceling Scheduled Jobs&quot; on page 115</td>
</tr>
<tr>
<td>Software Release / Document Revision</td>
<td>Changes</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td><strong>Modified topics:</strong></td>
</tr>
<tr>
<td></td>
<td>• The topic title &quot;Enabling Global Searches in Fortify Software Security Center&quot; was changed to &quot;Enabling Global Searches&quot;</td>
</tr>
<tr>
<td></td>
<td>• &quot;About Using HTTPS and SSL Communications&quot; on page 36 now includes information about how to configure some Fortify SCA tools to communicate with Fortify Software Security Center using https.</td>
</tr>
<tr>
<td></td>
<td>• &quot;Installing and Configuring the Database Server Software&quot; on page 47</td>
</tr>
<tr>
<td></td>
<td>• &quot;Configuring Fortify Software Security Center to Work with a Central Authorization Server&quot; on page 118</td>
</tr>
<tr>
<td></td>
<td>• &quot;Setting up Kerberos Authentication with Fortify Software Security Center&quot; on page 118</td>
</tr>
<tr>
<td></td>
<td>• &quot;Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single Sign-On Solutions&quot; on page 119</td>
</tr>
<tr>
<td></td>
<td>• &quot;Configuring Fortify Software Security Center to Work with Single Sign-On and Single Logout Solutions that use HTTP Headers&quot; on page 122</td>
</tr>
<tr>
<td></td>
<td>• &quot;Configuring Fortify Software Security Center to use X.509 Certification-based SSO&quot; on page 123</td>
</tr>
<tr>
<td></td>
<td><strong>Removed topics:</strong></td>
</tr>
<tr>
<td></td>
<td>• Software Security Center Deployment in JBoss Enterprise Application Platform</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

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

If you are not installing Fortify Software Security Center for the first time, see the instructions on how to upgrade from an earlier version "Upgrading Fortify Software Security Center" on page 141).

This section contains the following topics:

- Intended Audience .................................................. 21
- Document Structure .................................................. 22
- What’s New in Fortify Software Security Center 17.20 .................................................. 22
- Switching Between the New User Interface and the Legacy User Interface ............................. 24
- Disabling the Legacy User Interface .................................................. 25
- Viewing Fortify Software Security Center Keyboard Shortcuts .................................................. 25
- Disabling Keyboard Shortcuts (Hotkeys) .................................................. 26
- Related Documents .................................................. 26
- Accessing the Software Security Center API Documentation .................................................. 33

Intended Audience

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

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

- System and instance administrators
- Database administrators

For information about how to access the Software Security Center API Documentation, see "Accessing the Software Security Center API Documentation" on page 33.
Document Structure

This document is divided into two main parts. Part 1 ("Fortify Software Security Center Deployment" on page 34) includes chapters that describe the deployment environment and provide instructions for installing and configuring Fortify Software Security Center. Part 2 ("Using Fortify Software Security Center" on page 153) includes chapters that describe how to use Fortify Software Security Center.

What's New in Fortify Software Security Center 17.20

The Fortify Software Security Center 17.20 release introduces several new features, which are described here.

New Setup Wizard Replaces the Configuration Wizard

The configuration wizard has been replaced by the new Setup wizard, which is part of the Fortify Software Security Center user interface. For more information, see "Configuring Fortify Software Security Center for the First Time" on page 70.

New Path for Fortify Software Security Center Configuration and Resources

As of this release, server configuration files and other Fortify Software Security Center resources reside in fortify.home. For more information, see "About the fortify.home Directory" on page 61.

New Software Distribution Bundles

The single software distribution bundle for Fortify Software Security Center is now delivered as the following application server-specific installation bundles:

- HPE_Security_Fortify_17.20_Server_WAR_Tomcat.zip
- HPE_Security_Fortify_17.20_Server_WAR_WebLogic.zip
- HPE_Security_Fortify_17.20_Server_WAR_WebSphere.zip
View Issues Based on the Dates They Were Introduced to Your Code

On the Audit page, you can now group issues based on the dates on which they were first detected in an application version. To view issues based on the date on which they were introduced, from the Group by list, select Introduced date. This option is available on the Audit and Overview pages for an application version.

Selecting the Prediction Policy for Audit Assistant

Previously, to specify the prediction policy to apply to your application versions, Audit Assistant users had to type the exact name of the policy into the box. Now, users can select the prediction policy name from a list. (See “Configuring Audit Assistant” on page 83.)

New Plugin Framework

This release introduces a new plugin framework. Fortify Software Security Center now supports third-party parser plugins and bug tracker plugins.

The 17.20 release introduces a new plugin framework to support a growing ecosystem of integrations. The framework supports running third-party parser plugins, bug tracker plugins, and is designed with the core goals of isolation, granularity, and reliability in mind.

Isolation: Each plugin defines and wraps its own dependencies inside of its bundle. The framework takes care of dependency isolation from the rest of the Fortify Software Security Center loaded libraries.

Granularity: The framework supports different kinds of plugins to perform different operations in Fortify Software Security Center. It is agnostic to the implementation type the plugin needs. In the 17.20 version, data parsers and bug trackers are supported.
Reliability: The framework is built with a robust and reliable messaging mechanism to ensure data integrity.

For more information, see "Adding and Managing Parser Plugins" on page 130 and "Managing Bug Tracker Plugins" on page 128.

Exporting Data to Comma-Separated Values Files

You can now export the data shown on the Issue Stats and Audit pages to CSV files for examination and manipulation outside of Fortify Software Security Center. For information, see "Exporting Data to Comma-Separated Values Files" on page 163.

Switching Between the New User Interface and the Legacy User Interface

To access the legacy user interface:

1. Log in to Fortify Software Security Center.

2. At the right end of the Hewlett Packard Enterprise header, click the user profile icon, and then select 4.30 UI.

   The legacy user interface opens in a new browser tab and displays your data.

To return to the new user interface from the legacy user interface:

- On the Hewlett Packard Enterprise header, click the Go to new UI link.

Accessing Legacy Documentation

If you need information about the legacy user interface, see the HP Fortify Software Security Center Installation and Configuration Guide or the HP Fortify Software Security Center User Guide for version 4.30.
Disabling the Legacy User Interface

You can prevent all users from accessing the Fortify Software Security Center legacy (4.30) user interface.

To disable the Fortify Software Security Center legacy user interface:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Hewlett Packard Enterprise header, click **Administration**.
2. In the left panel, click **Configuration**, and then click **Core**. The Core SSC Attributes page opens.
3. Near the bottom of the page, select the **Disable 4.30 legacy UI** check box.
4. Click **Save**. Fortify Software Security Center removes the **4.30 UI** item from the user profile list instance-wide.
5. Restart the server.

Viewing Fortify Software Security Center Keyboard Shortcuts

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

1. Log in to Fortify Software Security Center.
2. Do one of the following:
   - At the right end of the Hewlett Packard Enterprise header, click the user profile icon, and then select **Hotkeys**.
   - Press the question mark key (?) on your keyboard.

See Also

"Disabling Keyboard Shortcuts (Hotkeys)" on the next page
Disabling Keyboard Shortcuts (Hotkeys)

To disable Fortify Software Security Center keyboard shortcuts:

1. Log in to Fortify Software Security Center.

2. At the right end of the Hewlett Packard Enterprise header, click the user profile icon, and then select Preferences.

3. In the Preferences dialog box, select the Disable Hotkeys check box, and then click Save.

Related Documents

This topic describes documents that provide information about HPE Security Fortify Software Security Center.

Note: The Protect724 site location is https://www.protect724.hpe.com/community/fortify/fortify-product-documentation.
All Products

The following documents provide general information for all products. Unless otherwise noted, these documents are available on the Protect724 site.

<table>
<thead>
<tr>
<th>Document / File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Fortify Product Documentation</td>
<td>This paper provides information about how to access Fortify product documentation.</td>
</tr>
<tr>
<td>About_Fortify_Doc_&lt;version&gt;.pdf</td>
<td>Note: This document is included only with product download.</td>
</tr>
<tr>
<td>HPE Security Fortify Software System Requirements</td>
<td>This document provides the details about the environments and products supported for this version of HPE Security Fortify Software.</td>
</tr>
<tr>
<td>HPE_Sys_Reqs_&lt;version&gt;.pdf</td>
<td></td>
</tr>
<tr>
<td>HPE Security Fortify Software Release Notes</td>
<td>This document provides an overview of the changes made to HPE Security Fortify Software for this release and important information not included elsewhere in the product documentation.</td>
</tr>
<tr>
<td>HPE_FortifySW_RN_&lt;version&gt;.txt</td>
<td></td>
</tr>
<tr>
<td>What's New in HPE Security Fortify Software &lt;version&gt;</td>
<td>This document describes the new features in HPE Security Fortify Software products.</td>
</tr>
<tr>
<td>HPE Whats_New_&lt;version&gt;.pdf</td>
<td></td>
</tr>
<tr>
<td>HPE Security Fortify Open Source and Third-Party License Agreements</td>
<td>This document provides open source and third-party software license agreements for software components used in HPE Security Fortify Software.</td>
</tr>
<tr>
<td>HPE_OpenSrc_&lt;version&gt;.pdf</td>
<td></td>
</tr>
</tbody>
</table>

HPE Security Fortify CloudScan

The following documents provide information about Fortify CloudScan. Unless otherwise noted, these documents are available on the Protect724 site.

<table>
<thead>
<tr>
<th>Document / File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPE Security Fortify CloudScan</td>
<td>This document provides information about how to</td>
</tr>
</tbody>
</table>
### Installation, Configuration, and Usage Guide

HPE_CloudScan_Guide_<version>.pdf

HPE_CloudScan_Help_<version>

install, configure, and use Fortify CloudScan to streamline the static code analysis process. It is written for anyone who intends to install, configure, or use Fortify CloudScan for offloading the scanning phase of their Fortify Static Code Analyzer process.

### HPE Security Fortify Software Security Center

The following documents provide information about Fortify Software Security Center. Unless otherwise noted, these documents are available on the Protect724 site.

<table>
<thead>
<tr>
<th>Document / File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPE_SCC_Proc_Design_Guide_Legacy_&lt;version&gt;.pdf</td>
<td>This document provides information about how to start the Process Designer, configure its connection to your Fortify Software Security Center instance, and then use it to work with Fortify Software Security Center process templates, which are used only in the Fortify Software Security Center legacy (version 4.30) user interface.</td>
</tr>
<tr>
<td>HPE_SCC_Proc_Design_Help_&lt;version&gt;</td>
<td></td>
</tr>
</tbody>
</table>

### HPE Security Fortify Static Code Analyzer

The following documents provide information about Fortify Static Code Analyzer. Unless otherwise noted, these documents are available on the Protect724 site.

<table>
<thead>
<tr>
<th>Document / File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPE_SCA_Install_Help_&lt;version&gt;</td>
<td></td>
</tr>
<tr>
<td>Document / File Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **HPE Security Fortify Static Code Analyzer User Guide**  
HPE_SCA_Help_<version>  
PDF only; no help file | This document describes how to use Fortify Static Code Analyzer to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding. |
| **HPE Security Fortify Static Code Analyzer Performance Guide**  
PDF only; no help file | This document provides guidelines for selecting hardware to scan different types of codebases and offers tips for optimizing memory usage and performance. |
| **Note:** This document is included only with the product download. |
| **HPE Security Fortify Static Code Analyzer Custom Rules Guide**  
HPE_SCA_Cust_Rules_Guide_<version>.zip  
PDF only; no help file | This document provides the information that you need to create custom rules for Fortify Static Code Analyzer. This guide includes examples that apply rule-writing concepts to real-world security issues. |
| **HPE Security Fortify Audit Workbench User Guide**  
HPE_AWB_Guide_<version>.pdf  
HPE_AWB_Help_<version>  
PDF only; no help file | This document describes how to use 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. |
| **HPE Security Fortify Remediation Extension for JDeveloper Installation and Usage Guide**  
HPE_Jdev_Plugin_Guide_<version>.pdf  
HPE_Jdev_Plugin_Help_<version>  
PDF only; no help file | This document provides an overview of the Fortify Remediation Extension for JDeveloper and instructions on how to install and use the extension to remediate issues uncovered in your source code. |
| **HPE Security Fortify Package for Visual Studio User Guide**  
HPE_VS_Pkg_Guide_<version>.pdf  
HPE_VS_Pkgs_Help_<version>  
PDF only; no help file | This document provides information about how to install and use the Fortify Visual Studio Package to analyze, audit, and remediate your code to resolve security-related issues in solutions and projects. |
<table>
<thead>
<tr>
<th>Document / File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPE Security Fortify Plugins for Eclipse Installation and Usage Guide</td>
<td>This document provides information about how to install and use the Fortify Complete and the Fortify Remediation Plugins for Eclipse.</td>
</tr>
<tr>
<td>HPE_Eclipse_Plugins_Guide_&lt;version&gt;.pdf</td>
<td></td>
</tr>
<tr>
<td>HPE_Eclipse_Plugins_Help_&lt;version&gt;</td>
<td></td>
</tr>
<tr>
<td>HPE_IntelliJ_AndStud_Plugins_Guide_&lt;version&gt;.pdf</td>
<td></td>
</tr>
<tr>
<td>HPE_IntelliJ_AndStud_Plugins_Help_&lt;version&gt;</td>
<td></td>
</tr>
<tr>
<td>HPE_SCA_Tools_Props_Ref_&lt;version&gt;.pdf</td>
<td></td>
</tr>
<tr>
<td>HPE_SCA_Tools_Props_Ref_Help_&lt;version&gt;</td>
<td></td>
</tr>
<tr>
<td>HPE Security Fortify Jenkins Plugin Installation and Usage Guide</td>
<td>This document provides instructions on how to prepare Fortify Software Security Center to work with the Jenkins plugin, and how to install, configure, and use the plugin.</td>
</tr>
<tr>
<td>HPE_Jenkins_Plugin_Guide_&lt;version&gt;.pdf</td>
<td></td>
</tr>
<tr>
<td>HPE_Jenkins_Plugin_Help_&lt;version&gt;</td>
<td></td>
</tr>
<tr>
<td>HPE Security Fortify Security Assistant Plugin for Eclipse User Guide</td>
<td>This document describes how to install and use Fortify Security Assistant to provide alerts to security issues as you write your Java code.</td>
</tr>
<tr>
<td>HPE_SecAssist_Guide_&lt;version&gt;.pdf</td>
<td></td>
</tr>
</tbody>
</table>
### HPE Security Fortify WebInspect

The following documents provide information about Fortify WebInspect. Unless otherwise noted, these documents are available on the Protect724 site, and help files are available in the product.

<table>
<thead>
<tr>
<th>Document / File Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **HPE Security Fortify WebInspect Installation Guide**  
HPE_WI_Install_<version>.pdf  
PDF only; no help file | This document provides an overview of Fortify WebInspect and instructions for installing Fortify WebInspect and activating the product license. |
| **HPE Security Fortify WebInspect User Guide**  
HPE_WI_Guide_<version>.pdf | This document describes how to configure and use HPE Security Fortify WebInspect to scan and analyze Web applications and Web services.  
**Note:** This document is a PDF version of the Fortify WebInspect help. This PDF 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. |
| **HPE Security Fortify WebInspect Tools Guide**  
HPE_WI_Tools_Guide_<version>.pdf | This document describes how to use the Fortify WebInspect diagnostic and penetration testing tools and configuration utilities packaged with Fortify WebInspect and Fortify WebInspect Enterprise. |
| **HPE Security Fortify WebInspect Runtime Agent Installation Guide**  
HPE_WI_RT_Agent_Install_<version>.pdf | This document describes how to install the Fortify WebInspect Runtime Agent for applications running under a supported Java Runtime Environment (JRE) on a supported application server or service and |
<table>
<thead>
<tr>
<th><strong>Document / File Name</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| HPE_WI_RT_Agent.Install_Help_<version> | applications running under a supported .NET Framework on a supported version of IIS.  
*Note:* The HTML file is available on the Protect724 site. |
| **HPE Security Fortify WebInspect Agent Rulepack Kit Guide**  
HPE_WI_Agent_Rulepack_Guide_<version>.pdf | This document describes the detection capabilities of Fortify WebInspect Agent Rulepack Kit. Fortify WebInspect Agent Rulepack Kit runs atop HPE Security Fortify’s Runtime Agent, allowing it to monitor your code for software security vulnerabilities as it runs. Fortify WebInspect Agent Rulepack Kit provides the runtime technology to help connect your dynamic results to your static ones. |

## HPE Security Fortify WebInspect Enterprise

The following documents provide information about Fortify WebInspect Enterprise. Unless otherwise noted, these documents are available on the Protect724 site, and help files are available in the product.

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

This document describes how to use the Fortify WebInspect diagnostic and penetration testing tools and configuration utilities packaged with Fortify WebInspect and Fortify WebInspect Enterprise.

**Accessing the Software Security Center API Documentation**

To access the Software Security Center API Documentation:


2. Click **API Documentation**. The HPE Security Software Security Center API Documentation <version> page opens.
Part I: Fortify Software Security Center Deployment

The following chapters describe the Fortify Software Security Center deployment environment and provide instructions for installing and configuring Fortify Software Security Center.
Chapter 2: Providing for Secure Deployment

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

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

This section contains the following topics:

- Securing Access to Facilities ................................................................. 35
- Securing the Application Server ......................................................... 35
- Setting Application Server Attributes to Protect Sensitive Data in Cookies ................................................................. 35
- About Using HTTPS and SSL Communications ............................................. 36
- About Securing Passwords and User Roles ................................................. 37
- Managing Computer Services and Accounts ............................................. 38

Securing Access to Facilities

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

Securing the Application Server

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

Setting Application Server Attributes to Protect Sensitive Data in Cookies

Some application server settings might make the sensitive information in some cookies vulnerable to unnecessary disclosure.
To protect sensitive data, Fortify recommends that you add the following attributes (flags) for cookies on the application server:

- **Secure**: The Secure attribute prevents the cookie from being transmitted on requests that are not protected with SSL or TLS. Use this option to prevent cookies that could disclose sensitive information (for example, session identifiers) from leaking information over insecure channels (such as HTTP).

- **HttpOnly**: The HttpOnly attribute prevents the cookie value from being accessed through client-side scripting routines. Fortify recommends that you keep this attribute enabled unless the cookie is being read by client-side JavaScript routines.

For information about how to set the Secure and HttpOnly attributes, see the documentation for your application server.

### About Using HTTPS and SSL Communications

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

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

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

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

However, if you are using a self-signed certificate or one signed by an internal or local signing authority, the Fortify Static Code Analyzer tools Audit Workbench, fortifyclient, Process Designer, the Eclipse Complete plugin, and the Visual Studio package do not trust such certificates by default. In this case, to use https to communicate with Fortify Software Security Center, you must install the self- or locally-signed certificate into the keystore that these Fortify Static Code Analyzer tools use.

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

To install a self-signed or locally-signed certificate into the keystore used by Fortify Static Code Analyzer tools, do the following on every machine on which Audit Workbench, fortifyclient, Process Designer, the Eclipse Complete plugin, or the Visual Studio package is installed:

Open a command prompt, and then run the following:

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

where YourCertFile.cer is the same certificate file that you imported on your application server.

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

```bash
cd <java_home>/jre/bin
dirkeytool -export -alias SSC -keystore <keystore_used_by_app_server> -file YourCertFile.cer
```

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

**Additional Information**

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

If you deployed Fortify Software Security Center in Tomcat, when you create a connector in the server.xml file for HTTPS, make sure that you include the attribute keyAlias, using the name of the alias for the certificate in your keystore. Otherwise, if the keystore contains multiple certificates, it uses the first certificate it finds.

**Running Reports with WebSphere Application Server**

Fortify strongly recommends that you use SSL. However, if Fortify Software Security Center users must run reports, you can configure a reverse proxy in front of WAS.

Fortify Software Security Center cannot run reports with WebSphere Application Server (WAS) JRE while SSL is enabled. An external process such as BIRT ReportRunner does not have WebSphere SSL libraries on its classpath. SSL with IBM JRE works only for web applications deployed to WAS—not for standalone applications.

**About Securing Passwords and User Roles**

Fortify recommends that, after you deploy Fortify Software Security Center and log in for the first time, you immediately create one or more new local administrator accounts and delete the default administrator account. For information about how to log in to Fortify Software Security Center, see “Logging in to Fortify Software Security Center” on page 74.

Fortify Software Security Center account security features include:

- The ability for administrators to suspend accounts that have become temporarily inactive
- The automatic lock-out of accounts on the basis of failed log-on attempts
For more information about Fortify Software Security Center account management, see "Managing User Accounts" on page 166.

If you are using LDAP to authenticate Fortify Software Security Center users, configure your LDAP server to use secure LDAP communications. For information about how to configure Fortify Software Security Center to use LDAP authentication, see "LDAP User Authentication" on page 57.

### Managing Computer Services and Accounts

When you install Fortify Software Security Center, configure it as a service running under a least-privileged user account. Also, because Fortify Software Security Center temporarily stores files that are uploaded from a user account to the computer’s file system, always install and run updated anti-virus software on the machine that hosts Fortify Software Security Center.
Chapter 3: Preparing for Fortify Software Security Center Deployment

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

This section contains the following topics:

- High-Level Deployment Tasks .................................................. 39
- Deployment Overview .............................................................. 41
- Downloading Fortify Software Security Center Files ...................... 44
- Unpacking and Deploying Fortify Software Security Center Software 44
- About the Fortify Software Security Center Database ..................... 45
- LDAP User Authentication ....................................................... 57

High-Level Deployment Tasks

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

**Note:** If you are upgrading Fortify Software Security Center, see “Upgrading Fortify Software Security Center” on page 141.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Information and Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download the Fortify Software Security Center software files and the fortify.license file.</td>
<td>&quot;Downloading Fortify Software Security Center Files&quot; on page 44</td>
</tr>
<tr>
<td>2</td>
<td>Prepare your application server for Fortify Software Security Center deployment.</td>
<td>&quot;Deploying Fortify Software Security Center in an Application Server&quot; on page 61</td>
</tr>
<tr>
<td>3</td>
<td>Unpack and deploy the installation bundle. Then deploy Fortify Software Security Center in your application server.</td>
<td>&quot;Unpacking and Deploying Fortify&quot;</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Information and Instructions</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>4</td>
<td>Install and configure the software for the database server you plan to use for the Fortify Software Security Center database.</td>
<td>About the Fortify Software Security Center Database on page 45</td>
</tr>
<tr>
<td>5</td>
<td>Configure the JDBC driver you plan to use so that your application server can access it.</td>
<td>Adding the JDBC Driver to Fortify Software Security Center on page 46</td>
</tr>
<tr>
<td>6</td>
<td>Log in to Fortify Software Security Center. (See Logging in to Fortify Software Security Center on page 74)</td>
<td>Logging in to Fortify Software Security Center on page 74</td>
</tr>
<tr>
<td>7</td>
<td>Use the Fortify Software Security Center Setup wizard to perform initial configuration. (Locate your Fortify license, create the Fortify Software Security Center database tables and initialize the database schema, seed the database, and so on.)</td>
<td>Configuring Fortify Software Security Center for the First Time on page 70</td>
</tr>
<tr>
<td>8</td>
<td>Restart the Fortify Software Security Center server.</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Complete the Fortify Software Security Center configuration settings in the Administration view. (For the list of the options to configure in the Administration view, see Configuration Options Available in the Administration View on page 78.)</td>
<td>Additional Fortify Software Security Center Configuration on page 76</td>
</tr>
<tr>
<td>10</td>
<td>Perform additional tasks such as configuring an Eclipse plugin update site, setting up bug tracker integration, configuring single sign-on, administering users, registering LDAP entities, managing LDAP user roles, and creating custom attributes that users can assign to their applications.</td>
<td>Additional Installation-Related Tasks on page 125</td>
</tr>
</tbody>
</table>

This section also contains information about the JDBC drivers that are required to interface with the database.
If you no longer need the Fortify Software Security Center database, you can find instructions in this section for permanently deleting it (“Permanently Deleting a Fortify Software Security Center Database” on page 57).

**Deployment Overview**

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

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

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

After you finish the initial Fortify Software Security Center configuration, complete the configuration of the core parameters and configure additional settings from the Administration view. For instructions, see "Additional Fortify Software Security Center Configuration" on page 76.

For system requirements information, see the HPE Security Fortify Software System Requirements document.

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

- **Required components**
  - Third-party application server
  - Third-party database
  - Fortify Security Content Server

- **Optional components**
  - Third-party LDAP authentication server
  - Defect-tracking system
  - Parser plugin
  - SMTP email server
  - One or more Fortify analysis agents and tools

**The Fortify Software Security Center Installation Environment**

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

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

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>Fortify Software Security Center</td>
</tr>
<tr>
<td></td>
<td>Fortify Software Security Center is delivered as a Web Archive (WAR) file run by a web application server (A1).</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>----</td>
<td>-------------</td>
</tr>
<tr>
<td>D1</td>
<td>Third-party database that Fortify Software Security Center requires to store user and artifact data. Before you put Fortify Software Security Center into production, you must install a supported third-party database.</td>
</tr>
<tr>
<td>A1</td>
<td>Application server Fortify Software Security Center (S1) is delivered as a Web Archive (WAR) file and run by a web application server.</td>
</tr>
<tr>
<td>A2</td>
<td>Optional third-party LDAP authentication server You can configure Fortify Software Security Center to use LDAP authentication.</td>
</tr>
<tr>
<td>A3</td>
<td>Optional defect-tracking server You can configure Fortify Software Security Center to enable bug submission directly to Bugzilla, JIRA, ALM, Team Foundation Server (TFS), or a customized bug-tracking system.</td>
</tr>
<tr>
<td>A4</td>
<td>Optional third-party email server You can configure Fortify Software Security Center to use an external SMTP email server to send alerts to application collaborators.</td>
</tr>
<tr>
<td>C1</td>
<td>Optional Fortify Static Code Analyzer analysis agent Fortify Static Code Analyzer scans source code and identifies issues.</td>
</tr>
<tr>
<td>C2</td>
<td>Optional analysis agent Fortify Runtime analyzes instrumented code running in a production environment.</td>
</tr>
<tr>
<td>C3</td>
<td>Fortify Audit Workbench source code auditing tool Although it is technically optional, most Fortify Software Security Center installations use Fortify Audit Workbench to audit issues and categorize vulnerabilities.</td>
</tr>
<tr>
<td>C4</td>
<td>Fortify CloudScan Cloud of machines used to handle the processor-intensive scanning phase of static code analysis.</td>
</tr>
<tr>
<td>C5</td>
<td>Optional analysis agent - Fortify WebInspect Enterprise</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
</tr>
<tr>
<td>F1</td>
<td>Connects with Fortify WebInspect agents to retrieve issue audit information.</td>
</tr>
</tbody>
</table>
| F2  | Fortify download server  
Used to acquire installation programs. |
| F2  | Fortify Security Content update server  
Used to acquire and update Security Content. |

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

### Downloading Fortify Software Security Center Files

Fortify software is available only as an electronic download from the [Fortify Customer Portal](https://customerportal.fortify.com). For descriptions of the Fortify software installation packages available there, see the [HPE Security Fortify Software System Requirements document](https://customerportal.fortify.com).

Download the Fortify Software Security Center installation files and the `fortify.license` file following the instructions in the [HPE Security Fortify Software System Requirements document](https://customerportal.fortify.com).

**See Next**

"Unpacking and Deploying Fortify Software Security Center Software" below

### Unpacking and Deploying Fortify Software Security Center Software

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

1. Extract the contents of the installation file into a temporary directory in a secure location.  
   (The installation file is the file you downloaded using the instructions in "Downloading Fortify Software Security Center Files" above.)

2. Locate the distribution file for your application server (`HPE_Security_Fortify_<version>_Server_WAR_<application server>.zip`) and extract all of the contents into a directory in a secure location. This creates the HPE-Fortify-Server-WAR directory, which contains the resources and tools you need for tasks such as configuring Fortify Software Security Center and migrating applications from previous versions.

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

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

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

The seed bundles are described in the following table.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP_Fortify_Process_Seed_Bundle_2017_Q3.zip</td>
<td>Process template seed bundle used to seed your third-party database tables. It provides a default admin user account and issue template data.</td>
</tr>
<tr>
<td>HP_Fortify_Report_Seed_Bundle_2017_Q3.zip</td>
<td>Report seed bundle used to seed the third-party database tables. It provides the default set of Fortify Software Security Center reports.</td>
</tr>
<tr>
<td>HP_Fortify_PCI_Basic_Seed_Bundle_2017_Q3.zip</td>
<td>(Optional) PCI Basic seed bundle adds a Payment Card Industry process template and its associated report to the default set of issue templates and reports.</td>
</tr>
</tbody>
</table>

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

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

**About the Fortify Software Security Center Database**

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

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

If you are already a Software Security Center user and your database is case-insensitive, see "Correcting a Case-Insensitive SQL Server Database Deployment" on page 49 or "Correcting a Case-Insensitive MySQL Database Deployment" on page 54.

If you are installing a SQL Server or MySQL database, your installation requires special attention. For more information, see "Using a Microsoft SQL Server Database" on page 49 or "Configuring a MySQL Database" on page 52.
**Note:** DB2 and Oracle databases are always case-sensitive.

Later, after you go on to Fortify Software Security Center for the first time, you will use the Fortify Software Security Center Setup wizard to configure connectivity to the database and then seed the database. (See “Configuring Fortify Software Security Center for the First Time” on page 70.)

Topics covered in this section:

- About JDBC Drivers ................................................................. 46
- About Fortify Software Security Center Database Character Set Support .......................... 47
- Installing and Configuring the Database Server Software ........................................... 47
- Database User Account Privileges .............................................................................. 47
- Database-Specific Configuration Requirements .............................................................. 48
- About the Fortify Software Security Center Database Tables and the Schema ............... 56
- About Seeding the Fortify Software Security Center Database ....................................... 56
- Permanently Deleting a Fortify Software Security Center Database .............................. 57

**About JDBC Drivers**

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

**Important:** Before you deploy Fortify Software Security Center for the first time or upgrade an existing instance, you must first verify that the application server class path includes the location of the JDBC driver.

For information about the database driver classes that Fortify Software Security Center supports, see the *HPE Security Fortify Software System Requirements* document. For instructions on how to add the JDBC driver to the system, see “Adding the JDBC Driver to Fortify Software Security Center” below.

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

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

- (Recommended) Add the JDBC JAR file location to the class path of the application server on which you plan to deploy Fortify Software Security Center. For instructions on how to include the library on the class path, see the documentation for your application server.

  The following table lists examples of where you might place the driver, depending on the application server you use.
### Application Server | JDBC Driver Location
--- | ---
Tomcat | `<tomcat_dir>/lib`
WebLogic | Set PRE_CLASSPATH to point to the driver file (for example, setDomainEnv.cmd or setDomainEnv.sh).
WebSphere | `<websphere_dir>/AppServer/lib/ext`

- Do this only if adding the JDBC driver file location to the classpath might interfere with another application deployed on the application server:
  a. Unzip the Fortify Software Security Center installation bundle for your application server (HPE_Security_Fortify_<version>_Server_WAR_<app_server_name>.zip).
  b. Unzip the ssc.war file.
  c. Open the WEB-INF folder, and then place the JDBC JAR file in the lib folder.
  d. Save the ssc.war file, and then re-zip the installation bundle.

### About Fortify Software Security Center Database Character Set Support

For a list of the supported character sets for each third-party database type that Fortify Software Security Center supports, see the HPE Security Fortify Software System Requirements document.

### Installing and Configuring the Database Server Software

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

For information about supported databases, see the HPE Security Fortify Software System Requirements document.

### Database User Account Privileges

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

- **Perform runtime tasks**
  A user who performs runtime tasks requires privileges to do the following:
  - Perform SELECT, UPDATE, INSERT, and DELETE operations in all the database tables
  - Execute stored procedures.

- **Execute migration scripts**
  
  **Important! Important:** Fortify strongly recommends that you create a separate user account to be used for executing migration scripts.
A user who executes migration scripts requires privileges to do the following:
- Perform SELECT, UPDATE, INSERT, and DELETE operations in all the database tables
- Execute stored procedures
- Create, alter, and drop database tables, views, and indexes
- For Oracle databases, permission to enable sequences.

**Create and manage the database**

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

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

**Create and generates reports**

To add an extra measure of security to reporting, create a database user account with read-only access to the Fortify Software Security Center database, and then use the account credentials to configure enhanced security for your BIRT reports (see “Configuring Security for BIRT Reporting” on page 84).

**Database-Specific Configuration Requirements**

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

**Configuring an IBM DB2 Database**

If you are using an IBM DB2 as the Fortify Software Security Center database, do the following:
- Make sure that buffer pools with a page size of 32K are available for the database table spaces (including temporary table spaces).
- Make sure that the DB2 database has enough transaction logs and that they are scaled correctly to account for the load you plan to put through it. Use the following formula to calculate the minimum size and number of transaction logs based on scan size and number of
concurrent jobs you plan to process in Fortify Software Security Center:

\[
\text{page}_\text{size} \ast \text{logfilsize} \ast (\text{primary}_\text{logs} + \text{secondary}_\text{logs}) > \text{your}_\text{largest}_\text{scan}_\text{size} \ast \text{org.quartz.threadPool.threadCount}
\]

- In the DB2 Control Center (Tools, Configuration Assistant, Configure, DB2 Registry), set the values of the following registry variables to ON:
  - DB2_EVALUNCOMMITTED
  - DB2_SKIPDELETED
  - DB2_SKIPINSERTED

**Note:** Fortify Software Security Center does not support internationalization of DB2 databases. For information about DB2 character set support, see "About Fortify Software Security Center Database Character Set Support" on page 47.

**Using a Microsoft SQL Server Database**

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

- Make sure that your SQL Server database schema collation is *case-sensitive*. The default installation of SQL Server is *case-insensitive*.

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

  **For additional information,** see "Correcting a Case-Insensitive SQL Server Database Deployment" below or "Correcting a Case-Insensitive MySQL Database Deployment" on page 54.

- Before you run the fortify-provided SQL scripts, verify that there are no open connections to the database.
- Make sure that snapshot isolation is enabled (ALLOW_SNAPSHOT_ISOLATION and READ_COMMITTED_SNAPSHOT are set to ON) on the database schema used for the installation.
- During SQL script executions, check the client tool to make sure that its ANSI null default option is set to ON. To do this, you can either use a SET command (set ANSI_NULL_DFLT_ON to ON) or the Query Editor.
- For Windows domain authentication, make sure that you add integratedSecurity=true to the JDBC URL.

**Correcting a Case-Insensitive SQL Server Database Deployment**

Fortify Software Security Center does not support case-insensitive database collation. If you currently use case-insensitive collation of Microsoft SQL Server (SQL Server), you must change to case-sensitive collation. The procedures described here show how to do this.
**Note:** The following procedure on how to export and import the database into the correct collation has been tested and is provided only as a sample. (Altering only the tables collation is not a valid solution.)

To change to case-sensitive collation for SQL Server:

2. Stop the Fortify Software Security Center server.
3. Create a new case-sensitive database and initialize it for your Fortify Software Security Center version.

**Important:** The destination database must be the same version as the source database. If the source is version 2016, then the destination database must be version 2014 version. Use create-tables.sql from 2016 version to create the destination database.

If a previous attempt to migrate failed, review mappings for the columns in which the error occurred. The mapping of source columns and destination columns must be identical, which means that both the column type and column size must be the same.

4. To find out whether the source and destination databases are of different types or sizes, run following query:

```sql
SELECT src.TABLE_NAME,
       src.COLUMN_NAME,
       src.DATA_TYPE,
       src.CHARACTER_MAXIMUM_LENGTH,
       dst.TABLE_NAME,
       dst.COLUMN_NAME,
       dst.DATA_TYPE,
       dst.CHARACTER_MAXIMUM_LENGTH
FROM SOURCE_DB.INFORMATION_SCHEMA.COLUMNS src
INNER JOIN DESTINATION_DB.INFORMATION_SCHEMA.COLUMNS dst
ON dst.TABLE_NAME COLLATE DATABASE_DEFAULT = src.TABLE_NAME COLLATE DATABASE_DEFAULT
AND dst.COLUMN_NAME COLLATE DATABASE_DEFAULT = src.COLUMN_NAME COLLATE DATABASE_DEFAULT
WHERE dst.CHARACTER_MAXIMUM_LENGTH < src.CHARACTER_MAXIMUM_LENGTH
OR dst.DATA_TYPE COLLATE DATABASE_DEFAULT < src.DATA_TYPE COLLATE DATABASE_DEFAULT;
```

5. Change the columns returned by the preceding query to make the destination database the same type and size as the source database.

6. Disable all constraints for all tables in the new database, as follows:

```sql
EXEC sp_MSforeachtable "ALTER TABLE ? NOCHECK CONSTRAINT all"
```

7. Find non-empty tables in the new case-sensitive database as follows:
EXEC sp_MSforeachtable 'IF EXISTS (SELECT 1 FROM ?) PRINT ''?'''

This returns the following tables:
- configproperty
- applicationstate
- databasechangelocklog
- databasechangeloglog
- qrtz_locks

**Note:** The number of returned tables may vary, depending on your Fortify Software Security Center version, but you must still run TRUNCATE on all tables in the next step.

8. Use the TRUNCATE TABLE statement to empty data from the tables returned in step 7.

9. In SQL Server Management Studio, do the following:
   a. Right-click your case-insensitive database, select Tasks, and then select Export Data. The SQL Server Import and Export Wizard starts.
   b. Specify your data source (case-insensitive database) destination, and destination database (case-sensitive database).
   c. On the **Specify Table Copy or Query** step, select **Copy data from one or more tables or views**, and then click **Next**.
   d. On the **Select Source Tables and Views** step, check in all tables (make sure that you select no views).

   **Note:** Views have a different icon associated with them and are often labeled "view." If you include views, the migration takes longer because views are migrated as tables and become tables in the destination database.

   e. Select all tables, and then click **Edit Mappings**.
   f. In the Column Mappings window, select the **Enable identity insert** check box, and then click **OK**.
   g. Check to make sure that you have enough space in your system temp directory. It should be at least as large as the largest table in original Fortify Software Security Center database.
   h. Click **Next**, and then click **Finish** to complete the data export to your case-sensitive database.

   **Important:** Check to make sure that you have enough space in your system temp directory. It should be at least as large as the largest table in the original Fortify Software Security Center database.

10. Make certain that after you export the data, you re-enable all constraints for all tables, as follows:
EXEC sp_MSforeachtable "ALTER TABLE ? WITH CHECK CHECK CONSTRAINT all"

11. Rebuild all indexes as follows:

```sql
DECLARE @TableName VARCHAR(255)
DECLARE @sql NVARCHAR(500)
DECLARE @fillfactor INT
SET @fillfactor = 80
DECLARE TableCursor CURSOR FOR
SELECT OBJECT_SCHEMA_NAME([object_id])+'.'+name AS TableName
FROM sys.tables
OPEN TableCursor
FETCH NEXT FROM TableCursor INTO @TableName
WHILE @@FETCH_STATUS = 0BEGIN
SET @sql = 'ALTER INDEX ALL ON ' + @TableName + ' REBUILD WITH (FILLFACTOR = ' + CONVERT(VARCHAR(3),@fillfactor) + ')
EXEC (@sql)
FETCH NEXT FROM TableCursor INTO @TableName
END
CLOSE TableCursor
DEALLOCATE TableCursor
GO
```

12. After the change from case-insensitive collation to case-sensitive collation is finished, check the memory usage on the server. SQL Server does not release the server after the process is complete, so you must restart SQL server manually.

**See Also**

"Using a Microsoft SQL Server Database" on page 49

**Configuring a MySQL Database**

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

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

MySQL database configuration requires special attention case sensitivity. For additional information, see "Correcting a Case-Insensitive MySQL Database Deployment" on page 54.

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

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

To configure the MySQL options file:

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

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

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

4. In both the `[mysqld]` and `[mysqldump]` sections, set `max_allowed_packet` to 1G.
   If the `[mysqldump]` section is not there, create it.

5. In the `[mysqld]` section, configure the settings in the following table. If a listed setting is not included in the file, add it.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>innodb_log_file_size</code></td>
<td>512M (Fortify recommends 2.5GB or more)</td>
</tr>
<tr>
<td></td>
<td>Set this to approximately 25 to 100 percent of your <code>innodb_buffer_pool_size</code> value. Note, however, that increasing this value increases recovery time.</td>
</tr>
<tr>
<td><code>innodb_lock_wait_timeout</code></td>
<td>300 (recommended) Expressed in seconds</td>
</tr>
<tr>
<td><code>query_cache_type</code></td>
<td>Any non-zero value</td>
</tr>
<tr>
<td><code>query_cache_size</code></td>
<td>Between 64M and 228M</td>
</tr>
<tr>
<td><code>innodb_buffer_pool_size</code></td>
<td>512M (Fortify recommends 10GB or more)</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If you increase this value without also increasing the <code>innodb_log_file_size</code> value, uploads of large FPR files can fail.</td>
</tr>
<tr>
<td>default-</td>
<td>INNODB</td>
</tr>
<tr>
<td>Setting</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>storage-engine</td>
<td></td>
</tr>
<tr>
<td>innodb_file_format</td>
<td>Barracuda</td>
</tr>
<tr>
<td>innodb_large_prefix</td>
<td>1</td>
</tr>
</tbody>
</table>

6. Make sure that MySQL is set up with Barracuda or a newer file format to enable the dynamic row format feature. For more information, see the MySQL documentation for the innodb file format and for dynamic row formats.

7. Save the file.

8. Restart the MySQL server.

Correcting a Case-Insensitive MySQL Database Deployment

Fortify Software Security Center does not support case-insensitive database collation. If you currently use case-insensitive collation of MySQL, you must change to case-sensitive collation. The following procedure describes how to do this.

To change to case-sensitive collation for MySQL:

1. Determine the collation of your current Fortify Software Security Center database. (If the collation is latin1_swedish_ci, the collation of the new database will be latin1_general_cs. If it is utf8_general_ci, the collation of the new database will be utf8_bin.)

2. Using either MySQL Workbench or the MySQL command prompt, create a new database with the correct collation.
   
   For example, if you were upgrading from Fortify Software Security Center 17.10, and the collation of your database is latin1_swedish_ci, then you would use the following command to create a new case-sensitive database:
   
   ```
   CREATE DATABASE `ssc-cs`
   DEFAULT CHARACTER SET latin1
   COLLATE latin1_general_cs;
   ```

3. Using either MySQL Workbench or the MySQL command prompt, run the create-tables.sql script on the new database. Make sure that you run the script for the currently installed Fortify Software Security Center version. For example, if Fortify Software Security Center version 17.10 is currently installed, you would use a command similar to the following:

   ```
   cd /D "D:\HP\Fortify\Software\v17.10\SSC Server\HP-Fortify-Server-WAR\sql\mysql"
   mysql -u root -p ssc-cs < create-tables.sql
   ```
4. After the create-tables.sql script has completed successfully, run the following statements on the new case-sensitive database to clear out five tables that were populated during the script run:

   TRUNCATE TABLE configproperty;
   TRUNCATE TABLE qrtz_locks;
   TRUNCATE TABLE applicationstate;
   TRUNCATE TABLE DATABASECHANGELOG;
   TRUNCATE TABLE DATABASECHANGELOGLOCK;

5. Start the Migration Wizard in MySQL Workbench (Database > Migration Wizard).

6. Click Start Migration.

7. On the Source Selection and Target Selection steps, configure your source and target RDBMS connections, respectively. (Specifying the default schema has no effect on migration).

8. Click Next until you reach the Schema Selection step.

9. Select the source database, and then click Next.

10. On the Source Objects step, select only the Migrate Table objects check box, and then click Next.

11. On the Manual Editing step:
   a. From the View list, select All Objects.
   b. In the Target Object column, click the database name, and then type the name of your case-sensitive target database (for example, ssc-cs).
   c. Click Next.

12. On the Target Creation Options step, clear all three check boxes.

13. Click Next until you reach the Data Transfer Setup step, and then do the following:
   a. Select the Online copy of table data to target RDBMS option.
   b. Under Options, clear both options, and then, in the Worker tasks box, type 1.

14. Click Next.

The data migration begins. Depending on the size of your source database, this may take several hours to complete.

You can now proceed to upgrade Fortify Software Security Center. Make sure that you specify your case-sensitive MySQL database as you configure the database from the Setup wizard. (See “Configuring Fortify Software Security Center After an Upgrade” on page 144.)

Now the case-sensitive database is prepared for upgrade to the newest Fortify Software Security Center version.

See Next

“Configuring a MySQL Database” on page 52
Configuring an Oracle Database

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

Preventing the “No more data to read from socket” Error

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

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

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

About the Fortify Software Security Center Database Tables and the Schema

The Fortify Software Security Center installation directory contains an initialization script for each supported third-party database type. During initial configuration (see "Configuring Fortify Software Security Center for the First Time" on page 70), run this script for your database type to create the database tables and initialize the database schema for Fortify Software Security Center.

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

- "Database User Account Privileges" on page 47
- "Database-Specific Configuration Requirements" on page 48

About Seeding the Fortify Software Security Center Database

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

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

Fortify Software Security Center requires two of the downloaded seed bundles (see "Unpacking and Deploying Fortify Software Security Center Software" on page 44):

- The issue template seed bundle (HP_Fortify_Process_Seed_Bundle_2017_Q3.zip) provides a default admin user account and issue template data.
- The report seed bundle (HP_Fortify_Report_Seed_Bundle_2017_Q3.zip) provides the default set of Fortify Software Security Center reports.
You can also install the optional PCI Basic Bundle (HP_Fortify_PCI_Basic_Seed_Bundle_2017_Q3.zip), which adds a Payment Card Industry process template and an associated report to the default set of Fortify Software Security Center templates and reports.

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 76.

See Also

"Seeding the Database with Seed Bundles Delivered with Quarterly Security Content Releases" on page 151

Permanently Deleting a Fortify Software Security Center Database

To permanently delete a Fortify Software Security Center database schema along with all the data in the database, you run the drop-tables.sql script.

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

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

1. Navigate to the <ssc_install_dir>/sql directory, and open the subdirectory for the third-party database you plan to use with Fortify Software Security Center:
   - db2
   - mysql
   - Oracle
   - sqlserver
2. Copy the drop-tables.sql script from the subdirectory that matches your Fortify Software Security Center database type to the database server or other location where you will run the script.
3. In the database client program, log into the database account you created for use with Fortify Software Security Center.
4. Review the warning in the introduction to this topic.
5. Remove the Fortify Software Security Center database schema and all the data in the database by running the following script:

   drop-tables.sql

LDAP User Authentication

The topics in this section provide information about user authentication in Fortify Software Security Center and configuring LDAP authentication and LDAP server options.
**Note:** For information about how to manage LDAP entities and user roles in Fortify Software Security Center, see "Registering LDAP Entities" on page 176 and "About Managing LDAP User Roles" on page 135.

Topics covered in this section:

- **About Fortify Software Security Center User Authentication** .......................................................... 58
- **Preparing to Configure LDAP Authentication** .......................................................... 58
- **About the LDAP Server Referrals Feature** .......................................................... 59
- **Disabling LDAP Referrals Support** .......................................................... 60

### About Fortify Software Security Center User Authentication

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

Database-only authentication imposes a separate administrative process for creating and managing Fortify Software Security Center user accounts and roles. The default database-only authentication method can be augmented by using LDAP to authenticate users. Most administrators prefer to augment the Fortify Software Security Center default database-only authentication with LDAP. LDAP authentication enables a single administrative process to manage user authentication for multiple network entities, including Fortify Software Security Center. You can configure Fortify Software Security Center to augment its native database-only user authentication with LDAP user authentication.

### Preparing to Configure LDAP Authentication

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

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

2. **Create an LDAP account for Fortify Software Security Center to use.**
   
   If your LDAP server does not permit anonymous binding, create a read-only LDAP account for Fortify Software Security Center to use. Fortify Software Security Center requires an account with permissions necessary to read user attributes and authenticate users. (Even if your LDAP server supports anonymous binding, you may prefer to create an LDAP read-only account for Fortify Software Security Center.)
Note: For information about how to configure the primary source looking up users, see "Configuring Core Settings" on page 87.

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

3. Check for conflicts between account names.

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

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

4. Gather and record required Information.

Review "LDAP Configuration Property Descriptions" on page 297 and record any information you need to configure LDAP authentication. (Note that most of the fields have default values that you can leave in place.)

5. Fortify recommends that you disable the referrals feature.

See "About the LDAP Server Referrals Feature" below and "Disabling LDAP Referrals Support" on the next page.

See Also

"Configuring LDAP Servers" on page 94

About the LDAP Server Referrals Feature

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

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

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

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

To disable referrals support:
1. On the Hewlett Packard Enterprise header, click **Administration**.
2. In the left panel, select **Configuration**, and then select **LDAP Servers**.
3. On the Integration with LDAP servers page, click the LDAP server connection for which you want to disable referrals support.
4. Scroll down to the **Advanced Integration Properties** section.
5. From the LDAP referrals processing strategy list, select **ignore**.
6. Save your changes.
Chapter 4: Deploying Fortify Software Security Center in an Application Server

The topics in this section provide instructions on how to prepare an application server for Fortify Software Security Center deployment, and then deploy Fortify Software Security Center in the application server.

After you deploy Fortify Software Security Center in an application server, complete the configuration tasks in the Administration view in Fortify Software Security Center. For information and instructions, see "Additional Fortify Software Security Center Configuration" on page 76.

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

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

This section contains the following topics:

- About the fortify.home Directory ................................................................. 61
- About Supported Application Servers and Secure Deployment ....................... 62
- About Deploying Fortify Software Security Center in Apache Tomcat .................. 62
- About Deploying Fortify Software Security Center in IBM WebSphere .................. 64
- Deploying Fortify Software Security Center in WebLogic 12c .......................... 68

**About the fortify.home Directory**

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

**Note:** Although the default directory is `<user.home>/.fortify`, you can specify a different directory using the Setup wizard during configuration. (See "Configuring Fortify Software Security Center for the First Time" on page 70.)

**Directory Structure**

The `fortify.home` directory is structured as follows:
<fortify.home>/
  <app_context>/
  conf/
    app.properties
    datasource.properties
    log4j2.xml
    version.properties
  logs/
    ssc.log
    ...
    init.token
  fortify.license
  plugin-framework/

About Supported Application Servers and Secure Deployment

Before you can successfully run Fortify Software Security Center, you must prepare a supported third-party application server for Fortify Software Security Center deployment. For information about the supported application servers and versions, see the HPE Security Fortify Software System Requirements document.

Secure deployment is particularly important for application server configuration, operation, and communications. For information about secure deployment considerations for third-party application servers running Fortify Software Security Center, see "Securing the Application Server" on page 35 and "Setting Application Server Attributes to Protect Sensitive Data in Cookies" on page 35.

About Deploying Fortify Software Security Center in Apache Tomcat

The following topics describe what you need to do to deploy Fortify Software Security Center in an Apache Tomcat application server.

Tomcat Memory Settings

If you intend to use Apache Tomcat as your application server, you must specify the Tomcat server memory settings. This enables Fortify Software Security Center to use several frameworks that dynamically subclass an application's core classes. Dynamic subclassing requires an increased number of class definitions in the Java runtime's permanent memory heap.

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

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

About Configuring the Tomcat Connectors

Configure the Tomcat connectors and ports, as necessary. See the Tomcat documentation for instructions for configuring the connectors and setting up SSL/TLS (if required).

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

See Next

"Deploying Fortify Software Security Center in Tomcat" below

Configuring Tomcat to Unpack WAR Files

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

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

For information about how to set the unpackWars attribute, see:


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

Deploying Fortify Software Security Center in Tomcat

To deploy Fortify Software Security Center in Tomcat:

1. Stop the Tomcat server.
2. Navigate to the <tomcat>/webapps directory.
3. Delete the ssc subdirectory.
4. Copy the ssc.war file to the <tomcat>/webapps directory.

Note: It could take several minutes for Tomcat to deploy the ssc.war file.

5. Restart the Tomcat server:

   - On a Linux system, run <tomcat>/bin/startup.sh.
About Deploying Fortify Software Security Center in IBM WebSphere

To deploy Fortify Software Security Center in IBM WebSphere Application Server (WAS), perform the tasks listed in the following table.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Export a copy of the HPE Security web certificate in X.509 DER format.</td>
<td>&quot;About Security Website Certificates for WebSphere&quot; below</td>
</tr>
<tr>
<td>2</td>
<td>Use IBM’s iKeyman utility to add the HPE Security web certificate to the WAS certificate store.</td>
<td>&quot;Adding a Fortify Website Certificate to IBM WebSphere&quot; on page 66</td>
</tr>
<tr>
<td>4</td>
<td>Deploy Fortify Software Security Center in WAS.</td>
<td>&quot;Deploying Fortify Software Security Center in IBM WebSphere&quot; on page 67</td>
</tr>
</tbody>
</table>

About Security Website Certificates for WebSphere

The Fortify website certificate enables the Fortify Software Security Center instance running under the WebSphere server to establish an HTTPS connection with the HPE Security Rulepack update server at https://update.fortify.com.

The following procedures describe how to export a copy of the security certificate in X.509 DER format using a Firefox or Internet Explorer web browser:

**Exporting a Fortify Website Certificate Using Firefox** .......................................................... 64

**Exporting a Fortify Website Certificate Using Internet Explorer** ............................................. 65

**Exporting a Fortify Website Certificate Using Firefox**

To export a Fortify website certificate using Firefox:

1. In Firefox, navigate to the Fortify Customer Portal (https://update.fortify.com), and then log in using your Customer Portal credentials.
   The **Your Products** page opens.
2. Open the certificate export tool:
a. Right-click the page, and select View Page Info from the shortcut menu. Firefox displays the Page Info window.
b. In the Page Info window, click Security.
c. In the Website Identity section, click View Certificate.
d. In the Certificate Viewer dialog box, click the Details tab.
e. Click Export.

3. In the Save Certificate to File dialog box:
   a. Browse to the directory to which you want to save the certificate file.
   b. In the File Name box, type a file name, and make a note of the name.
   c. In the Save as type list, leave X.509 Certificate (PEM) selected.

4. Click Save.

5. Close the Certificate Viewer dialog box.

See Next

"Adding a Fortify Website Certificate to IBM WebSphere" on the next page

Exporting a Fortify Website Certificate Using Internet Explorer

To export a Fortify website certificate using Internet Explorer:

1. From Internet Explorer, navigate to the Fortify Customer Portal (https://update.fortify.com), and then log in using your Customer Portal credentials.
   The Your Products page opens.

2. To open the Certificate Export Wizard:
   a. Right-click the page, and select Properties from the shortcut menu.
   b. In the Properties dialog box, click Certificates.
   c. In the Certificate dialog box, click the Details tab, and then click Copy to File.
      The Certificate Export Wizard starts.

3. To export the certificate as an X.509 DER file:
   a. Click Next.
   b. On the Export File Format step, leave DER Encoded Binary X.509 (.CER) selected and click Next.
   c. On the Export to File step, browse to the directory to which you want to save the certificate file, type a file name, and then click OK.
   d. Click Next.
   e. On the completion step, review your settings.
   f. Click Finish.

See Next

"Adding a Fortify Website Certificate to IBM WebSphere" on the next page
Adding a Fortify Website Certificate to IBM WebSphere

After you export a Fortify website certificate, use IBM’s iKeyman utility to add the HPE Security web certificate to the certificate store of the WAS, as follows:

1. Start the IBM key management utility (iKeyman). For instructions, see IBM’s online documentation for certificate management.
2. To open the WAS key store for updating:
   a. From the **Key Database File** menu, select **Open**.
   b. From the **Key database type** list in the Open dialog box, select **PKCS12**.
   c. Browse to the following location: `<WebSphere_Install Dir>/profiles/<AppServer>/config(cells/<Cell/Node Name>/Nodes/<Node Name>/trust.p12.`
   d. Click **OK**.
      The iKeyman utility prompts for a password.
3. Type the WAS keystore password. (The default password is WebAS.)
4. To add the HPE Security web certificate:
   a. Click **Add**.
   b. Browse to and select the HPE Security web certificate you downloaded (see "About Security Website Certificates for WebSphere" on page 64), and then click **OK**.
   The iKeyman utility prompts you to label the certificate.
   c. The **Enter a Label** box displays the default label **ssc_war**. Replace this value with **ssc**.
   d. Click **OK**.
      The iKeyman utility adds the HPE Security web certificate to the WAS certificate store.
5. In the iKeyman utility **Key Database File**, click **Exit**.

**See Next**

"Preparing IBM WebSphere Application Server for Fortify Software Security Center Deployment" below

Preparing IBM WebSphere Application Server for Fortify Software Security Center Deployment

After you export the Fortify web certificate and add it to WebSphere Application Server (WAS), prepare WAS for Fortify Software Security Center deployment, as follows:

1. Set SDK (a supported version) as the default runtime configuration for WAS.
2. Start WAS and log in as an administrator.
3. Open the WAS console.
4. Navigate to **Application Servers > <server_name> > Web Container > Custom properties** where `<server_name>` is the server that contains the Fortify Software Security Center application. For example, server1.
5. Add the following property to the server web container:

   ```properties
   com.ibm.ws.webcontainer.invokefilterscompatibility
   ```

6. Set the value of the new property to true.

   **Caution!** If you do not set this property, logging fails. Errors are logged to `logs/ffdc/<filename>.txt`.

7. On the Application servers page (for example, Application servers > server1), in the server-specific application settings, set "Class loading mode" = Parent last.

   **Note:** You may want to set `-Xmx` to a higher value, depending on the amount of available memory and your needs. For information, see the WebSphere Application Server documentation.

8. Save your changes.
9. Restart WAS.

See Next

"Deploying Fortify Software Security Center in IBM WebSphere" below

Deploying Fortify Software Security Center in IBM WebSphere

To deploy Fortify Software Security Center using the WAS console:

1. Start WAS and log in to the administrative console.
2. In the navigation tree, select Applications > Application Types > Websphere enterprise applications.
3. In the Enterprise Applications view, click Install.
4. Navigate to and select the ssc.war file, and then continue the installation process.
5. Update the context root (for example /ssc), which is empty by default.
6. In the Name field in the General Properties area of the panel on the right, type ssc.war.
7. In the Modules area, navigate to Enterprise applications > <ssc_application>, and then click Manage Modules.
8. Select the Fortify Software Security Center application module.
9. In the Class loader order list, select Classes loaded with application class loader first (parent last).
10. Click Apply.
11. Navigate to Enterprise applications > <ssc_application> > Class loading and update detection.
12. In the Polling interval for updated files field, type 20.
13. In the Class loader order list, select Classes loaded with application class loader first (parent last).
14. Click OK.
15. Restart WAS.

## Deploying Fortify Software Security Center in WebLogic 12c

To deploy Fortify Software Security Center in WebLogic 12c:

**Note:** For the supported versions of WebLogic 12c, see the HPE Security Fortify Software System Requirements document.

1. Stop the WebLogic Server.
2. Navigate to the WebLogic Server `<WebLogic_Install>/user_projects/domains/ssc/bin` directory and open the `setDomainEnv.cmd` (Windows) or `setDomainEnv.sh` (Linux) batch script file in a text editor.
3. On a Windows system, add:
   ```
   set USER_MEM_ARGS=-Xmx4096m -XX:MaxPermSize=256m
   
   **Note:** You may want to set `-Xmx` to a higher value, depending on the amount of memory available and your needs. For information, see the WebLogic Application Server documentation.
   ```
   ```
   set JAVA_OPTIONS=-Djava.awt.headless=true
   ```
4. On a Linux system, add the following lines to the head of the file:
   ```
   export USER_MEM_ARGS="-Xmx4096m -XX:MaxPermSize=256m"
   
   **Note:** You may want to set `-Xmx` to a higher value, depending on the amount of memory available and your needs. For information, see the application server documentation.
   ```
   ```
   export JAVA_OPTIONS=-Djava.awt.headless=true
   ```
5. Navigate to the WebLogic Server `<WebLogic_Install>/user_projects/domains/ssc/config` directory and open the `config.xml` file in a text editor.
6. In the `<security-configuration>` element, add the following:
   ```
   <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>
   ```
7. Start the WebLogic server.
8. To start the Administration Console for your local instance of WebLogic Server, type the following URL in a Web browser address field:
   ```
   http://localhost:7001/console/
   ```
9. Log in to the Administration Console.
10. In the Domain Structure tree, select **Deployments**.
11. Click **Install**.
12. Browse to and select the `ssc.war` file.
13. Select **Install this deployment as an application**.
14. Click **Next** until the final step is displayed, and then click **Finish**.
Chapter 5: Configuring Fortify Software Security Center for the First Time

After you deploy Fortify Software Security Center in your application server for the first time and then enter the Fortify Software Security Center URL in a browser window, the Fortify Software Security Center Setup wizard (Setup wizard) opens. Here, you can complete the steps for the initial server configuration. The Setup wizard is available to administrators only after you first deploy Fortify Software Security Center, after you upgrade it, or after you place Fortify Software Security Center in maintenance mode (see “Placing Fortify Software Security Center in Maintenance Mode” on page 139).

To configure Fortify Software Security Center for the first time:

1. After you deploy a new version of the Fortify Software Security Center WAR file in your application server, open a browser window and type your Fortify Software Security Center server URL (https://<host_IP>:<port>/<app_context>/).
2. In the upper right corner of the web page, click Administrators.
3. Go to the <fortify.home><app_context> directory, and open the init.token file in a text editor.
4. Copy the contents of the init.token file to the clipboard.
5. On the web page, paste the string you copied from the init.token file into the text box, and then click Sign in.
   The Fortify Software Security Center Setup wizard opens.
6. Read the information on the Start page of the Setup wizard, and then click Next.
7. On the **Configuration** step, under **Upload Fortify license**, do the following:
   a. Click **Upload**.
   b. From the Upload Fortify license dialog box, browse to and select your fortify.license file, and then click **Upload**.

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

   The right panel displays the default path of the configuration directory in which your configuration files (app.properties, datasource.properties and version.properties) are to reside.

8. To save your configuration properties file in a directory other than the default shown, on the application server on which Fortify Software Security Center is deployed, specify a different path for the JVM system property **fortify.home**.

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

9. Read the warning note about sensitive information in the configuration file directory, and then select the **I have read and understood this warning** check box.

10. Click **Next**.

11. On the **Core Configuration Settings** step, do the following:
   a. In the **Fortify Software Security Center URL** box, type the URL for your **Fortify Software Security Center** server.
   b. In the center panel, select the **Enable HTTP host header validation** check box to ensure that the HTTP Host header value matches the value configured in the Fortify Software Security Center URL (host.url property). Both the host and port must match. This affects both browsers and direct REST APIs access. If validation is turned off, any HTTP Host header can access Fortify Software Security Center.
   c. To enable global searches in Fortify Software Security Center, select the **Enable global Search** check box, and then, in the box below, type the directory path for search index files. Fortify Software Security Center indexes data to this location. (Passwords are not indexed.)

   **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.

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

12. In the **Global Search** panel, read the warning, and then select the **I have read and understood this warning** check box.

13. Click **Next**.

14. On the **Datasource** step, do the following:
a. In the **Database type** box, select the database type you are using with Fortify Software Security Center.

b. In the **Database username** box, type the username for your Fortify Software Security Center database. For more information, see "Database User Account Privileges" on page 47.

   **Note:** Make sure that the database user credentials specified in the **Database username** and **Database password** fields are for a user account that has the privileges required to execute migration scripts. These privileges are described in "Database User Account Privileges" on page 47.

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.

   **Important:** If you are using MySQL Server database, you must append the following property setting to the end of the URL: `connectionCollation=COLLATION` where `COLLATION` is the collation type of your database.

   **Examples:**
   
   jdbc:mysql://localhost:3306/ssc?connectionCollation=utf8_bin
   jdbc:mysql://localhost:3306/ssc?connectionCollation=latin1_general_cs

   **Important:** If you are using an IBM DB2 database, you must include the following property settings in the URL:
   
   progressiveStreaming=2
   fullyMaterializeInputStreams=true
   allowNextOnExhaustedResultSet=1

   **Example:**
   
   jdbc:db2://mydb2database:50000/fortifydb:progressiveStreamin=2;fullyMaterializeInputStreams=true;allowNextOnExhaustedResultSet=1;

e. In the **Maximum idle connections** box, type the maximum number of idle connections that can remain in the pool. The default value is 50.

f. In the **Maximum active connections** box, type the maximum number of active connections that can remain in the pool. The default value is 100.

g. In the **Maximum wait time (ms)** box, type the maximum number of milliseconds for the pool to wait for a connection (when no connections are available) before the system throws an exception. The default value is 60000. To extend the wait indefinitely, set the value to zero (0).

h. To test your settings, click **Test Connection**.

15. Before you continue on to the **Database Seeding** step, run the `create-tables.sql` script. For instructions, see "About the Fortify Software Security Center Database Tables and the Schema" on page 56.

16. After you initialize the database, click **Next**.
17. On the **Database Seeding** step, do the following:
   a. In the left panel, use **Browse** to locate and select your HP_Fortify_Process_Seed_Bundle_2017_Q3.zip file, and then click **Seed Database**.
   b. Use **Browse** to locate and select your HP_Fortify_Report_Seed_Bundle_2017_Q3.zip file, and then click **Seed Database**.
   c. (Optional) Use **Browse** to locate and select your HP_Fortify_PCI_Basic_Seed_Bundle_2017_Q3.zip file, and then click **Seed Database**.

18. Click **Next**.

19. Click **Finish**.

20. Restart your application server.

21. Back up your ssc.war file. This enables you to import your settings if and when you upgrade to a later release.

After you finish the initial Fortify Software Security Center configuration, complete the configuration of the core parameters and configure additional settings in the Administration view. (For information about the Administration view, see "Additional Fortify Software Security Center Configuration" on page 76.)

**Note:** If you later find that you need to change any of the configuration settings, you can place Fortify Software Security Center in maintenance mode, and then make any necessary changes. For instructions on how to place Fortify Software Security Center in maintenance mode, see "Placing Fortify Software Security Center in Maintenance Mode" on page 139.
Chapter 6: Logging in to Fortify Software Security Center

After you create and initialize your Fortify Software Security Center database, configure your application server, and deploy Fortify Software Security Center in the application server, log in to Fortify Software Security Center.

**Important:** After you log in, create at least one non-default administrator account, and then delete the default administrator account. For more information about how to manage Fortify Software Security Center user accounts and roles, see "About Fortify Software Security Center User Administration" on page 131.

To log in to Fortify Software Security Center:

1. In a web browser, type the URL for your Fortify Software Security Center instance:
   - If Fortify Software Security Center is configured to use secure HTTPS protocol, type the following URL:
     
     https://<host_IP>:<port>/<ssc>/
   
   where `<port>` represents the port number used by the application server and `<ssc>` is the context root name.

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

   - If Fortify Software Security Center is configured to use insecure HTTP protocol (not recommended), type the following URL:
     
     http://<host_IP>:<port>/<ssc>/
   
   where `<port>` represents the port number used by the application server and `<ssc>` is the context root name.

2. Type your username and password.
   - If you are logging on to Fortify Software Security Center for the first time, type `admin` in both the **Username** and **Password** boxes. These are the default credentials for a new installation.

   **Note:** You are asked to change your credentials the first time you log in.

3. Click **Log in**.
   - If you are logging on to Fortify Software Security Center for the first time, you are prompted to change your password.
4. If Fortify Software Security Center prompts you to change your password, enter a new one. Passwords must be at least eight characters long and contain at least one of each of the following:

- Upper-case letter
- Lower-case letter
- Non-alphanumeric character

**See Next**

"Additional Fortify Software Security Center Configuration" on page 76
Chapter 7: Additional Fortify Software Security Center Configuration

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

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

This section contains the following topics:

Accessing the Configuration Settings in the Administration View .................................................76
Configuring Issue Stats Thresholds ........................................................................................................77
Configuration Options Available in the Administration View ..........................................................78

Accessing the Configuration Settings in the Administration View

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

To access the Configuration category:

1. Log in to Fortify Software Security Center as an administrator user. For log-in instructions, see "Logging in to Fortify Software Security Center" on page 74.
2. Do one of the following:
   - If you are accessing Fortify Software Security Center for the first time, a banner similar to the following is displayed at the top of the page. Click Go to open the Configuration category in the Administration view.

   ![This is either a fresh installation or a newly migrated instance of Software Security Center. Please see the Configuration section on the Administration page.](image)

   Otherwise,
   - On the Hewlett Packard Enterprise header, click Administration.

     The Administration view opens. The navigation panel on the left displays links to the categories that are available in the Administration view. The event logs page is displayed
b. In the navigation panel, click **Configuration**.

The panel displays the configuration category options. For information about these options, see "Configuration Options Available in the Administration View" on the next page.

## Configuring Issue Stats Thresholds

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

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

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

1. On the Hewlett Packard Enterprise header, select **Administration**.
2. In the left panel, select **Metrics & Tracking**, and then select **Issue Age**.

   The Issue Age page opens. The minimum and maximum values for **Average Days to Review** and **Average Days to Remediate** are set to 100 and 365, respectively.
3. To reset the thresholds for the average number of days to review Issues, under for **Average Days to Review**, do one of the following:
   - Adjust the slider control.
   - Change the values shown in the Min. and Max. combo boxes.

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

5. Click **Save**.
   The color coded values on the Issue Stats dashboard page reflect your changes.

**Configuration Options Available in the Administration View**

The following table lists the configuration options available in the Administration view. (On the Hewlett Packard Enterprise header, select **Administration**. Then, in the left panel, select **Configuration**.)

**Note:** Changes to some configuration options do not take effect until the system is restarted.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Assistant</td>
<td>Use to enable and configure Audit Assistant, which uses Fortify Scan Analytics to automatically audit Fortify Static Code Analyzer scans.</td>
<td>&quot;Configuring Audit Assistant&quot; on page 83</td>
</tr>
<tr>
<td>BIRT Reports</td>
<td>Use to apply enhanced security to reporting in Fortify Software Security Center.</td>
<td>&quot;Configuring Security for BIRT Reporting&quot; on page 84</td>
</tr>
<tr>
<td>CloudScan</td>
<td>Use to configure Fortify Software Security Center to monitor CloudScan and to display CloudScan results in Fortify Software Security Center.</td>
<td>&quot;Configuring CloudScan Monitoring in Fortify Software Security Center&quot; on page 86</td>
</tr>
<tr>
<td>Core</td>
<td>Use to configure core Fortify Software Security Center settings such as the timeout and lockout settings and the proxy for secure coding Rulepacks updates.</td>
<td>&quot;Configuring Core Settings&quot; on page 87</td>
</tr>
<tr>
<td>Email</td>
<td>Use to configure the server settings used to send email alerts to users.</td>
<td>&quot;Configuring Email Alert Notification Settings&quot; on page 91</td>
</tr>
<tr>
<td>Issue Audit</td>
<td>Use to select the setting that determines how issue audit conflicts are resolved.</td>
<td>&quot;Setting the Strategy for Resolving Issue Audit Conflicts&quot; on page 243</td>
</tr>
<tr>
<td>JMS</td>
<td>Use to configure Fortify Software Security Center to publish system events to the Java Message Service (JMS).</td>
<td>&quot;Configuring Java Message Service Settings&quot; on page 93</td>
</tr>
<tr>
<td>LDAP Servers</td>
<td>Use to configure LDAP authentication and LDAP server options for one or more LDAP servers.</td>
<td>&quot;Configuring LDAP Servers&quot; on page 94</td>
</tr>
<tr>
<td>Maintenance Mode</td>
<td>If, at any time, you need to change any server configuration settings, you can place Fortify Software Security Center</td>
<td>&quot;Placing Fortify Software Security Center in Maintenance Mode&quot; on page 139</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Instructions</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>in maintenance mode, and then make the necessary changes.</td>
<td></td>
</tr>
<tr>
<td>NetWeaver</td>
<td>Use to configure the Fortify Software Security Center connection to NetWeaver.</td>
<td>&quot;About the SAP NetWeaver Plugin for Fortify Software Security Center&quot; on page 108</td>
</tr>
<tr>
<td>Runtime</td>
<td>Use to enable or disable Runtime Application Protection communications with Fortify Software Security Center.</td>
<td>&quot;Configuring Fortify Runtime Application Protection Communication Settings&quot; on page 110</td>
</tr>
<tr>
<td>Scheduler</td>
<td>Use to configure the Fortify Software Security Center job scheduler settings.</td>
<td>&quot;Configuring Job Scheduler Settings&quot; on page 111</td>
</tr>
<tr>
<td>Seed Bundles</td>
<td>Use to seed the database with seed bundles distributed in a quarterly security content release.</td>
<td>&quot;Seeding the Database with Seed Bundles Delivered with Quarterly Security Content Releases&quot; on page 151</td>
</tr>
<tr>
<td>SSO</td>
<td>Use to configure Fortify Software Security Center to work with one of the following SSO solutions:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Central Authentication Server (CAS)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SPNEGO/Kerberos</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SAML SSO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- HTTP SSO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- X.509 SSO</td>
<td></td>
</tr>
<tr>
<td>Web Services</td>
<td>Use to configure Fortify Software Security Center web services.</td>
<td>&quot;Configuring Web Services to Require Token Authentication&quot; on page 124</td>
</tr>
</tbody>
</table>
About Audit Assistant

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

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

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

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

Audit Assistant Workflow

The workflow for using Audit Assistant is as follows:

1. Obtain a Fortify Scan Analytics account, as follows:
b. Click **Need an Account?**

c. Complete the fields on the Request a Fortify Scan Analytics Tenant form, and then click **Request Now.**

Fortify sends an email with information about how to connect to Fortify Scan Analytics.

1. From Fortify Scan Analytics, create one or more classifiers.
2. From Fortify Scan Analytics, create one or more policies.
3. (Optional) Choose to share anonymous metadata.
4. Obtain a Fortify Scan Analytics token.
5. From Fortify Software Security Center, configure and test the connection to Fortify Scan Analytics.
6. From Fortify Software Security Center, open an application version, and submit the latest completely audited scan to Audit Assistant. This step is referred to as **training.**
7. From Fortify Software Security Center, open an application version and submit its Fortify Static Code Analyzer scan results to Audit Assistant.
8. After Audit Assistant completes its assessment, view those results and, if necessary, adjust them.
9. Submit corrected results to Audit Assistant.

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

**See Also**

*Configuring Audit Assistant* on the next page

*About Classifiers and Prediction Policies* on page 260

*Defining Classifiers* on page 260

*Defining a Catch-All Classifier* on page 264

*Defining Prediction Policies* on page 264

*Enabling Metadata Sharing* on page 266

*Submitting Training Data to Audit Assistant* on page 266

*Reviewing Audit Assistant Results* on page 267

**Getting a Fortify Scan Analytics Authentication Token**

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

To obtain a Scan Analytics authentication token:

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

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

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Required</td>
<td>Description</td>
</tr>
<tr>
<td>Automated Auditing</td>
<td></td>
</tr>
<tr>
<td>Enable Audit Assistant</td>
<td>Select this check box to enable the remaining fields.</td>
</tr>
<tr>
<td>* Authentication token</td>
<td>Paste the authentication token you obtained from Fortify Scan Analytics here. For instructions on how to get a token, select How do I get a token? or, see &quot;Getting a Fortify Scan Analytics Authentication Token&quot; on the previous page.</td>
</tr>
<tr>
<td>Server Connection Settings</td>
<td></td>
</tr>
<tr>
<td>*Audit Assistant server URL</td>
<td>Specify the URL for the Fortify Scan Analytics server.</td>
</tr>
<tr>
<td>Use SSC proxy</td>
<td>Select this check box to enable proxy.</td>
</tr>
</tbody>
</table>

4. To test the connection to the Application Security Analytics server, click Test Connection.
5. Click Save.
After the connection is successfully tested, Fortify Software Security Center adds the Prediction Policy section.

6. From the Prediction policy name list, select the name of the prediction policy to apply to all application versions. (The policy is defined in Scan Analytics.)

Configuring Security for BIRT Reporting

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

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

**Note:** Fortify Software Security Center cannot run reports with WebSphere Application Server (WAS) JRE while SSL is enabled. For more Information, see "About Using HTTPS and SSL Communications" on page 36.

To enable Java Security manager:

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

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

5. Click Save.

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 report.
2. For the new user account, enable read (only) access to the following tables and views:

<table>
<thead>
<tr>
<th>Tables</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>activity</td>
<td>filterset</td>
<td>requirement</td>
</tr>
<tr>
<td>activitycomment</td>
<td>folder</td>
<td>requirementcomment</td>
</tr>
<tr>
<td>activityinstance</td>
<td>foldercountcache</td>
<td>requirementinstance</td>
</tr>
</tbody>
</table>
3. Log in to Fortify Software Security Center as an administrator.
4. On the Hewlett Packard Enterprise header, click Administration.
5. In the left panel, select Configuration, and then click BIRT Reports.
   Fortify Software Security Center displays the BIRT Reports page.
6. In the DB Username and DB Password boxes, type the credentials for the database account that has read-only database access.
7. To test the database user account access to the database, click Test Connection.
8. Click Save.

See Also

"Allocating Memory for Report Generation" below

"Setting Report Generation Timeout" on the next page

Allocating Memory for Report Generation

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

1. On the Hewlett Packard Enterprise header, select Administration.
2. In the left panel, select Configuration, and then click BIRT Reports.
3. In the Set up BIRT execution section, select the default value in the **Maximum heap size (MB)** box, and then type a new value. (For minimum and recommended values for java heap size, see the *HPE Security Fortify Software System Requirements* document.)

4. Click **Save**.

**Setting Report Generation Timeout**

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

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

**Configuring CloudScan Monitoring in Fortify Software Security Center**

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

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

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

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

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

## Configuring Core Settings

In addition to the initial configuration you performed on the Setup wizard, you must also configure several core attributes in the **Configuration** section of the Administration view. These attributes include user account timeout and lockout settings, the display of user information, maximum events per Fortify WebInspect Agent issue, the base URL for the runtime event description server, and the user administrator's email address. You also configure the proxy used for Rulepack updates on this page. For information about the Rulepacks updates proxy, see "About Configuring a Proxy for Rulepack Updates" on page 90.

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

1. Log in to Fortify Software Security Center as an administrator, and then, on the Hewlett Packard Enterprise header, click **Administration**.
2. In the left panel of the Administration view, select **Configuration**, and then select **Core**. The **Core** page opens.
3. Configure the settings described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absolute session timeout (minutes)</td>
<td>Number of minutes a user can be continuously active before Fortify Software Security Center automatically logs a user off. The default value is 240.</td>
</tr>
<tr>
<td>Days before password reset</td>
<td>Number of days the Fortify Software Security Center password is valid before the user must change it. The default value is 30.</td>
</tr>
<tr>
<td>Login attempts before lockout</td>
<td>Number of times a user can try to log in to Fortify Software Security Center using invalid credentials before Fortify Software Security Center locks the user's account. If Fortify Software Security Center locks a user out, that user is prevented from attempting a new logon for the number of minutes specified in the <strong>Lockout time (minutes)</strong> box.</td>
</tr>
</tbody>
</table>

**Note:** For information about how to unlock a user account, see "Unlocking User Accounts (Local Users Only)" on page 179. The default value is 3.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lockout time (minutes)</strong></td>
<td>If a user attempts and fails to log in to Fortify Software Security Center the number of times specified for <strong>Login Attempts before Lockout</strong>, Fortify Software Security Center locks the user account for the number of minutes specified in the <strong>Lockout time (minutes)</strong> box. The default value is 30.</td>
</tr>
<tr>
<td><strong>User lookup strategy</strong></td>
<td>If LDAP is enabled, select one of the following user lookup strategies from this list:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Local users first, fallback to LDAP users (compatibility)</strong></td>
</tr>
<tr>
<td></td>
<td>Search local users first, then search LDAP users. To avoid potential authorization errors and user confusion, make sure that usernames are not duplicated on the LDAP server and local storage.</td>
</tr>
<tr>
<td></td>
<td>- <strong>LDAP users first, fallback to local users</strong></td>
</tr>
<tr>
<td></td>
<td>Search LDAP users first, then local users. To avoid potential authorization errors and user confusion, make sure that user names are not duplicated on the LDAP server and local storage.</td>
</tr>
<tr>
<td></td>
<td>- <strong>LDAP users exclusive, fallback to local administrator</strong></td>
</tr>
<tr>
<td></td>
<td>(Recommended strategy for SSO) Search LDAP users only, and allow local administrator access.</td>
</tr>
<tr>
<td><strong>Display user first/last names and emails in user fields, along with login names</strong></td>
<td>Select this check box to display the following user information, when applicable: login name, first and last names, and email address. This check box is selected by default.</td>
</tr>
<tr>
<td><strong>Maximum events per WebInspect Agent Issue</strong></td>
<td>Determines the maximum number of events to log within a single Fortify WebInspect Agent issue. After that threshold is reached, new events related to the same issue are ignored.</td>
</tr>
<tr>
<td><strong>Inactive session timeout</strong></td>
<td>Type the number of minutes a user can be inactive before Fortify Software Security Center automatically logs the user off. The default value is 30.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>(minutes)</td>
<td></td>
</tr>
<tr>
<td>Locale for Rulepacks</td>
<td>Type one of the following:</td>
</tr>
<tr>
<td></td>
<td>en (English)</td>
</tr>
<tr>
<td></td>
<td>ja (Japanese)</td>
</tr>
<tr>
<td></td>
<td>zh_CN (simplified Chinese)</td>
</tr>
<tr>
<td></td>
<td>zh_TW (traditional Chinese)</td>
</tr>
<tr>
<td></td>
<td>es (Spanish)</td>
</tr>
<tr>
<td></td>
<td>pt_BR (Portuguese Brazilian)</td>
</tr>
<tr>
<td>Proxy for Rulepack update</td>
<td>Type the network name or IP address proxy.</td>
</tr>
<tr>
<td>Proxy port</td>
<td>Type the port number associated with the network name or IP address</td>
</tr>
<tr>
<td></td>
<td>you specified as the Proxy for Rulepack Update.</td>
</tr>
<tr>
<td>Proxy username</td>
<td>Type a valid username for the Rulepack proxy server.</td>
</tr>
<tr>
<td>Proxy password</td>
<td>Type a valid password for the Rulepack proxy server.</td>
</tr>
<tr>
<td>Rulepack update URL</td>
<td>Important: Do not change the default value of the Rulepack Update URL</td>
</tr>
<tr>
<td></td>
<td>field unless your HPE Security Technical Support</td>
</tr>
<tr>
<td></td>
<td>(<a href="https://support.fortify.com">https://support.fortify.com</a>) representative directs you to do so.</td>
</tr>
<tr>
<td></td>
<td>The default value is <a href="https://update.fortify.com">https://update.fortify.com</a>.</td>
</tr>
<tr>
<td>Base URL for runtime</td>
<td>The runtime event details include a link to a description of the event</td>
</tr>
<tr>
<td>event description server</td>
<td>category, which is hosted on a Fortify Software Security Center instance.</td>
</tr>
<tr>
<td></td>
<td>If you do not want your Fortify Software Security Center instance to</td>
</tr>
<tr>
<td></td>
<td>access the Internet, change the base URL for the event category</td>
</tr>
<tr>
<td></td>
<td>descriptions.</td>
</tr>
<tr>
<td></td>
<td>The default value is</td>
</tr>
</tbody>
</table>
|                           |   https://content.fortify.com/products/360/rtadecription
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ns/</td>
<td></td>
</tr>
<tr>
<td>User Administrator's email address (for user account requests)</td>
<td>Type the email address of the user who is to receive system email alerts and notifications when email notifications are enabled. Requests for new user accounts are sent to this address when the Can't access or need an account? link is available on the Fortify Software Security Center login page.</td>
</tr>
<tr>
<td>Disable 4.30 legacy UI</td>
<td>Select this check box to make the legacy (v4.30) user interface unavailable to users.</td>
</tr>
<tr>
<td>Enable export to CSV</td>
<td>Clear this check box to prevent users from exporting Fortify Software Security Center data to comma-separated values files. <strong>Note:</strong> If you are changing only this property on the Core page, a server restart is not required to implement the change.</td>
</tr>
</tbody>
</table>

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

**See Also**

"Unlocking User Accounts (Local Users Only)" on page 179

**About Configuring a Proxy for Rulepack Updates**

By default, Fortify Software Security Center downloads the current versions of HPE Security Fortify Secure Coding Rulepacks you subscribe to from the HPE Security Fortify Customer Portal at [https://update.fortify.com](https://update.fortify.com). For installations that do not permit downloads directly from an external network source, you can configure Fortify Software Security Center to download Rulepacks from a proxy server.

To configure a proxy for Rulepack updates, you need the following:

- A current subscription to one or more Secure Coding Rulepacks
- The URL, port number, and username for the proxy server to use to update Secure Coding Rulepacks

You configure a proxy for secure coding Rulepacks updates in the Configuration category in the Fortify Software Security Center Administration view. For instructions, see "Configuring Core Settings" on page 87.
Configuring Email Alert Notification Settings

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

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

For information about alerts and how to configure Fortify Software Security Center to send alerts as email alert notifications, see "Enabling and Disabling Receipt of Email Alerts" on page 159.

To configure the settings used for sending email alert notifications:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Hewlett Packard Enterprise header, select Administration.
2. In the left panel, select Configuration, and then select Email.
   The Email service configuration attributes page opens.
3. Configure the settings as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable email</td>
<td>Select this check box to enable Fortify Software Security Center to send email messages of all types and to add the &quot;Can't access or need an account?&quot; link to the login dialog box. This check box is cleared by default.</td>
</tr>
<tr>
<td>From email address</td>
<td>Type the email address that Fortify Software Security Center uses to identify emails sent from Fortify Software Security Center. For example, <a href="mailto:fortifyserver@example.com">fortifyserver@example.com</a>.</td>
</tr>
<tr>
<td>Default encoding of the email content</td>
<td>Type the encoding method to be used for the email content. The default value is UTF-8.</td>
</tr>
<tr>
<td>SMTP server</td>
<td>Type the SMTP server location. For example, mail.example.com.</td>
</tr>
<tr>
<td>SMTP server port</td>
<td>Type the port number for the SMTP server. The default value is 25.</td>
</tr>
<tr>
<td>SMTP username</td>
<td>If authentication is required on the SMTP server, type the SMTP username.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>SMTP password</td>
<td>If authentication is required on the SMTP server, type the SMTP password.</td>
</tr>
<tr>
<td>Enable SSL/TLS encryption</td>
<td>Select this check box to enable communications security using SSL and TLS protocols.</td>
</tr>
<tr>
<td>Trust the certificate provided by the SMTP server</td>
<td>Select this check box to always treat the specified SMTP server certificate as trusted.</td>
</tr>
</tbody>
</table>

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

**Setting the Strategy for Resolving Issue Audit Conflicts**

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

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

**Example of the default strategy for resolving audit conflicts:**

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

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

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

On a different 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. Log in to Fortify Software Security Center as an administrator.
2. On the Hewlett Packard Enterprise header, select Administration.
3. In the left panel, select Configuration, and then select Issue Audit.
   The Issue Audit page opens.
4. From the Issue Audit list, select one of the following:
   - Conflicts are resolved in favor of the SSC changes
   - Conflicts are resolved in favor of the most recent changes
5. Click Save.

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

**See Also**

"About Current Issues State" on page 242

**Configuring Java Message Service Settings**

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

To configure JMS settings:

1. On the Hewlett Packard Enterprise header, select Administration.
2. In the left panel of the Administration view, select Configuration, and then select JMS.
3. The JMS Integration Attributes page opens.
4. Configure the settings as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish system events to JMS</td>
<td>Select this check box to publish system events to JMS.</td>
</tr>
<tr>
<td>JMS server URL</td>
<td>Type the URL for the JMS server.</td>
</tr>
<tr>
<td></td>
<td>For example, tcp://123.0.1.2:12345.</td>
</tr>
</tbody>
</table>
Include username in JMS body

Select this check box to include the user name in the body of the JMS message.

This check box is selected by default.

JMS topic

Type the JMS message topic.

The default value is Fortify.Advisory.EventNotification.

5. Click **Save**.
6. Restart the server.

**Configuring LDAP Servers**

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

**Important! Important:** Before you configure the properties on the LDAP page, you must prepare for LDAP authentication as described in "LDAP User Authentication" on page 57.

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

To configure one or more LDAP server connections for Fortify Software Security Center:

1. On the Hewlett Packard Enterprise header, click **Administration**.
2. In the left panel, select **Configuration**, and then select **LDAP Servers**.
3. On the Integration with LDAP servers page, click **New**.

   The Create New LDAP Configuration dialog box opens.

4. Configure the attributes described in the following table.

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Server Properties</strong></td>
<td></td>
</tr>
<tr>
<td>Enable this LDAP Integration</td>
<td>Select this check box to make this LDAP server available for Fortify Software Security Center to use.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Type a unique name for this server.</td>
</tr>
</tbody>
</table>

**Important:** If you configure multiple LDAP servers, you must make sure...
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>that you specify a unique server name for each.</td>
<td>Type the LDAP authentication server URL. If you use unsecured LDAP, enter the URL in the following format: <code>ldap://&lt;hostname&gt;:&lt;port&gt;</code> If you use secured LDAPS, enter the URL in the following format: <code>ldaps://&lt;hostname&gt;:&lt;port&gt;</code> LDAPS ensures that only encrypted user credentials are transmitted.</td>
</tr>
<tr>
<td>Server URL (<code>ldap://&lt;host&gt;:&lt;port&gt;</code>)</td>
<td>Type the Base Distinguished Name (DN) for LDAP directory structure searches. For example, the Base DN for <code>companyName.com</code> is <code>dc=companyName,dc=com</code>. All DN values are case-sensitive, must not contain extra spaces, and must exactly match LDAP server entries. 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.</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Bind User DN</td>
<td>Type the full distinguished name (DN) of the account Fortify Software Security Center uses to connect to the authentication server. The general format for an account specifier is as follows:</td>
</tr>
<tr>
<td>Note: If your LDAP server supports anonymous binding, you are not required to specify values for Bind User DN and Bind User Password. Check with your LDAP administrator to find</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| out whether your LDAP server supports anonymous binding. | `<cn=<accountName>,ou=users,dc=<domainName>,dc=com` where `<accountName>` represents the minimum privilege, read-only authentication server account you created for exclusive use by Fortify Software Security Center.  
**Caution:** For security reasons, never use a real user account name in a production environment.  
If you use Active Directory, specify the domain name and username in the following format:  
`<domain_name><username>` |
| Bind User Password | Type the password for the Bind User DN account.  
**Note:** If your LDAP server supports anonymous binding, you are not required to specify values for Bind User DN and Bind User Password. Check with your LDAP administrator to find out whether your LDAP server supports anonymous binding. |
<p>| Relative Search DNs (1 per line) | (Optional) Type the Relative Distinguished Name (RDN). An RDN defines the starting point from the Base DN for LDAP directory searches. Fortify recommends that you search from the base DN. However, if your 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>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For example: To search within the base DN companyName.com and all entries under that base DN, specify the following to recursively search all entries under that path:</td>
</tr>
<tr>
<td></td>
<td>cn=users</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>cn=users,ou=divisionName</td>
</tr>
<tr>
<td>Ignore Partial Result Exception</td>
<td>To avoid search failures when search results include more records than the LDAP server can return, leave this check box selected.</td>
</tr>
<tr>
<td></td>
<td>You can also enable this flag to hide LDAP server misconfiguration. For example, if the LDAP server limits the number of query results to 500, but there are 600 actual results, with this flag enabled, Fortify Software Security Center silently returns only 500 records.</td>
</tr>
</tbody>
</table>

Because most people use Microsoft Active Directory, the remaining LDAP attributes on the page are configured to work with the default Active Directory configuration. However, if your LDAP server is set up differently, you can change these attribute values.

**Base Schema**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object class attribute</td>
<td>Type the class of the object. For example, if this is set to objectClass, Fortify Software Security Center looks at the objectClass attribute to determine the entity type to search. The default value is objectClass.</td>
</tr>
<tr>
<td>Organizational unit class</td>
<td>Type the object class that defines an LDAP object as an organizational unit. The default value is container.</td>
</tr>
<tr>
<td>User class</td>
<td>Type the object class that identifies an LDAP object type as a user. The default value is user.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>value is organizationalPerson.</td>
<td></td>
</tr>
<tr>
<td>Organizational unit name attribute</td>
<td>Type the group attribute that specifies the organizational unit name. The default value is <code>cn</code>.</td>
</tr>
<tr>
<td>Group class</td>
<td>Type the object class that identifies an LDAP object type as a group. The default value is <code>group</code>.</td>
</tr>
<tr>
<td>Distinguished name (DN) attribute</td>
<td>Type the value that determines the attribute Fortify Software Security Center looks at to find the distinguished name of the entity. The default value is <code>distinguishedName</code>.</td>
</tr>
</tbody>
</table>

**User Lookup Schema**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User first name attribute</td>
<td>Type the user object attribute that specifies a user’s first name. The default value is <code>givenName</code>.</td>
</tr>
<tr>
<td>User last name attribute</td>
<td>Type the user object attribute that specifies a user’s last name. The default value is <code>sn</code>.</td>
</tr>
<tr>
<td>Group name attribute</td>
<td>Type the group attribute that specifies the group name. The default value is <code>cn</code>.</td>
</tr>
<tr>
<td>User username attribute</td>
<td>Type the user object attribute that specifies a username. The default value is <code>sAMAccountName</code>.</td>
</tr>
<tr>
<td>User password attribute</td>
<td>Type the user object attribute that specifies a user’s password. The default value is <code>userPassword</code>.</td>
</tr>
<tr>
<td>Group member attribute</td>
<td>Type the group attribute that defines the members of the group. The default value is <code>cn</code>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>member.</td>
</tr>
<tr>
<td>User email attribute</td>
<td>Type the user object attribute that specifies a user’s email address. The default value is mail.</td>
</tr>
<tr>
<td>User memberOf attribute</td>
<td>Type the name of an LDAP attribute that includes the LDAP group names for LDAP users.</td>
</tr>
</tbody>
</table>

**User Photo**

| User photo enabled            | Select this check box to enable the retrieval of user photos from the LDAP server. |
| User thumbnail photo attribute| ThumbnailPhoto attribute for Active Directory.                                 |
| User thumbnail mime default attribute| Thumbnail mime default attribute                                               |

**Advanced Integration Properties**

<p>| Cache LDAP User Data          | Select this check box to enable LDAP user data caching in Fortify Software Security Center. You can refresh the LDAP cache manually from the Administration view in Fortify Software Security Center. For instructions, see &quot;Refreshing LDAP Entities Manually&quot; on page 107. |
|                               | <strong>Note:</strong> Fortify recommends that you leave LDAP user caching enabled. Changes to user information made directly in the LDAP server may not be reflected in Fortify Software Security Center for up to an hour. However, a slow connection between Fortify Software Security Center and the LDAP server or a large LDAP directory with slow searches could degrade Fortify Software Security Center performance. User data are seldom changed directly in the LDAP server. |
| Cache: Max threads per cache  | Type the maximum number of threads dedicated for each update process (user |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>action). Each time a user clicks <strong>Update</strong>, a new update process starts. The default value is 4.</td>
</tr>
<tr>
<td>Cache: Max object lifetime (ms, &quot;-1&quot; to turn off)</td>
<td>If you want objects in the cache refreshed more frequently than the default refresh time (typically 1 hour), type the maximum amount of time (in milliseconds) that an object can be in the cache before it is refreshed with new information from the LDAP server. The default value is -1.</td>
</tr>
<tr>
<td>Cache: Initial thread pool size</td>
<td>Type the initial number of available cache update threads. This value is used to configure the thread pool for the task executor, which updates the LDAP cache in several threads simultaneously. The default value is 4.</td>
</tr>
<tr>
<td>Cache: Max thread pool size</td>
<td>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.</td>
</tr>
<tr>
<td>Enable paging in LDAP search queries</td>
<td>Select this check box to enable paging in LDAP search queries. <strong>Note:</strong> Not all LDAP servers support paging. Check to make sure that your LDAP server supports this feature.</td>
</tr>
<tr>
<td>Page size of LDAP search request results</td>
<td>If your LDAP server limits the size of the search results by a certain number of objects and <strong>Enable paging in LDAP search queries</strong> is selected, type a value that is less than or equal to your LDAP server limit. The default value is 999.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>LDAP referrals processing strategy</td>
<td>If you have only one LDAP server, HPE recommends that you select <code>ignore</code> so that LDAP works faster. If you have a multi-domain LDAP configuration and you use LDAP referrals, select <code>follow</code>. The default value is <code>ignore</code>. <strong>Note:</strong> If referrals are not used on your LDAP server, see &quot;About the LDAP Server Referrals Feature&quot; on page 59.</td>
</tr>
</tbody>
</table>
| LDAP Authenticator type | From this list, select one of the following LDAP authentication types to use:  
  - **BIND_AUTHENTICATOR**—Authentication directly to the LDAP server ("bind" authentication).  
  - **PASSWORD_COMPARISON_AUTHENTICATOR**—The password the user supplies is compared to the one stored in the repository.  
  
For more information about LDAP authentication types, see [http://docs.spring.io/spring-security/site/docs/3.1.x/reference/ldap.html](http://docs.spring.io/spring-security/site/docs/3.1.x/reference/ldap.html). |
| LDAP Password Encoder type | Select a value from this list only if the LDAP authentication method is password comparison.  
  You must select the encoder type that the LDAP server uses. Fortify Software Security Center compares encoded passwords. If, for example, the LDAP server uses `LDAP_SHA_PASSWORD_ENCODER` to encode passwords, but you select `MD4_PASSWORD_ENCODER`, password comparisons will fail. |
<p>| Enable Nested LDAP Groups | Select this check box to enable nested group support for LDAP in Fortify Software Security Center (wherein a given group... |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>you absolutely must. Enabling nested LDAP groups forces Fortify Software Security Center to perform extra tree traversals during authentication. HPE strongly recommends that you clear this check box if you do not plan to use nested groups.</td>
<td>member might itself be a group).</td>
</tr>
<tr>
<td>Interval between LDAP server validation attempts (ms)</td>
<td>Number of milliseconds the LDAP server waits after a validation attempt before next attempting a validation. The default value is 5000.</td>
</tr>
<tr>
<td>Time to wait LDAP validation (ms)</td>
<td>Type the length of time (in milliseconds) that Fortify Software Security Center is to wait for a response after sending a request to the LDAP server to update the cache. If a response is not received at the end of the designated time, the update is not performed. The request is sent again at the frequency determined by the value set for the Interval between LDAP server validation attempts field. The default value is 5000.</td>
</tr>
<tr>
<td>Base security identifier of ActiveDirectory objects</td>
<td>Specify the base security identifier (SID) of LDAP directory objects.</td>
</tr>
<tr>
<td>Object SID (objectSid) attribute</td>
<td>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.</td>
</tr>
</tbody>
</table>
To check the validity of and save the configuration, click **Save**.

To configure another LDAP server, repeat steps 3 through 6.

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

### See Also

"Importing an LDAP Server Configuration" below

"LDAP User Authentication" on page 57

"Registering LDAP Entities" on page 176

"About Managing LDAP User Roles" on page 135

"Editing an LDAP Server Configuration" below

"Deleting an LDAP Server Configuration" on page 107

### Editing an LDAP Server Configuration

To edit an LDAP server connection:

1. On the Hewlett Packard Enterprise header, click **Administration**.
2. In the left panel, select **Configuration**, and then select **LDAP Servers**.
3. On the Integration with LDAP servers page, click the LDAP server connection that you want to edit.
   The row expands to reveal the LDAP server details.
4. At the upper right of the server details section, click **Edit**.
5. Make all necessary changes to the attributes described in "Configuring LDAP Servers" on page 94.
6. To check the validity of the configuration, click **Validate Connection**.
7. To check the validity of and save the configuration, click **Save**.

### See Also

"LDAP User Authentication" on page 57

"Registering LDAP Entities" on page 176

"About Managing LDAP User Roles" on page 135

### 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 Hewlett Packard Enterprise header, click **Administration**.
2. In the left panel, select **Configuration**, and then scroll down and select **LDAP Servers**.
3. On the LDAP Servers header, click **Import**.
   The Import Legacy LDAP Configuration wizard opens.

4. Manually copy the content of your legacy ldap.properties file for the LDAP configuration to import, and paste it into the text box.
   If Fortify Software Security Center detects problems with the copied content, it displays an error message and a link to click for more information.

   **Note:** The encoded Bind User DN (ldap.user.dn) and Bind User Password (ldap.user.password) values are not imported. You must enter these manually in "Configure the attributes described in the table in step 4 in "Configuring LDAP Servers" on page 94." below.

5. Correct any problems, and then click **Next**.
6. Configure the attributes described in the table in step 4 in "Configuring LDAP Servers" on page 94.
7. To check the validity of the configuration, click **Validate Connection**.
8. To check the validity of and save the configuration, click **Save**.

**See Also**

"LDAP User Authentication" on page 57

"Registering LDAP Entities" on page 176

"About Managing LDAP User Roles" on page 135

**Registering LDAP Entities**

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

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

1. Log in to Fortify Software Security Center as an Administrator, and then, on the Hewlett Packard Enterprise header, click **Administration**.
2. In the left panel, click **Users**, and then select **LDAP**.
3. On the **LDAP** toolbar, click **Add**.
   The **Add New LDAP Entity** window opens.
4. From the **LDAP Entity** list, select the type of LDAP entity you want to register (**Group**, **User**, or **Organizational Unit**).

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

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

7. To provide the LDAP entity access to versions of an application, in the **Access** section, do the following.

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

The Select Application Version dialog box opens.

b. From the **Application** list, select the name of an application that you want the LDAP entity to access.

The **Versions** section lists all active versions of the application.

c. To display inactive versions of the application, select the **Show Inactive Versions** check box.

d. In the **Versions** section, select the check boxes for all of the versions that you want the entity to access.

e. Click **Done**.

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

8. Do one of the following:
   - To save your changes and close the Add New LDAP Entity dialog box, click **Save**.
   - To save your changes and register another LDAP entity, click **Save And Add Another**.

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

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

9. To initiate the LDAP refresh process manually so that your changes are evident sooner than they would be otherwise:
   a. On the LDAP page, select the check box for the LDAP entity you want to refresh.
   b. On the LDAP toolbar, click **Refresh**.

For information about how to configure LDAP servers, see "Configuring LDAP Servers" on page 94.
Refreshing LDAP Entities Manually

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

To initiate the LDAP refresh process manually:

1. Log in to Fortify Software Security Center as an Administrator, and then, on the Hewlett Packard Enterprise header, click Administration.
2. In the left panel, select Users, and then select LDAP.
3. In the list of LDAP entities, select the check box for the LDAP entity to refresh.
4. On the LDAP toolbar, click Refresh.

For information about how to configure LDAP servers, see "Configuring LDAP Servers" on page 94.

Deleting an LDAP Server Configuration

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

To delete an LDAP server connection:

1. On the Hewlett Packard Enterprise header, click Administration.
2. In the left panel, select Configuration, and then select LDAP Servers.
3. Do one of the following:
   - On the Integration with LDAP Servers page, select the check box for the LDAP server that you want to delete, and then, on the LDAP Servers toolbar, click Delete.
   - Alternatively,
     - On the Integration with LDAP servers page, click the LDAP server connection that you want to delete, and then, at the upper right of the expanded server details section, click Delete.

   The Delete LDAP configuration dialog box prompts you to confirm that you want to proceed with the deletion.
4. Click OK.
5. To force all LDAP users to re-authenticate, restart the Fortify Software Security Center server.

See Also

"LDAP User Authentication" on page 57
"Registering LDAP Entities" on page 176
"About Managing LDAP User Roles" on page 135

About the SAP NetWeaver Plugin for Fortify Software Security Center

If your organization uses SAP NetWeaver Code Vulnerability Analyzer (CVA) to search for vulnerabilities in ABAP source code, you can use the NetWeaver plugin to map your CVA scans to a Fortify Software Security Center application version, and then import the results for investigation from Fortify Software Security Center.

Fortify Software Security Center displays the individual CVA findings, and identifies their source code file names and line numbers, assigns each a Fortify Priority Order, and then displays them in the Fortify Software Security Center user interface for auditing.

Setting up the NetWeaver Plugin

Setting up the NetWeaver plugin involves the following tasks:

1. Download the SAP JCo driver from the official SAP download site. You can download the driver from the SAP Software Downloads Center.
2. Add the SAP JCo driver to Fortify Software Security Center
   For instructions, see "Adding the SAP JCo Driver to Fortify Software Security Center" below.
3. Configure the connection to NetWeaver. See "Connecting to SAP NetWeaver" on the next page.

After you complete this setup, you can map your CVA results to Fortify Software Security Center application versions. For instructions, see "Uploading SAP NetWeaver Data to an Application Version" on page 231.

Adding the SAP JCo Driver to Fortify Software Security Center

To integrate Fortify Software Security Center with NetWeaver, you must add the SAP JCo driver to the system.

Important: (Windows only) Before you add the JCo driver, you must first install the latest Visual Studio C/C++ runtime libraries. For up-to-date information about the requirements for SAP JCo driver installation, see the SAP JCo documentation.

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

- Add the SAP JCo JAR file location to the class path of the web application server on which you plan to deploy Fortify Software Security Center.
Or,

a. Unzip the Fortify Software Security Center installation bundle for your application server (HPE_Security_Fortify_<version>_Server_WAR_<app_server_name>.zip).

b. Unzip the ssc.war file.

c. Open the WEB-INF folder, and then place the SAP JCo file in the lib folder.

d. Save the ssc.war file, and then re-zip the installation bundle.

See Next

"Connecting to SAP NetWeaver" below

See Also

"About the SAP NetWeaver Plugin for Fortify Software Security Center" on the previous page

Connecting to SAP NetWeaver

To complete the NetWeaver plugin setup after you download the SAP JCo driver and add it to the system (see "Adding the SAP JCo Driver to Fortify Software Security Center" on the previous page), you configure the Fortify Software Security Center connection to NetWeaver.

To configure a connection to NetWeaver:

1. On the Hewlett Packard Enterprise header, select Administration.
2. In the left panel of the Administration view, select Configuration, and then click NetWeaver.
3. On the NetWeaver page, provide the information described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable NetWeaver Integration</td>
<td>Select this check box to enable editing of the remaining fields on the page.</td>
</tr>
<tr>
<td>NetWeaver host</td>
<td>IP address of your SAP NetWeaver host.</td>
</tr>
<tr>
<td>System number</td>
<td>System number for your SAP NetWeaver Gateway host.</td>
</tr>
<tr>
<td>Client number</td>
<td>Number for the SAP client to which you want to connect.</td>
</tr>
<tr>
<td>Username</td>
<td>User name for the NetWeaver user.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the NetWeaver user.</td>
</tr>
<tr>
<td>Language</td>
<td>Two-letter language code.</td>
</tr>
<tr>
<td>Pool capacity</td>
<td>Maximum number of connections held open for reuse in the NetWeaver connection pool.</td>
</tr>
</tbody>
</table>
Maximum connections | Maximum number of connections that can be obtained from the NetWeaver connection pool during peak usage times.

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

### Configuring Fortify Runtime Application Protection Communication Settings

If you need Fortify Software Security Center to communicate with Fortify Runtime Application Protection, you enable Runtime in the Configuration category in the Fortify Software Security Center Administration view.

**Note:** For information about how to configure, monitor, and manage instances of Runtime Application Protection that are running in federated mode, see the *HPE Security Fortify Runtime Application Protection Operator Guide*.

To enable Fortify Software Security Center to communicate with Runtime Application Protection:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Hewlett Packard Enterprise header, select **Administration**.
2. In the left panel, select **Configuration**, and then select **Runtime**. The Runtime integration attributes page opens.
3. Configure the settings described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Runtime</td>
<td>Select this check box to enable runtime communications with Fortify Software Security Center.</td>
</tr>
<tr>
<td>Email addresses (comma separated) to notify when a runtime configuration error occurs</td>
<td>Type the email addresses of the users to notify when a Runtime configuration error occurs. Separate the addresses with commas. For example, <a href="mailto:runtime.admin@abc_co.com">runtime.admin@abc_co.com</a>, <a href="mailto:runtime.manager@abc_co.com">runtime.manager@abc_co.com</a>.</td>
</tr>
<tr>
<td>Port for Runtime federation</td>
<td>Type the number of the port that is used for runtime federation. <strong>Caution!</strong> Do not change this setting unless HPE Security support specifically directs you to do so.</td>
</tr>
</tbody>
</table>
4. Click Save.
5. Restart the server.

**Configuring Job Scheduler Settings**

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

To configure job scheduler settings:

1. On the Hewlett Packard Enterprise header, select Administration.
2. In the left panel, select Configuration, and then select Scheduler.
   The Job scheduler attributes page opens.
3. Configure the settings as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of days after which executed jobs will be removed</td>
<td>The number of days after which finished jobs are removed from Fortify Software Security Center. The default value is 2 (days).</td>
</tr>
<tr>
<td>Job execution strategy</td>
<td>Select the job execution strategy to use. Options are as follows:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Conservative:</strong> Enables highly concurrent FPR processing. With this option, the job scheduler can run FPR processing on all workers available to the scheduler and up to two report jobs at a time. Low concurrency jobs such as artifact and application version deletion are executed in sequence.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Aggressive:</strong> Enables high concurrency. With this option, the job</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>scheduler does not enforce any limitations on how jobs are executed. All jobs are equal and executed on all available workers.</td>
</tr>
<tr>
<td></td>
<td><strong>Exclusive jobs:</strong> Enables jobs to run in sequence, one at a time. The default value is Conservative.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Two worker threads are dedicated to exporting to comma-separated values (CSV) jobs for both conservative and aggressive strategies. (See &quot;Exporting Data to Comma-Separated Values Files&quot; on page 163.)</td>
</tr>
</tbody>
</table>

**Snapshot refresh** - Use the fields in this section to schedule the snapshot job.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Days to preserve</td>
<td>Type the number of days after which HPE removes past events. To specify no event removal, type 0 (zero). Fortify Software Security Center uses the new value during the next run of the dedicated cleaning job. A new job is created daily at 11:30 p.m. and if it is not blocked, it starts its work immediately.</td>
</tr>
</tbody>
</table>

4. Click **Save**.

5. Restart the server.

**See Also**

“Canceling Scheduled Jobs” on the next page

### Setting Job Execution Priority

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

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

To set the priority for a scheduled job:

1. On the Hewlett Packard Enterprise header, select **Administration**.
2. In the left panel of the Administration view, under **Metrics & Tracking**, select **Jobs**.
3. On the right end of the **Jobs** toolbar, from the **Filter by** list, select **Prepared**.
4. Scroll through the listed jobs and expand (click) the row for the job you want to re-prioritize.
5. From the **Set Priority** list, select one of the following priority values:
   - Very Low
   - Low
   - Medium
   - High
   - Very High
Changing job priority may affect other jobs in the queue. If the priority you set for a job potentially affects other jobs, Fortify Software Security Center displays a message to advise you of the potential effect, and prompts you to confirm that you want to continue with the change.

6. To continue, click **OK**.

The jobs table now reflects the changed priority setting.

**See Also**

"Configuring Job Scheduler Settings" on page 111

"Canceling Scheduled Jobs" below

**Canceling Scheduled Jobs**

If you are a Fortify Software Security Center administrator or a security lead, you can cancel scheduled jobs that are still in the PREPARED state. (The job state can be PREPARED, RUNNING, FINISHED, FAILED, or CANCELED.)

To cancel a job:

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

**See Also**

"Configuring Job Scheduler Settings" on page 111

**Configuring Browser Access Security for Fortify Software Security Center**

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

1. On the Hewlett Packard Enterprise header, select **Administration**.
2. In the left panel, select **Configuration**, and then select **Security**.
    The Security page opens.
3. Configure the settings as described in the following table.
### Field: Content-Security-Policy

Specify what (if any) level of CSP to use. Using the HTTP Content-Security-Policy header controls the resources browsers can load and what actions they can perform on pages loaded from Fortify Software Security Center. This helps guard against cross-site scripting attacks.

Select one of the following options:

- To restrict access to only the base URL configured using the `host.url` property (set using the Fortify Software Security Center configuration wizard), select **Strict**.

- To enable a less restrictive policy than strict CSP, select **Relaxed**. This is the default setting. It allows access to the Fortify Software Security Center domain from any host:port.

- To disable the Content-Security-Policy header, select **Disabled**. Although Fortify recommends that you not disable the Content-Security-Policy header, this option is available if CSP causes unexpected problems.

### Field: Set value for Strict-Transport-Security header

Type the value for the Strict-Transport-Security header. This header signals to browsers to use HTTPS instead of HTTP to communicate with Fortify Software Security Center.

**Important:** Setting this value can prevent users from accessing applications on this domain or its sub-domains for a long time.

The Strict-Transport-Security header is sent only through a secure channel determined by the application server.

### Field: Set value for Public-Key-Pins header

Type the value for the Public-Key-Pins header. This decreases the risk of man-in-the-middle (MitM) attacks.
### Field | Description
--- | ---
 | Important: Setting this value can prevent users from accessing applications on this domain or its sub-domains for a long time. The Public-Key-Pins header is sent only through a secure channel determined by the application server.

4. Click **Save**.

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

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

<table>
<thead>
<tr>
<th>SSO Solution</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Authorization Server (CAS)</td>
<td>&quot;Configuring Fortify Software Security Center to Work with a Central Authorization Server&quot; on the next page</td>
</tr>
<tr>
<td>SPNEGO-based Kerberos</td>
<td>&quot;Setting up Kerberos Authentication with Fortify Software Security Center&quot; on the next page</td>
</tr>
<tr>
<td>SAML 2.0-compliant single sign-on</td>
<td>&quot;Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single Sign-On Solutions&quot; on page 119</td>
</tr>
<tr>
<td>HTTP headers</td>
<td>&quot;Configuring Fortify Software Security Center to Work with Single Sign-On and Single Logout Solutions that use HTTP Headers&quot; on page 122</td>
</tr>
<tr>
<td>X.509 certification</td>
<td>&quot;Configuring Fortify Software Security Center to use X.509 Certification-based SSO&quot; on page 123</td>
</tr>
</tbody>
</table>

**Notes:**
You can only use the SSO solutions that Fortify Software Security Center supports to give users access to the Fortify Software Security Center user interface. A user who wants to access Audit Workbench, fortifyclient, or any of the IDE plugins, must use an LDAP or local Fortify Software Security Center user account and password to log in.
Configuring Fortify Software Security Center to Work with a Central Authorization Server

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

1. Log in to Fortify Software Security Center as an administrator, and then, on the Hewlett Packard Enterprise header, click Administration.

2. In the left panel of the Administration view, select Configuration, and then select SSO. The Single Sign On page opens to the CAS SSO tab.

3. Configure the settings described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Central Authentication Server integration</td>
<td>Select this check box to enable integration with CAS.</td>
</tr>
<tr>
<td>HPE Security Fortify Software Security Center Location</td>
<td>Type the Fortify Software Security Center server URL. The default is <a href="http://localhost:8180/ssc">http://localhost:8180/ssc</a>.</td>
</tr>
<tr>
<td>Central Authentication Server URL</td>
<td>Type the URL for the CAS server. The default is <a href="http://localhost:8080/cas">http://localhost:8080/cas</a>.</td>
</tr>
</tbody>
</table>

4. Click Save.

5. Restart the server.

Setting up Kerberos Authentication with Fortify Software Security Center

To set up Kerberos authentication with Fortify Software Security Center:

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

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

2. Create a keytab file.

   **Example:**

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

3. Log in to Fortify Software Security Center as an administrator, and then, on the Hewlett Packard Enterprise header, select Administration.
4. In the left panel of the Administration view, select **Configuration**, and then select **SSO**. The Single Sign On page opens.
5. Click the **SPNEGO/Kerberos SSO** tab.
6. Select the **Enable SPNEGO/Kerberos integration** check box.
7. In the **Service principal name** box, type the service principal name (SPN) of Fortify Software Security Center in the Kerberos realm.
8. In the **Keytab location** box, type the location of the keytab file (created in step 2), which contains Fortify Software Security Center principal keys.
   Make sure that you use the correct resource prefix. Example: file:///.
9. (Optional) In the **Krb5.conf location** box, type the Krb5.conf file location.
   This sets the java.security.ker5.conf property.
10. To enable debug mode, select the **Enable debug mode** check box.
11. Click **Save**.
12. Check to make sure that the **User username attribute** setting for your LDAP server is correct. (See "Configuring LDAP Servers" on page 94.)
13. Restart the server.
14. Verify that the LDAP user names resolve correctly. Format the LDAP user name values as follows:

   `username@domain`

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

   **Important:** Check to make sure that the Fortify Software Security Center LDAP configuration username mapping matches the LDAP User entry attribute, where the attribute holds a username sent in the Kerberos ticket. In configurations that use Microsoft Active Directory, the User Principal Name (UPN) attribute should hold the username sent in the Kerberos ticket. However, verify this before you change configuration settings.

   **See Also**
   "Configuring Fortify Software Security Center to Work with Single Sign-On" on page 117

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

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

   To configure Fortify Software Security Center to work with SSO that uses SAML 2.0:
1. If you are using 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 57.)

2. If your IdP runs with SSL (https), configure Fortify Software Security Center to run with SSL. Otherwise, protocol switching during authenticating against IdP could interfere with authentication.

3. Get SAML metadata from the IdP server and store it on the Fortify Software Security Center file system.

4. Open the metadata file and make a note of the entityID for your IdP EntityDescriptor (EntityDescriptor entityID="THE_VALUE_YOU_ARE_LOOKING_FOR").

5. Log in to Fortify Software Security Center and, on the Hewlett Packard Enterprise header, select Administration.

6. In the left panel of the Administration view, select Configuration, and then select SSO. The Single Sign On page opens.

7. Click the SAML SSO tab.

8. Provide the information described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SAML 2.0 integration</td>
<td>Select this check box to enable the remaining configuration fields on the page.</td>
</tr>
<tr>
<td>IdP metadata location</td>
<td>Location of your identity provider metadata (the metadata obtained in step 2):</td>
</tr>
<tr>
<td></td>
<td>file:///location/of/idp-metadata.xml</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If your IdP is behind a proxy server, you must download IdP metadata to your local file system and reference it locally. Current SAML implementation does not support getting metadata over http proxy.</td>
</tr>
<tr>
<td>Default IdP</td>
<td>entityId of your IdP EntityDescriptor (from IdP metadata)</td>
</tr>
<tr>
<td>SP entity ID</td>
<td>Service provider entity ID</td>
</tr>
<tr>
<td></td>
<td>You can specify the Fortify Software Security Center URL or a Uniform Resource Name (URN) such as urn:ssc:saml.</td>
</tr>
<tr>
<td>SP alias</td>
<td>Fortify Software Security Center alias</td>
</tr>
<tr>
<td></td>
<td>To simplify things, you can use the URN (urn:ssc:saml).</td>
</tr>
<tr>
<td>Keystore location</td>
<td>Location of your Java keystore for encrypting and signing SAML assertions</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Keystore password</td>
<td>Java keystore file password</td>
</tr>
<tr>
<td>Signing &amp; encryption key</td>
<td>Signing/encryption key</td>
</tr>
<tr>
<td>Signing &amp; encryption key password</td>
<td>Signing/encryption key password</td>
</tr>
<tr>
<td>SAML name Identifier</td>
<td>Username attribute (any string assertion attribute)</td>
</tr>
</tbody>
</table>

9. Click **Save**.

10. Verify that the `host.url` property in `<fortify.home>/<app-context>/conf/app.properties` designates a URL that the IDP server can access. The URL is used as a base URL for Fortify Software Security Center SAML metadata.

   **Note:** For Fortify Software Security Center version 17.10 and earlier versions, you can find the `host.url` property in `<WAR>/WEB-INF/config/ssc.properties` or use the configuration wizard to set up the URL.


12. Generate the Fortify Software Security Center (SP) metadata at `<hostname>:\<port>\<app_context>\saml/metadata`.

13. Open the metadata generated in previous step and verify that the values for the following are the same as the values you specified in the **SAML SSO** tab:
   - The entity ID value matches the one you specified in the "SP entity ID" on the previous page box.
   - The SP alias in the metadata is the one you specified in the "SP alias" on the previous page box.
   - The location URLs in `<AssertionConsumerService>` bindings are accessible from the IDP server.

14. Upload the Fortify Software Security Center metadata to the IDP server.

15. Try to access `<hostname>:\<port>\<app_context>`. You are redirected to the IDP server, where you can enter your credentials. After successful authentication, the IDP server redirects you back to Fortify Software Security Center.

**Troubleshooting**

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

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

**Issue:** "I'm authenticated with IDP, but Fortify Software Security Center doesn't authorize me."
- The username received in the SAML assertion from IdP does not match any LDAP or local Fortify Software Security Center user (based on user lookup strategy). Verify the following:
  - The “SAML name identifier” in your Fortify Software Security Center SAML configuration is set to an attribute in the SAML assertion that contains the username.
  - The user exists in Fortify Software Security Center.
  - The user lookup strategy is correctly configured (see “Configuring Core Settings” on page 87).

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

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

**See Also**

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

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

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

1. On the Hewlett Packard Enterprise header, select **Administration**.
2. In the left panel, select **Configuration**, and then select **SSO**.
   The Single Sign On page opens.
3. Select the **HTTP SSO** tab.
4. Configure the settings as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Single Sign On</strong></td>
<td></td>
</tr>
<tr>
<td>Enable HTTP SSO integration</td>
<td>Select this check box to enable the remaining fields.</td>
</tr>
<tr>
<td>HTTP header for username</td>
<td>Type the HTTP header to use for SSO logons.</td>
</tr>
<tr>
<td></td>
<td>The default value is <strong>username</strong>.</td>
</tr>
<tr>
<td>IdP login page</td>
<td>Type the URL for the identity provider login page.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>SSO Logon</strong></td>
<td></td>
</tr>
<tr>
<td>Enable SSO logon</td>
<td>Select this check box to enable single logout.</td>
</tr>
<tr>
<td>SSO logon page</td>
<td>Type the logout page address to which users are to be redirected after</td>
</tr>
<tr>
<td></td>
<td>logging out of Fortify Software Security Center.</td>
</tr>
<tr>
<td>SSO logon response</td>
<td>Type the dynamic directive header.</td>
</tr>
<tr>
<td>response header</td>
<td></td>
</tr>
<tr>
<td><strong>SSO Logon Response Directive</strong></td>
<td></td>
</tr>
<tr>
<td>SSO logon response</td>
<td>Type the dynamic directive code in this box.</td>
</tr>
<tr>
<td>response code</td>
<td></td>
</tr>
<tr>
<td>SSO logon response</td>
<td>Type the dynamic directive message in this box.</td>
</tr>
<tr>
<td>response text</td>
<td></td>
</tr>
</tbody>
</table>

5. Click **Save**.


7. Restart the server.

**See Also**

“Configuring Fortify Software Security Center to Work with Single Sign-On” on page 117

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

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

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

### Configuring Web Services to Require Token Authentication

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

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

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

Token authentication is enabled by default. If you do not want to use token authentication, you must disable it on the **Web Service Attributes** page.

For additional information about authentication tokens, see "fortifyclient Authentication Tokens" on page 300.

To enable or disable token authentication:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Hewlett Packard Enterprise header, select **Administration**.
2. In the left panel, select **Configuration**, and then select **Web Services**.
   The **Web Service Attributes** page opens.
3. Do one of the following:
   - To enable token authentication, select the **Allow token authentication** check box.
   - To disable token authentication, clear the **Allow token authentication** check box.
4. Click **Save**.
5. Restart the server.
Chapter 8: Additional Installation-Related Tasks

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

This section contains the following topics:

Disabling the Legacy User Interface .............................................................. 125
Setting the Legacy User Interface as the Default User Interface .......................... 126
Blocking Data Export to CSV Files .................................................................... 126
Configuring an Eclipse Plugin Update Site .......................................................... 127
About Bug Tracker Integration ........................................................................... 127
Adding and Managing Parser Plugins ............................................................... 130
About Fortify Software Security Center User Administration ............................. 131
About Managing LDAP User Roles .................................................................... 135
Creating Custom Application Attributes ............................................................ 136
Global Search Functionality in Fortify Software Security Center ........................ 138
Placing Fortify Software Security Center in Maintenance Mode ........................... 139

Disabling the Legacy User Interface

You can prevent all users from accessing the Fortify Software Security Center legacy (4.30) user interface.

To disable the Fortify Software Security Center legacy user interface:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Hewlett Packard Enterprise header, click Administration.
2. In the left panel, click Configuration, and then click Core.
   The Core SSC Attributes page opens.
3. Near the bottom of the page, select the Disable 4.30 legacy UI check box.
4. Click Save.
   Fortify Software Security Center removes the 4.30 UI item from the user profile list instance-wide.
5. Restart the server.
Setting the Legacy User Interface as the Default User Interface

You can, if you prefer, set the legacy (v 4.30) user interface as the default user interface for Fortify Software Security Center users.

To make the legacy user interface the default user interface for Fortify Software Security Center users:

1. Navigate to the `<fortify.home>/<app_context>/conf` directory, and then open the `app.properties` file in a text editor.
2. Change the value of the `default.ui.url` property as follows:
   ```
   default.ui.url=/flex/index.jsp
   ```
   **Note:** If no value is assigned to `default.ui.url` (the default), the new UI is the default UI. The `default.ui.url` property must be present in the `ssc.properties` regardless of whether a value is assigned to it.
3. Save and close the `app.properties` file.
4. Restart the Fortify Software Security Center server.

See Also

“Disabling the Legacy User Interface” on the previous page

Blocking Data Export to CSV Files

By default, users can export selected Fortify Software Security Center data displayed on the Issue Stats and Audit pages to comma-separated values (CSV) files. You can block this functionality.

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

1. Log in to Fortify Software Security Center as an administrator, and then, on the Hewlett Packard Enterprise header, click Administration.
2. In the left panel of the Administration view, select Configuration, and then select Core. The Core page opens.
3. Scroll to the bottom of the page, and then clear the **Enable export to CSV** check box.
4. Click Save.

See Also

“Configuring Core Settings” on page 87
Configuring an Eclipse Plugin Update Site

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

To configure an Eclipse update site:

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

   **Note:** `<ssc_install_dir>` is the directory in which Fortify Software Security Center is deployed. For example, for Tomcat, the `<ssc_install_dir>` directory is `<tomcat>/webapps/ssc`.

2. Locate the following line of text:

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

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

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

4. Save the `securityContext.xml` file.

5. Enable the mapping for the Eclipse Update site.

6. Run the HPE_Security_Fortify_SCA_and_Apps installer.

7. Copy the contents of `<sca_install_dir>/plugins/eclipse` (this consists of a `site.xml` file and jar files in the features and plugins directories) to the `update-site` directory on your web server. `<sca_install_dir>` is the location in which the Static Code Analyzer and Applications installer installed the files.

Your developers can now point to the URL from their Eclipse IDE. For complete client-side installation details, see the [HPE Security Fortify Plugins for Eclipse Installation and Usage Guide](#).

About Bug Tracker Integration

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

- Bugzilla
- JIRA
- HPE ALM
- TFS/VSTS
Notes:

- If your organization uses a bug tracking system other than those that Fortify supplies, you can author a new plugin for that system. For instructions, see "Authoring Bug Tracker Plugins" on page 314.
- If you are using a bug tracker plugin from a Fortify Software Security Center version earlier than 3.30, contact HPE Security technical support for assistance with migrating to the current release.

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 198.

Managing Bug Tracker Plugins

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

Adding Bug Tracker Plugins

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

To add a bug tracker plugin to the system:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Hewlett Packard Enterprise header, select Administration.
2. In the left panel of the Administration view, select Plugins, and then select Bug Tracking. The Bug Tracking page opens.
3. On the page header, click Add.
4. Read the warning and, if you accept the potential risk involved in uploading the plugin, click OK. The Upload Plugin Bundle dialog box opens.
5. Click Browse, and then locate and select the JAR file for your plugin.
6. Click Start upload. After the upload is completed, the Bug Tracking table lists the new plugin.
7. To enable the bug tracker plugin, click Enable. The Plugin State field for the plugin now displays the value ENABLED.

Removing Bug Tracker Plugins

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

1. Log in to Fortify Software Security Center as an administrator, and then, on the Hewlett Packard Enterprise header, select Administration.
2. In the left panel of the Administration view, select Plugins, and then select Bug Trackers. The Bug Tracking page opens.
3. Expand the row for the plugin you want to remove.
4. Click Disable, and then, after the plugin is disabled, click Remove.

See Also

"About Bug Tracker Integration" on page 127
"Authoring Bug Tracker Plugins" on page 314
"Adding and Managing Parser Plugins" on the next page

Securing Logon Credentials for Bug Tracking Systems

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

If, in your deployment architecture, the session is persisted to a database or file system, passwords for the bug-tracking systems may also be persisted using an internally developed symmetric key encryption. Make sure that you secure these data.

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

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

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

Bug Tracker Parameters

A bug submitted with a bug tracker requires that a standard summary and bug description be entered in the Submit Bug dialog box. You can also add values for priority level, a due date for the fix, and the assignee. Fortify Software Security Center fetches values for the Issue Type and Affects version fields dynamically from the bug tracking system based on the selected application.

If your application requires additional fields, you might need to modify the plugin before you use it. For instructions, see "Authoring Bug Tracker Plugins" on page 314 or contact HPE Security Fortify Support (https://support.fortify.com).
HPE ALM Parameters

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

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

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

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

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

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

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

Adding and Managing Parser Plugins

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

To add a parser plugin to the system:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Hewlett Packard Enterprise header, select **Administration**.
2. In the left panel of the Administration view, select **Plugins**, and then select **Parsers**.
   
   The Parsers page opens.

3. On the Parsers page header, click **Add**.
Fortify Software Security Center displays the Upload Plugin Warning to advise you of the risk of uploading untested plugins.

4. To acknowledge the warning and continue, click **OK**.
   The Upload Plugin Bundle dialog box opens.
5. Click **Browse**, and then locate and select the bundle file (JAR file) for your plugin.
6. Click **Start upload**.
   The Parsers page lists the plugin you uploaded.
7. To expand the row that displayed the parser name, click it.
8. To enable the parser plugin, click **Enable**.
   Fortify Software Security Center displays the Enable Plugin Warning to advise you of the risk of enabling untested plugins.
9. Click **OK**.

**See Also**

"Managing Bug Tracker Plugins" on page 128

**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** .......................................................... 131
- **Fortify Software Security Center User Accounts** ............................ 132
- **About Creating User Accounts** .................................................. 132
- **Preventing Destructive Library and Template Uploads to Fortify Software Security Center** .......................... 133
- **Viewing Permission Information for Fortify Software Security Center Roles** ........................................ 133
- **Unlocking User Accounts (Local Users Only)** ............................... 134

**Administrator Accounts**

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

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

Fortify Software Security Center permits the explicit addition of Administrator-level accounts to application versions. This enables Administrator users to be assigned issues from the Audit page.
Fortify Software Security Center User Accounts

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

- **Administrator**: An Administrator has access to all application versions and can perform all actions in the system.
- **Security Lead**: A Security Lead has access to all administrative operations except user account creation and editing. The Security Lead can create application versions and edit all aspects of the versions that they created or to which they are assigned.
- **Manager**: A Manager has read-only access to most administrative data. Managers can create and edit all data for the application versions to which they are assigned.
- **Developer**: A Developer has read-only access to some administrative data. Developers can create and edit a subset of data for the application versions to which they are assigned.
- **View-Only**: A View-Only user can view general information and issues for application versions to which he has access. A View-Only user cannot upload analysis results or audit issues.
- **Application Security Tester**: An Application Security Tester can perform operations that pertain to execution of dynamic scan requests. An Application Security Tester can view application versions, view and generate reports, process dynamic scans, upload results and audit issues.
- **WebInspect Enterprise System**: Users assigned the Fortify WebInspect Enterprise System role can register and de-register a Fortify WebInspect Enterprise instance from Software Security Center and can retrieve issue audit information. This role is intended for Fortify WebInspect Enterprise use only.

Note: Fortify Software Security Center user account types can edit their own account information (in the legacy user interface).

For more information about user accounts, see “User Accounts and Access” on page 155.

Related Topics

"About Creating User Accounts" below

"Unlocking User Accounts (Local Users Only)" on page 179

About Creating User Accounts

The Fortify Software Security Center Users module provides the tools you use to edit, delete, or suspend user accounts.

Fortify recommends that after you log on to Fortify Software Security Center for the first time, you create at least one non-default administrator account, and then delete the default administrator account.

After you create the non-default administrator account, use the new account to create the user accounts.
**Note:** As a Fortify Software Security Center administrator, you can delete or suspend all user accounts except for the last remaining administrator-level account. Fortify Software Security Center automatically disables the suspend and delete features for such an account.

For instructions on how to create a user account, see "Creating Local User Accounts" on page 175.

For information about how to configure Fortify Software Security Center user account timeout and lockout settings, see "Configuring Core Settings" on page 87. For more information about user account privileges, see "Fortify Software Security Center User Account Management" on page 166.

**See Also**

- "Viewing Permission Information for Fortify Software Security Center Roles" below
- "Unlocking User Accounts (Local Users Only)" on page 179

### Preventing Destructive Library and Template Uploads to Fortify Software Security Center

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

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

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

### Viewing Permission Information for Fortify Software Security Center Roles

To view detailed information about the actions that users assigned the various Fortify Software Security Center roles can perform:

1. On the Hewlett Packard Enterprise header, select **Administration**.
2. In the left panel, select **Users**, and then select **Roles**.
   The Roles page displays a table with the names and descriptions of all of the roles in the system.
3. Select the row for the role you are interested in.

   The row expands to reveal details for the role, including a table that lists all of the permissions granted to users assigned that role.
For more information about user accounts, see “Managing User Accounts” on page 166.

**Related Topics**

“Pre-configured Roles” on page 167

“About Creating User Accounts” on page 132

"Unlocking User Accounts (Local Users Only)" on page 179

**Unlocking User Accounts (Local Users Only)**

After a local user tries unsuccessfully to log in to Fortify Software Security Center more than three times in a row, Fortify Software Security Center prevents the user from attempting more logons. If email notifications are enabled, the user receives an email to advise the user that he or she is locked out and should notify the Fortify Software Security Center administrator. As an administrator, you can unlock the account for the user.

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

1. On the Hewlett Packard Enterprise header, select **Administration**.
2. In the left panel of the Administration view, select **Users**, and then click **Local**.
3. Bring up the locked user account, expand the row to view account details, and then click **Edit**.

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

4. To the right of the message, click **unlock**.

   Fortify Software Security Center prompts you to confirm that you want to unlock the account.
5. Click **Yes**.
6. Click **Save**.

**About Managing LDAP User Roles**

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

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

**Group Membership in Fortify Software Security Center**

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

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

**Important** Use nested LDAP groups only if you absolutely must. Enabling nested LDAP groups forces Fortify Software Security Center to perform extra tree traversals during authentication. Fortify strongly recommends that you clear this check box if you do not plan to use nested groups.

**See Also**

"Handling Failed LDAP User Logins" below

**Handling Failed LDAP User Logins**

If you have configured nested LDAP groups for your Fortify Software Security Center server, and LDAP authentication fails during an attempted login because of incorrect credentials, then the log includes a message about bad credentials. However, if the log contains the text "user is not authorized," you, as an administrator, must check to make sure that the user has been added to the correct LDAP group.

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

1. On the Hewlett Packard Enterprise header, select **Administration**.
2. In the left panel in the Administration view, select **Users**, and then select **LDAP**.
3. Select the check box for the LDAP server.
4. On the LDAP page header, click **Refresh**.
5. To determine whether the LDAP cache refresh has completed, from the Administration view, check either the Event Logs page or the Jobs page.

**Note:** Refreshing the data blocks your access to Fortify Software Security Center. An LDAP cache refresh can take a long time to complete.

**See Also**

"Group Membership in Fortify Software Security Center" on the previous page

**About Mapping Fortify Software Security Center Roles to LDAP Groups**

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

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

**Creating Custom Application Attributes**

Fortify Software Security Center comes with customizable technical and business attributes that enable administrators and security leads to categorize applications and application versions.

To create an application attribute:

1. Log in to Fortify Software Security Center as an administrator.
2. On the Hewlett Packard Enterprise header, click Administration.
3. In the panel on the left, in the Templates section, click Attributes.
   Fortify Software Security Center lists the attributes in a table to the right.
4. Click New.
   The Create New Attribute dialog box opens.
5. Complete the fields described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a descriptive name for the attribute.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a brief description that describes exactly what the attribute is for. The description is displayed under the attribute field in the Create New Application wizard.</td>
</tr>
<tr>
<td>Required</td>
<td>Select this check box to require users to set the attribute that you are defining here when they create an application template.</td>
</tr>
<tr>
<td>Hidden</td>
<td>Select this check box to prevent the new attribute from being displayed in the Create New Application wizard.</td>
</tr>
<tr>
<td>Category</td>
<td>Select <strong>Technical</strong> or <strong>Business</strong> to specify the attribute type. Depending on the category you select, the attribute is displayed on either the <strong>Business Attributes</strong> step or the <strong>Technical Attributes</strong> step of the Create Application Version wizard. <strong>Note:</strong> If your Fortify Software Security Center instance is integrated with Fortify WebInspect, the list also includes the <strong>Dynamic Scan Request</strong> category.</td>
</tr>
<tr>
<td>Scope</td>
<td>Select the value that indicates whether the attribute applies only to application versions, runtime applications, or to both.</td>
</tr>
</tbody>
</table>
| Type       | Select one of the following control types:  
- To create a check box for the attribute, select **Boolean**.  
- To create a calendar selection control for the attribute, select **Date**. **Note:** This type is not available for a Dynamic Scan Request attribute.  
- To create a list from which a user can select only a single value for the attribute, select **List of Values - Single Selection**.  
- To create a list from which a user can select multiple values for the attribute, select **List of Values - Multiple Selection**.  
- To create a field that accepts an integer value, select **Integer**.  
- To create a text field into which a user can type a single line of text, select **Text - Single Line**. |
### Global Search Functionality in Fortify Software Security Center

Fortify Software Security Center provides global, category-based search functionality that applies search terms across application versions, issues, reports, comments, and users. Newly added documents (artifacts, application versions, users) are indexed automatically and immediately.

You can enable global searches during configuration at first login or after an upgrade. (See "Configuring Fortify Software Security Center for the First Time" on page 70.)

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

To enable global searching on your Fortify Software Security Center server, you must provide your application server with read and write access to the search index directory.

- Provide your application server with read and write access to the search index directory.

**Recommended disk size**

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

**See Also**

- Troubleshooting Search Index Issues

### About Global Search Functionality

Fortify Software Security Center provides global, category-based search functionality that applies search terms across application versions, issues, reports, comments, and users. You can enable global searches during configuration at first login or after an upgrade. (See "Configuring Fortify Software Security Center for the First Time" on page 70.)

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To create a text field into which a user can type multiple lines of text, select <strong>Text - Multiple Lines</strong>.</td>
</tr>
</tbody>
</table>

**Note:** If you select one of the **List of Values** types, additional fields are displayed in which you add the values and their descriptions, and specify whether or not they are hidden.

6. Click **Save**.

The new attribute is available the next time a user uses the Create New Application wizard.
Software Security Center for the First Time on page 70 or "Configuring Fortify Software Security Center After an Upgrade" on page 144.

Recommended disk size

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

See Also

"Global Search Functionality in Fortify Software Security Center" on the previous page

"Troubleshooting Search Index Issues" below

Troubleshooting Search Index Issues

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

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

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

Search Index Maintenance

The index maintenance job, which is performed once a day, keeps the index healthy. You can change its run time from the Administration view. Fortify recommends that this job be scheduled to run once a day. For instructions on how to re-schedule executed jobs, see “Configuring Job Scheduler Settings" on page 111.

Placing Fortify Software Security Center in Maintenance Mode

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

To place Fortify Software Security Center in maintenance mode:

1. Log in to Fortify Software Security Center as an administrator, and then, on the Hewlett Packard Enterprise header, select Administration.

2. In the left panel, select Configuration, and then select Maintenance Mode. The Maintenance Mode page opens.
3. Select the **Set to maintenance mode** check box, and then click **Save**.

4. Restart the server.

5. Go to the `<fortify.home>/<app_context>` directory, and open the `init.token` file.

6. Copy the contents of the `init.token` file to the clipboard.

7. Open a web browser window and type the URL for your Fortify Software Security Center instance.

8. In the upper right corner of the Fortify Software Security Center Setup screen, click **Administrators**.

   ![Fortify Software Security Center Setup](image)

9. Paste the string you copied from the `init.token` file in the text box, and then click **Sign In**.

   The Fortify Software Security Center Setup wizard opens and displays all of the current configuration settings. For information about server configuration, see "Configuring Fortify Software Security Center for the First Time" on page 70.
Chapter 9: Upgrading Fortify Software Security Center

To perform a direct upgrade to the latest Fortify Software Security Center version, you must have one of the last two versions installed. For example, to upgrade to version 17.20, you must have either version 16.20 or 17.10 installed. If an earlier version is installed, you must upgrade to version 16.20 or 17.10 before you can upgrade to version 17.20.

If you cannot directly upgrade your current Fortify Software Security Center version to the latest version, see the version-specific Fortify Software Security Center documentation for instructions on how to upgrade to the previous release (or the release immediately before that).

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

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

This section contains the following topics:

- Fortify Software Security Center Database Upgrade Tasks ........................................141
- Preparing to Upgrade the Fortify Software Security Center Database ..........................142
- Preparing to Run the Database Upgrade Script .................................................................143
- Updating and Deploying the WAR File ..............................................................................143
- Configuring Fortify Software Security Center After an Upgrade .....................................144
- Troubleshooting Database Migration Problems ...............................................................147
- Troubleshooting an Error Received While Seeding an IBM DB2 Database .....................147
- Upgrading Fortify Static Code Analyzer from Fortify Audit Workbench .......................148
- Updating Expired Licenses ..............................................................................................150
- Seeding the Database with Seed Bundles Delivered with Quarterly Security Content Releases 151

**Fortify Software Security Center Database Upgrade Tasks**

Upgrade the Fortify Software Security Center database by performing the tasks described in the following table in the order listed.
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Delete the plugin framework folder from your <code>c:\users\&lt;username&gt;\.fortify\plugin-framework</code> or <code>&lt;fortify.home&gt;/plugin-framework</code> folder.</td>
<td><em>Preparing to Upgrade the Fortify Software Security Center Database</em> below</td>
</tr>
<tr>
<td>2</td>
<td>Prepare for the database upgrade.</td>
<td><em>Preparing to Run the Database Upgrade Script</em> on the next page</td>
</tr>
<tr>
<td>3</td>
<td>Configure core Fortify Software Security Center server properties and database settings.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Generate the migration SQL and run the migration SQL script on the database.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Reseed the database.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Undeploy the currently deployed WAR file.</td>
<td>See the documentation for your application server.</td>
</tr>
<tr>
<td>7</td>
<td>Deploy the new WAR file.</td>
<td><em>Updating and Deploying the WAR File</em> on the next page</td>
</tr>
<tr>
<td>8</td>
<td>Update expired licenses.</td>
<td><em>Updating Expired Licenses</em> on page 150</td>
</tr>
<tr>
<td>9</td>
<td>Import your LDAP configuration.</td>
<td><em>Importing an LDAP Server Configuration</em> on page 103</td>
</tr>
</tbody>
</table>

**Preparing to Upgrade the Fortify Software Security Center Database**

The Fortify Software Security Center database migration process creates larger transactions than those created during regular use. For Fortify Software Security Center databases that have been successfully run in production environments, database migration does not typically require changes to your database configuration or resources. For large databases, Fortify recommends that you review and, if necessary, increase the database resources and settings required to accommodate the migration process.
**Note:** Fortify recommends that you delete the plugin framework folder from your c:\users\<username>\.fortify\plugin-framework folder or <fortify.home>\plugin-framework folder before you upgrade.

If you are upgrading a MySQL database, see "Setting the Innodb Buffer Pool Size when Upgrading a MySQL Server Database" below and "Correcting a Case-Insensitive MySQL Database Deployment" on page 54. If you are upgrading a SQL Server database, see "Correcting a Case-Insensitive SQL Server Database Deployment" on page 49.

**Setting the Innodb Buffer Pool Size when Upgrading a MySQL Server Database**

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

For information about how to configure MySQL for use with Fortify Software Security Center, see "Configuring a MySQL Database" on page 52.

**Preparing to Run the Database Upgrade Script**

The Fortify Software Security Center database upgrade scripts require the same database privileges that the database creation scripts require.

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

- Back up your existing Fortify Software Security Center database using your database client tool.
- Acquire the database account information that was used to create the existing Fortify Software Security Center database. See "Database User Account Privileges" on page 47.

**Updating and Deploying the WAR File**

To update the ssc.war file:

1. Undeploy the currently deployed war file. For instructions, see the documentation for your application server.
2. Deploy the new ssc.war file. (See "Deploying Fortify Software Security Center in an Application Server" on page 61 "Deploying Fortify Software Security Center in an Application Server" on page 61.)

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" on the next page and "Additional Fortify Software Security Center Configuration" on page 76.
Configuring Fortify Software Security Center After an Upgrade

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

**Note:** The Setup wizard is available to administrators only, and only after first deployment of Fortify Software Security Center, after an upgrade, or after the server is placed in maintenance mode (see "Placing Fortify Software Security Center in Maintenance Mode" on page 139).

1. After you deploy a new version of the Fortify Software Security Center WAR file in your application server, open a browser window and type your Fortify Software Security Center server URL.

2. Go to the `<fortify.home>/app_context` directory, and open the `init.token` file.

3. Copy the contents of the `init.token` file to the clipboard.

4. In the upper right corner of the Fortify Software Security Center screen, click **Administrators**.
5. Paste the string you copied from the init.token file in the text box, and then click **Sign In**. The Fortify Software Security Center Setup wizard opens.

6. If you need to change any of the configuration settings on the Configuration or Core Settings steps, you can do so using the instructions provided in "Configuring Fortify Software Security Center for the First Time" on page 70. Alternatively, you can import the configuration settings from your existing WAR file, as follows.

   **Note:** You can only import the configuration settings from WAR files for Fortify Software Security Center version v17.10 and earlier installations. These WAR files store the server configuration. Starting with Fortify Software Security Center version 17.20, server configuration settings reside in the fortify.home directory.

   a. On the Start step of the Setup wizard, under **Import existing configuration**, select **click here**.

   b. Navigate to and select your previous version of the ssc.war file. The Setup wizard shows a message to indicate that the WAR file import was successful.

7. On the Fortify Software Security Center Setup wizard, click **Next** until you reach the **Datasource** step.

8. On the **Datasource** step, do the following:

   a. In the **Database username** box, type the username for your Fortify Software Security Center database. For more information, see "Database User Account Privileges" on page 47.

   b. In the **Database password** box, type the password for your Fortify Software Security Center database.

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

   d. In the right panel, click **Download Script**.
The opening ssc-migration.sql dialog box opens.

![Opening ssc-migration.sql dialog box](image)

- Save the ssc-migration.sql script file, and then click **OK**.

9. Run the ssc-migration.sql script. (For instructions, see "About the Fortify Software Security Center Database Tables and the Schema" on page 56.)

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

10. After you run the ssc-migration.sql script, click **Next**.

11. On the **Database Seeding** step, do the following.

   **Note:** If you encounter an error while seeding a DB2 database, see "Troubleshooting an Error Received While Seeding an IBM DB2 Database" on the next page.

   a. In the left panel, use **Browse** to locate and select your process seed bundle zip file, and then click **Seed Database**.

   b. Use **Browse** to locate and select your report seed bundle file, and then click **Seed Database**.

   c. (Optional) Use **Browse** to locate and select your PCI basic seed bundle file, and then click **Seed Database**.

12. Click **Next**.

13. Click **Finish**.

14. Restart your application server container.

   **Note:** If you later find that you need to change any of the configuration settings, you can place Fortify Software Security Center in maintenance mode, and then make any necessary changes. For instructions on how to place Fortify Software Security Center in maintenance mode, see "Placing Fortify Software Security Center in Maintenance Mode" on page 139.

**See Also**

"Configuring Fortify Software Security Center for the First Time" on page 70
Troubleshooting Database Migration Problems

When you use the HPE Security Fortify Software Security Center Setup wizard and you click **Test Connection** on the **Datasource** step, the wizard checks to see whether or not the database upgrade completed successfully. If the configuration wizard detects an error in the upgraded database, it displays the message "Database Validation Failed" or "you have unmigrated process templates."

**Note:** If you are migrating Fortify Software Security Center on a MySQL database, make sure that you have enough space in your MySQL tmp folder. The available disk space must be at least twice the size of the largest table.

Seeding error messages are formatted as follows:

```
ERROR  yyyy-mm-dd hh:mm:ss,nnn
[com.fortify.manager.DAL.impl.GlobalSeedManagerImpl] - Process template [templateName] is not migrated. Please seed the new seed bundle with this template, or update the template through process template designer.
```

If a database validation error message occurs, navigate to the `<fortify.home>/app_context>/logs` directory, open the `ssc-seeding.log` file in a text editor, and look for the cause of the error.

If you can use the information in `ssc-seeding.log` to correct the error, reseed the database with the version 17.10 seed bundles. If you cannot use the information in `ssc-seeding.log` to correct the error, contact HPE Security Technical Support (https://support.fortify.com) for assistance.

Troubleshooting an Error Received While Seeding an IBM DB2 Database

If you encounter an error while reseeding a DB2 database after an upgrade, your database is probably not large enough to process your SQL requests. To remedy this, increase the transaction log size.

To increase the transaction log size:

1. Stop the DB2 server.
2. Start the DB2 Command Editor, and then run the following commands:

```
UPDATE DATABASE CONFIGURATION FOR DATABASE_NAME USING LOGFILSIZ 100000;
```

```
UPDATE DATABASE CONFIGURATION FOR DATABASE_NAME
```
USING LOGPRIMARY 120;

UPDATE DATABASE CONFIGURATION FOR DATABASE_NAME
USING LOGSECOND 120;

3. Restart the DB2 server.
4. Reseed the database.

If reseeding fails, reset LOGFILSZ to a higher value. (On Windows systems, the maximum is 260000.)

See Next
"Updating and Deploying the WAR File" on page 143

See Also
"Troubleshooting Database Migration Problems" on the previous page

Upgrading Fortify Static Code Analyzer from Fortify Audit Workbench

A Fortify Audit Workbench user can check on the availability of new Fortify Static Code Analyzer and associated tools versions from the Fortify Audit Workbench user interface. If a version newer than the one installed is available, the user can download it and upgrade the local instance. A Fortify Audit Workbench user can also configure Fortify Audit Workbench to check for, download, and install new versions automatically at startup.

To enable this functionality for Fortify Audit Workbench users, a Fortify Software Security Center administrator must first set up the auto upgrade capability on the Fortify Software Security Center host machine.

For information about how to upgrade Fortify Static Code Analyzer and its associated tools from Fortify Audit Workbench, see the HPE Security Fortify Audit Workbench Users Guide.

Enabling Fortify Static Code Analyzer Suite Upgrades from Fortify Audit Workbench

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

1. On the Software Security Center host, navigate to the <ssc_install_dir>/WEB-INF/internal directory and open the securityContext.xml file in a text editor.

   Note: <ssc_install_dir> is the directory in which Fortify Software Security Center is deployed. For example, for Tomcat, the <ssc_install_dir> directory is <tomcat>/webapps/ssc.
2. Locate and uncomment the following line:

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

3. Save and close the securityContext.xml file.

4. Navigate to the `<ssc_install_dir>/update-site/installers` directory.

5. Open and read the readme.txt file.

6. In the readme.txt file, copy the sample `update.xml` file content (between and including the `<installerInformation>` and `</installerInformation>` tags).

7. Create a new text file and paste the copied text into it.

8. Update the version information for the installers to reflect your installation. For example:

```xml
<filename>HPE_Security_Fortify_SCA_and_Apps_17.10_windows_x64.exe</filename>
```

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

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

10. Name this file `update.xml` and save it to the `<ssc_install_dir>/update-site/installers` directory.

11. Restart the application server.

12. After you get a new SCA and Apps installer file (HPE_Security_Fortify_SCA_and_Apps_<version>_<OS>), do the following:
   a. Copy the new installer file to the `<ssc_install_dir>/update-site/installers` directory.
   b. Open the `update.xml` file in a text editor.
   c. Between the `versionId` tags, type the version ID for the new installer. (The version ID is the version number without the periods.)

```
    Check to make sure that the `versionId` tag value matches the Fortify Static Code Analyzer version in the installer.
```
   d. Save the edited `update.xml` file.

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

**Note:** The BitRock InstallBuilder tool used for the auto upgrade functionality supports only one Windows tag. If you have different versions of Windows, you must have corresponding configuration files for those versions. For information about how to create the additional configuration files, see the `readme.txt` file located in the `<ssc_install_dir>/update-site/installers` directory.
Updating Expired Licenses

Fortify Software Security Center licenses expire annually. You can get your updated license from the Fortify Customer Portal.

To update an expired Fortify Software Security Center license:

   - If you do not have an account, send an email to Fortify Technical Support (fortifytechsupport@hpe.com).
   - If you encounter a problem logging into your account, send an email to Fortify Technical Support with “Portal Access” as the subject.

2. After you log in to the Customer Portal, at the top of the page, click the My Licenses tab.
   - The Download Licenses page lists all licenses with current maintenance agreements. If you do not see your license, email Fortify Technical Support with “Maintenance Renewal Verification” as the subject. If your maintenance agreement was recently renewed, the Download Licenses page might not yet reflect this.

3. Click the link for the license you want to use.
   - The license is downloaded automatically to your machine.

4. Place your Fortify Software Security Center in maintenance mode. (For instructions, see “Placing Fortify Software Security Center in Maintenance Mode” on page 139.)

5. Go to the <fortify.home>/<app_context> directory, and open the init.token file.

6. Copy the contents of the init.token file to the clipboard.

7. Open a browser window and type your Fortify Software Security Center server URL.

8. In the upper right corner of the page, click Administrators.
9. Paste the string you copied from the init.token file in the text box, and then click **Sign In.**

The Fortify Software Security Center Setup wizard opens.

10. On the Start step, click **Next.**

11. In the left panel of the Configuration step, click **Update.**

12. Browse to and select the new fortify.license file.

13. In the right panel of the Configuration step, select the **I have read and understood this warning** check box.

14. Click **Next** until you reach the final step, and then click **Finish.**

15. To start Fortify Software Security Center in production mode, restart your application server.

### Seeding the Database with Seed Bundles Delivered with Quarterly Security Content Releases

Each quarter, Fortify releases new security content, which may include new seed bundles. Although you cannot reseed the database with these seed bundles using the Setup wizard, you can upload these bundles and reseed the database from the Administration view. For more information about seed bundles and seeding the database, see "About Seeding the Fortify Software Security Center Database" on page 56.

**Note:** Seeding the database blocks the creation of new application versions, and the execution of report jobs and FPR processing jobs.

To seed the database with seed bundles from a quarterly security content release:
1. Acquire seed bundles from a quarterly Security Content release. These may include HP_Fortify_Report_Seed_Bundle_YYYY_QN.zip, HP_Fortify_Process_Seed_Bundle_YYYY_QN.zip, and, optionally, HP_Fortify_PCI_Basic_Seed_Bundle_YYYY_QN.zip files.

2. On the Hewlett Packard Enterprise header, select Administration.

3. In the left panel, select Configuration, and then select Seed Bundles.

4. On the Seed Bundles page, click Browse, and then navigate to and select a seed bundle you obtained in step 1.

5. Click Seed Bundles. 

Fortify Software Security Center displays a message to let you know the bundle upload was successful.

See Also

"About Seeding the Fortify Software Security Center Database" on page 56
Part II: Using Fortify Software Security Center

The following chapters provide information about how to use Fortify Software Security Center.
Chapter 10: Using Fortify Software Security Center

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

This section contains the following topics:

- About the Central Role of Fortify Software Security Center .................................................. 154
- Security Management Workflow .............................................................................................. 155
- User Accounts and Access ......................................................................................................... 155
- About the Fortify Software Security Center Dashboard ................................................................. 160

About the Central Role of Fortify Software Security Center

Fortify Software Security Center provides a location for collecting, correlating, and exporting security analysis results. The Fortify Software Security Center server resides in a central location and receives results from different security activities, such as static, dynamic, and real-time analysis.

Fortify Software Security Center is designed to help you:

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

Fortify Software Security Center works within your organization to answer the following questions:

- How do we drive the adoption of good application security practices?
- How do we get actionable results to development teams?
- Do we measure application teams on a team-by-team basis or as a unit?
- How do we track results over time?
Security Management Workflow

The following figure illustrates the flow of security management processes within Fortify Software Security Center.

As development teams perform scans, they submit periodic scan results from a continuous integration server into Fortify Software Security Center.

Security teams submit periodic results of a dynamic assessment into Fortify Software Security Center.

Fortify Software Security Center correlates and tracks the scan results and assessment results over time, and makes the information available to developers through Audit Workbench, or through IDE plugins such as the Fortify Plugin for Eclipse, the Fortify Package for Visual Studio, and others.

Users can also push issues into defect tracking systems, including HPE ALM, JIRA, TFS/VSTS, and Bugzilla.

User Accounts and Access

Fortify Software Security Center supports two methods of authentication:

- Local user accounts created within the interface
- Active Directory/LDAP accounts associated with standard corporate authentication (Active Directory/LDAP integration supports user assignment by group or organizational unit)
Active Directory/LDAP Integration

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

The user who deploys Fortify Software Security Center must configure the integration with the Active Directory/LDAP during installation. For detailed information, see "Configuring LDAP Servers" on page 94.

See Also

*Registering LDAP Entities" on page 176

"Fortify Software Security Center User Account Management" on page 166

Logging in to Fortify Software Security Center for the First Time

To log in to Fortify Software Security Center, your Fortify Software Security Center administrator must provide you with the URL for your instance, a username, and a password.

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

1. To make sure that you access the newest version of the Fortify Software Security Center user interface, clear your web browser’s cache.

2. In a web browser, type the URL for your Fortify Software Security Center instance, as follows:
   - If Fortify Software Security Center is configured to use secure HTTP protocol, type the following URL:
     https://<host_ip>:<port>/ssc/
     where <port> represents the port number used by your application server.
   - If Fortify Software Security Center is configured to use insecure HTTP protocol (not recommended), type the following URL:
     http://<host_ip>:<port>/ssc/
     where <port> represents the port number used by your application server.
3. In the **Username** and **Password** boxes, type the credentials that your administrator has given you.
4. Click **Log in**.
5. If Fortify Software Security Center prompts you to change your password, do so.

**Requesting Access to Fortify Software Security Center**

If you do not yet have a Fortify Software Security Center user account or if you have forgotten your user name or password, you can request assistance from the Login page.

To request access to Fortify Software Security Center:

1. At the top of the Fortify Software Security Center Login screen, click the **Can't access or need an account?** link.

   **Note:** This link is available only if your Fortify Software Security Center administrator has enabled email notification. (See “Configuring Email Alert Notification Settings” on page 91.)

2. Type your email address, and then click **Submit**.
The Account Request dialog box opens.

3. Provide the required information, and then click **Send**.

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

**Changing Your Password**

To modify your user account information (other than your password), you must use the legacy user interface.

To change your password:

1. Log in to Fortify Software Security Center.

2. At the right end of the Hewlett Packard Enterprise header, click the user profile icon, and then select **Change Password**.
The HPE Security Fortify Software Security Center - Change Password dialog box opens.

For instructions on how to modify your other user account information, see the HP Fortify Software Security Center User Guide: Legacy User Interface.

**Enabling and Disabling Receipt of Email Alerts**

To enable or disable your receipt of email alerts:

1. Log in to Fortify Software Security Center.

2. At the right end of the Hewlett Packard Enterprise header, click the user profile icon, and then select **Preferences**.
3. In the Preferences dialog box, select or clear the Email Alert Notifications check box, and then click Save.

About the Fortify Software Security Center Dashboard

After you log in to Fortify Software Security Center, the Dashboard displays data for the application versions to which you have access and that pose the highest potential business risk to your organization.

Topics covered in this section:

Issue Stats Page ................................................................. 160
Exporting Data to Comma-Separated Values Files .................................. 163
Deactivating Application Versions .................................................... 164
Reactivating Application Versions .................................................... 164

Issue Stats Page

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

**Note:** If you are an administrator or security lead, you can set the thresholds that determine what users see when they review information on the Issue Stats page. For details, see “Configuring Issue Stats Thresholds” on page 77.

If you click an application version listed in the table, Fortify Software Security Center takes you directly to the Audit page for that application version. No filters are applied to the data.
The Dashboard provides three settings that you can use alone or in combination to refine the summary data displayed.

**Selecting a grouping attribute**

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

In addition to the grouping attribute you selected, the resulting data reflects any attributes you have selected from the Aggregate by and Filter by lists.

**Note:** You can achieve finer control over the data displayed if your Group by list includes custom attributes (of the single-select type). For instructions on how to create custom attributes, see "Creating Custom Attributes" on page 184.

**Selecting an aggregating attribute**
To aggregate the data shown on the Dashboard based on a single application attribute, select the attribute from the Aggregate by list. The Dashboard displays your data based on the aggregating attribute, and any attributes you have selected from the Group by and Filter by lists.

**Note:** You can achieve finer control over the data displayed if your Aggregate by list includes custom attributes (of the single-select type). For instructions on how to create custom attributes, see "Creating Custom Attributes" on page 184.

### Selecting one or more filtering attributes

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

The Dashboard displays your data based on the selected filter attributes, and any other attributes you have selected from the Group by and Aggregate by lists.

### Clearing selections from the custom attributes lists

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

You can export Fortify Software Security Center data displayed on the Issue Stats and Audit pages to comma-separated values (CSV) files. For details, see "Exporting Data to Comma-Separated Values Files" on the next page.
Exporting Data to Comma-Separated Values Files

You can export selected Fortify Software Security Center data displayed on the Issue Stats and Audit pages to comma-separated values (CSV) files.

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

1. (Optional) If you are exporting data from the Issue Stats page, you can select attributes to aggregate or filter by. On the Audit page, you can select attributes to filter by.

   **Note:** The Export button is removed if you group issues on either the Issue Stats page or the Audit page.

2. On the toolbar, click **Export**. The Export CSV dialog box opens.
3. In the **File Name** box, type the name for the file.
4. (Optional) In the **Notes** box, type any information about the data you are exporting.
5. Click **Save**.
6. To view the exported result:
   a. On the Hewlett Packard Enterprise header, click **Reports**.
   b. On the Reports page, click **Data Exports**.
   c. In the resulting table, move your cursor to the **File Name** box for the exported file, and then click **Download**.
   d. Specify whether to save or open the file.

To determine how long the system retains your CSV files before they are deleted, see the instructions provided in "Configuring Job Scheduler Settings" on page 111.
Deactivating Application Versions

Deactivating an application version hides that version on the Applications page. If you delete all versions of an application, Fortify Software Security Center automatically deletes the application.

To deactivate a Fortify Software Security Center application version:

1. From the Applications view, select the version name for the application version you want to deactivate.
   Fortify Software Security Center opens the Overview page for the selected version.
2. On the application version toolbar, click Profile.
3. In the Application Profile dialog box, click Application Settings.
4. In the Version Settings panel, click Deactivate.
   Fortify Software Security Center prompts you to confirm that you want to deactivate the version.
5. Click OK.
   The Deactivate button is now the Activate button. If you need to, you can re-activate the version later.
6. Close the Application Profile dialog box.

See Also

"Deleting an Application Version " on page 198

Reactivating Application Versions

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

If the deactivated application version was the only version of the application that exists, you can do one of the following to access and reactivate it:

- Return to the legacy user interface and reactivate it there. (For instructions, see the HP Fortify Software Security Center User Guide for version 4.30.
- Create a new version of the deactivated application, and then follow the procedure described below.

To reactivate an application version when another version of the application exists:

2. In the Applications view, select the Show inactive versions check box.
3. In the table, click the deactivated application version name.
   The Overview page for the selected application version opens.
4. On the application version toolbar, click Profile.
   The Application Profile dialog box opens.
5. Click Application Settings.
6. In the **Other Versions** section, next to the inactive version you want to reactivate, click **Activate**.

   Fortify Software Security Center prompts you to confirm the activation.

7. Click **OK**.

8. Close the Application Profile dialog box.

   The application version is again represented on the Fortify Software Security Center Dashboard and in the Applications view.
Chapter 11: Managing User Accounts

The topics in this chapter provide information about Fortify Software Security Center user accounts and how to work with them.

This section contains the following topics:

- Fortify Software Security Center User Account Management ........................................... 166
- Modifying Your User Account ............................................................................................... 166
- About Tracking Teams ........................................................................................................... 167
- About Roles .......................................................................................................................... 167
- Fortify Software Security Center Account Administration ............................................... 175

Fortify Software Security Center User Account Management

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

Fortify Software Security Center supports several default user roles. The following sections provide information about each of these roles.

This section contains information about Fortify Software Security Center roles, user account administration, and how to register AD/LDAP entities with Fortify Software Security Center.

Modifying Your User Account

To modify your user account information (other than your password), you must use the legacy user interface.
To access the legacy user interface:

1. Log in to Fortify Software Security Center.

2. At the right end of the Hewlett Packard Enterprise header, click the user profile icon, and then select 4.30 UI.

For instructions on how to modify your user account information, see the HP Fortify Software Security Center User Guide for version 4.30.

For instructions on how to change your password, see "Changing Your Password" on page 158.

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 173.

Pre-configured Roles

The following table lists the pre-configured roles you can assign to users in Software Security Center. For information about how to view the permissions associated with each pre-configured role, see "Viewing Permission Information for Fortify Software Security Center Roles" on page 133.
<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Has full access to the system and all results</td>
</tr>
<tr>
<td>Application Security Tester</td>
<td>Performs tasks required to execute dynamic scan requests, including:</td>
</tr>
<tr>
<td></td>
<td>• View application versions</td>
</tr>
<tr>
<td></td>
<td>• View and generate reports</td>
</tr>
<tr>
<td></td>
<td>• Process dynamic scans</td>
</tr>
<tr>
<td></td>
<td>• Upload scan results</td>
</tr>
<tr>
<td></td>
<td>• Audit issues</td>
</tr>
<tr>
<td>Developer</td>
<td>Developer responsible for producing security results and taking action to</td>
</tr>
<tr>
<td></td>
<td>triage or remediate security issues</td>
</tr>
<tr>
<td>Manager</td>
<td>Responsible for guiding developers to work on results</td>
</tr>
<tr>
<td></td>
<td>Managers cannot create applications but can grant or revoke access to</td>
</tr>
<tr>
<td></td>
<td>their team members</td>
</tr>
<tr>
<td>Security Lead</td>
<td>Security team member who can create application versions and users</td>
</tr>
<tr>
<td>View Only</td>
<td>Can view results, but cannot interfere with the issue triage or the</td>
</tr>
<tr>
<td></td>
<td>remediation process.</td>
</tr>
<tr>
<td></td>
<td>Example users: system automation account or temporary auditor</td>
</tr>
<tr>
<td>WebInspect Enterprise System</td>
<td>Can connect a WebInspect Enterprise instance to Fortify Software Security</td>
</tr>
<tr>
<td></td>
<td>Center and retrieve issue audit information.</td>
</tr>
<tr>
<td></td>
<td>This role is intended for use only by a WebInspect Enterprise instance.</td>
</tr>
</tbody>
</table>

See Also

"About Roles" on the previous page
"Creating Custom Roles" on page 173

Role-Based Permissions for Fortify Software Security Center

The following table shows what activities users assigned to various roles can and cannot perform in Fortify Software Security Center. Note that the table does not display permission information for Administrators. Users assigned the Administrator role have permission to perform all activities in Fortify Software Security Center.
<table>
<thead>
<tr>
<th>Activity</th>
<th>Security Lead</th>
<th>Manager</th>
<th>Developer</th>
<th>View Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Logs</td>
<td>View</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Export</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jobs</td>
<td>View</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Filter by</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cancel</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set priority</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance Indicators</td>
<td>View</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Rulepacks</td>
<td>View</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Update</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Export</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Import</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Variables</td>
<td>View</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Alerts</td>
<td>View</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>View others'</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Notify all app version</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Activity</td>
<td>Security Lead</td>
<td>Manager</td>
<td>Developer</td>
<td>View Only</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>---------</td>
<td>-----------</td>
<td>------------</td>
</tr>
<tr>
<td>users</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit own</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit others'</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Delete own</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Delete others'</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Attributes</td>
<td>View</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Custom Tags</td>
<td>View</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Issues</td>
<td>View</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Reports</td>
<td>View</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Activity</td>
<td>Security Lead</td>
<td>Manager</td>
<td>Developer</td>
<td>View Only</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>---------</td>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td>Delete</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Download</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Libraries</td>
<td>View</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Delete</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Import</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Download</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local</td>
<td>View</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Create</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>View</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Create</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Refresh</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roles</td>
<td>View</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Create</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity</td>
<td>Security Lead</td>
<td>Manager</td>
<td>Developer</td>
<td>View Only</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------</td>
<td>---------</td>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td>Edit</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration</td>
<td>View</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Reports</td>
<td>View</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>View others'</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Download</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Delete own</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Delete others'</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dashboard</td>
<td>View</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Create application</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Todo</td>
<td>This user only</td>
<td>This user only</td>
<td>This user only</td>
</tr>
<tr>
<td></td>
<td>Activity Feed</td>
<td>This user only</td>
<td>This user only</td>
<td>This user only</td>
</tr>
<tr>
<td>Version Dashboard</td>
<td>Create new version</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Scan artifacts</td>
<td>Upload</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Download app file</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Download</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Activity

<table>
<thead>
<tr>
<th>Activity</th>
<th>Security Lead</th>
<th>Manager</th>
<th>Developer</th>
<th>View Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Purge</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Approve</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Audit</td>
<td>Assign users</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Claim</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>File bugs</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Suppress</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Add comments</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Profile</td>
<td>Advanced options</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Custom tags</td>
<td>Yes</td>
<td>Yes</td>
<td>View only</td>
</tr>
<tr>
<td></td>
<td>Processing Rules</td>
<td>Yes</td>
<td>Yes</td>
<td>View only</td>
</tr>
<tr>
<td></td>
<td>Bug Tracker</td>
<td>Yes</td>
<td>Yes</td>
<td>View only</td>
</tr>
<tr>
<td></td>
<td>Application Settings</td>
<td>Yes</td>
<td>Yes</td>
<td>View only</td>
</tr>
</tbody>
</table>

### See Also

- "Pre-configured Roles" on page 167
- "Viewing Permission Information for Fortify Software Security Center Roles" on page 133

### Creating Custom Roles

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

To define and configure permissions for a new role:

1. Log in to Fortify Software Security Center as an Administrator, and then, on the Hewlett Packard Enterprise header, click **Administration**.
2. In the left panel of the **Administration** page, select **Users**, and then select **Roles**.
3. In the **Roles** toolbar, click **New**.
   The Create New Role dialog box opens.

4. Provide the information described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Role name</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional, but recommended) Role description</td>
</tr>
<tr>
<td>Universal Access</td>
<td>To assign the new role access to all application versions and runtime applications, select this check box.</td>
</tr>
</tbody>
</table>

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

5. To add permissions (specify the functional areas available to users in this role), click **+ Add Permissions**.
   The Add Permissions dialog box opens.

6. Scroll through the table and select the check boxes that correspond to the permissions that you want to grant to the new role.

7. Click **Done**.

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

**Deleting Custom Roles**

If a custom role listed on the Roles page is assigned to no user accounts, you can delete that role.

To delete a role:

1. Log in to Fortify Software Security Center as an Administrator or Security Lead, and then click **Administration**.
2. In the left panel of the Administration view, select **Users**, and then select **Roles**.
3. In the table, click the check box for the custom role you want to delete.
4. In the **Roles** toolbar, click **Delete**.
   Fortify Software Security Center prompts you to confirm that you want to delete the role.
5. Click **OK**.

**See Also**

“Creating Custom Roles” on the previous page
Fortify Software Security Center Account Administration

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

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

Topics covered in this section:

Creating Local User Accounts ................................................................. 175
Registering LDAP Entities ................................................................. 176
Unlocking User Accounts (Local Users Only) .................................................. 179

Creating Local User Accounts

Fortify Software Security Center Administrator-level users can add new local user accounts to the list of Fortify Software Security Center users.

To create an Fortify Software Security Center user account:

1. Log in to Fortify Software Security Center as an Administrator, and then click Administrator.
2. In the left panel of the Administration view, select Users, and then select Local. The Local page opens and lists local users.
3. In the Local toolbar, click New. The Create New User dialog box opens.
4. Provide the information listed in the following table.

<table>
<thead>
<tr>
<th>Field or Check Box</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Username for Fortify Software Security Center logon.</td>
</tr>
<tr>
<td>First Name</td>
<td>First name of user.</td>
</tr>
<tr>
<td>Last Name</td>
<td>Last name of user.</td>
</tr>
<tr>
<td>Email</td>
<td>Email address of user.</td>
</tr>
<tr>
<td>Roles</td>
<td>Select the check boxes that correspond to the roles you want to assign to the user.</td>
</tr>
<tr>
<td>Field or Check Box</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the new user.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Password for the new user.</td>
</tr>
<tr>
<td>User must change password at next login</td>
<td>Select this check box to require the user to change the password at the next login to Fortify Software Security Center.</td>
</tr>
<tr>
<td>Password never expires</td>
<td>Select this check box to allow the user to use the originally assigned password until he wants to change it. To require the user to change his or her password every thirty days, leave this check box cleared.</td>
</tr>
<tr>
<td>Suspended</td>
<td>Select this check box to suspend user access to Fortify Software Security Center.</td>
</tr>
</tbody>
</table>

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

6. Do one of the following:
   - To save your settings and exit the Create New User dialog box, click **Save**.
   - To save your settings and create another new user, click **Save and Add Another**.

Fortify Software Security Center adds the user account to the list of users.

**Registering LDAP Entities**

Users who have Administrator-level accounts can add LDAP groups, organizational units, and users to the list of Fortify Software Security Center users. Fortify Software Security Center automatically updates access control as users join and leave groups.
To register an LDAP organizational unit, group, or user with Fortify Software Security Center:

1. Log in to Fortify Software Security Center as an Administrator, and then, on the Hewlett Packard Enterprise header, click Administration.
2. In the left panel, click Users, and then select LDAP.
3. On the LDAP toolbar, click Add.
   The Add New LDAP Entity window opens.

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

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

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

   a. Click **Add**.

   ![Select Application Version dialog box](image)

   The Select Application Version dialog box opens.

   b. From the **Application** list, select the name of an application that you want the LDAP entity to access.

   The **Versions** section lists all active versions of the application.

   c. To display inactive versions of the application, select the **Show Inactive Versions** check box.

   d. In the **Versions** section, select the check boxes for all of the versions that you want the entity to access.

   e. Click **Done**.

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

8. Do one of the following:

   - To save your changes and close the Add New LDAP Entity dialog box, click **Save**.

   - To save your changes and register another LDAP entity, click **Save And Add Another**.

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

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

9. To initiate the LDAP refresh process manually so that your changes are evident sooner than they would be otherwise:
a. On the LDAP page, select the check box for the LDAP entity you want to refresh.

b. On the LDAP toolbar, click **Refresh**.

For information about how to configure LDAP servers, see "Configuring LDAP Servers" on page 94.

**See Also**

"LDAP User Authentication" on page 57

"About Managing LDAP User Roles" on page 135

**Unlocking User Accounts (Local Users Only)**

After a local user tries unsuccessfully to log in to Fortify Software Security Center more than three times in a row, Fortify Software Security Center prevents the user from attempting more logons. If email notifications are enabled, the user receives an email to advise the user that he or she is locked out and should notify the Fortify Software Security Center administrator. As an administrator, you can unlock the account for the user.

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

1. On the Hewlett Packard Enterprise header, select **Administration**.
2. In the left panel of the Administration view, select **Users**, and then click **Local**.
3. Bring up the locked user account, expand the row to view account details, and then click **Edit**.
   
   At the bottom left, the message **User has reached the maximum login attempts** is displayed.

4. To the right of the message, click **unlock**.
   
   Fortify Software Security Center prompts you to confirm that you want to unlock the account.

5. Click **Yes**.

6. Click **Save**.
Chapter 12: Applications and Application Versions

To obtain consistent measurement results in Fortify Software Security Center, you define an application for a single code base. Fortify Software Security Center organizes the iterative development and remediation of code bases into applications and application versions.

- An application is a code base that serves as a container for one or more application versions. If you are working with a new code base, you create a new Fortify Software Security Center application. Fortify Software Security Center automatically creates the first version of that application.
- An application version is an instance of the application or code base that is to eventually be deployed. It contains the data, auditing, and attributes for a particular version of the application code base. If you are working with an existing code base, you create new application versions rather than new applications.

An application version is the base unit for team tracking. It provides a destination for security results that is useful for getting information in front of developers and producing reports and performance indicators. Code analysis results for an application version are tracked as shown in the following table.

<table>
<thead>
<tr>
<th>Existing Analysis Results</th>
<th>+ New Scan Results</th>
<th>= Trending Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Results of any previous security analysis from Fortify Static Code Analyzer, Fortify WebInspect, or other analyzer</td>
<td>Merge with the existing results (from the same analyzer used to perform this scan)</td>
<td>Identify security issues that have been fixed, and issues that remain.</td>
</tr>
<tr>
<td></td>
<td>Mark resolved issues</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identify new issues</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Keep unchanged issues</td>
<td></td>
</tr>
</tbody>
</table>

Fortify Software Security Center analysis processing rules verify that the new scan is comparable to the older scan.

This content provides information about applications and application versions. It contains instructions for viewing and creating applications, configuring application attributes, assigning issue templates, and more.

This section contains the following topics:

About Tracking Development Teams ................................................................. 181
About Creating Application Versions .......................................................... 183
Searching Applications and Application Versions from the Applications View ............. 195
About Tracking Development Teams

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

Topics covered in this section:

- About the Application Creation Process ................................................................. 181
- Strategies for Creating Application Versions ......................................................... 182
- About Annotating Application Versions for Reporting .............................................. 182
- Viewing a List of Fortify Software Security Center Applications ............................... 182

About the Application Creation Process

After you log in to Fortify Software Security Center and start to add a new application, the Create New Application wizard displays a sequence of steps, each of which presents the team members responsible for creating the application version with one or more strategic choices. After the team agrees upon and makes their selections, the security lead can click Finish to complete the creation process.

Typically, the security team evaluates and decides on all the options before they actually start to create the application version. The following sections describe the options displayed on the creation wizard screens.

Next

"Application Version Attributes" on page 183

See Also

"Template Selection" on page 188
Strategies for Creating Application Versions

As a Security Lead, you might choose to create an application version that allows you to track vulnerabilities within deployed applications. Security vulnerabilities often occur in areas of code where different components come together. Although teams may work on different components, it is a good practice to track the entire software component as one piece. As an example, suppose that a text manipulation library is safe on its own, and a file access library is safe on its own. The combination of the text manipulation library and file access library is not necessarily safe, because one may not know the origin of the text being processed.

Strategies for Packaged Software

For software that ships or is deployed as a concrete version, you might use the following strategies:

- If you are creating a brand new application, start a new application version.
- Create a single application version for each release. For example, the Security Lead or Development Manager may deactivate past versions in Software Security Center to archive results and remove them from view.
- If you are working on an existing application with an evolving code base, create an application version based on an existing version. For example, Application A has several versions. Each new version is initiated based on the results of the previous version. Each successive version is just evolved code (versus a complete rewrite).

Strategies for Continuous Deployment

For applications that use continual deployment, running scans with the -build-label xxxx flag enables you to identify which source control checkout was scanned (where xxxx represents the ID from your version control system). Relating scans to source control checkout improves your ability to determine when individual issues were introduced and remediated.

About Annotating Application Versions for Reporting

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

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

Viewing a List of Fortify Software Security Center Applications

To view a list of all Fortify Software Security Center applications:

- On the Hewlett Packard Enterprise header, click Applications.
"Displaying Additional Application Versions on the Dashboard" on page 238

"Searching Applications and Application Versions from the Applications View" on page 195

About Creating Application Versions

You can create a new Fortify Software Security Center application version for an entirely new application or create one for existing application version. The following topics provide instructions for each method:

"About the Application Creation Process" on page 181

"Creating the First Version of a New Application" on page 189

"Adding a New Version to an Application" on page 192

Application Version Attributes

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

When you create a new application version, the Create New Version wizard guides you through the selection of required and optional business, technical, and organization application attributes. The application version type cannot be finished until you select values for all required attributes. For example, to create an application version, you must specify values for the following attributes:

- Development phase
- Development strategy
- Accessibility

In addition to the default attributes that Fortify Software Security Center provides, Administrators and Security Leads can create custom attributes to assign to application versions. Custom attributes are extremely useful when you need to focus on a highly specific subset of data. For instructions on how to create custom attributes, see "Creating Custom Attributes" on the next page.

The following table lists the default set of attributes for Fortify Software Security Center applications. Note that this list does not include custom attributes that a Fortify Software Security Center administrator may have added to the system. Attributes marked with an asterisk are required.

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

<table>
<thead>
<tr>
<th>Technical Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*Development Phase</td>
<td>Current phase of development the application version is in.</td>
</tr>
<tr>
<td><strong>Technical Attribute</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>*Development Strategy</td>
<td>Staffing strategy used for application development</td>
</tr>
<tr>
<td>*Accessibility</td>
<td>Level of access required to use the application</td>
</tr>
<tr>
<td>Application Type</td>
<td>Nature of the code base (library, application, or application component)</td>
</tr>
<tr>
<td>Target Deployment Platform</td>
<td>Deployment platform for the application</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Interfaces used to access the application</td>
</tr>
<tr>
<td>Development Languages</td>
<td>Languages used to develop the application</td>
</tr>
<tr>
<td>Authentication System</td>
<td>System used to authenticate users who try to access to the application</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Organization Attributes</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Unit</td>
<td>Business unit for which the application is to be developed or business unit to develop the application</td>
</tr>
<tr>
<td>Industry</td>
<td>Industry for which the application is to be developed</td>
</tr>
<tr>
<td>Region</td>
<td>Geographical location of the development team</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Business Risk Attributes</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Known Compliance Obligations</td>
<td>All known compliance obligations that the application must meet</td>
</tr>
<tr>
<td>Data Classification</td>
<td>Types data to be stored by this application</td>
</tr>
<tr>
<td>Application Classification</td>
<td>Direct consumers of the application</td>
</tr>
</tbody>
</table>

**Creating Custom Attributes**

Fortify Software Security Center comes with technical, organization, and business attributes that enable administrators and security leads to categorize applications and application versions. As an administrator or a security lead, you can create your own custom attributes that can be set for application versions.
**Note:** You can create custom attributes only if you have either an Administrator or Security Lead user account.

To create an attribute:

1. Log in to Fortify Software Security Center as an administrator or a security lead.
2. On the Hewlett Packard Enterprise header, click **Administration**.
3. In the left panel, under **Templates**, click **Attributes**.
   Fortify Software Security Center lists the attributes in a table to the right.
4. Click **New**.
   The Create New Attribute dialog box opens.

5. Provide the information described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a descriptive name for the attribute.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a brief description. The description is displayed under the attribute field in the Create New Application wizard.</td>
</tr>
<tr>
<td>Required</td>
<td>Select this check box to require users to set the attribute that you are defining here when they create an application template.</td>
</tr>
<tr>
<td>Hidden</td>
<td>Select this check box to prevent the new attribute from being displayed in the Create New Application wizard.</td>
</tr>
<tr>
<td>Category</td>
<td>Select <strong>Technical</strong>, <strong>Business</strong> or <strong>Organization</strong> to specify the attribute type. Depending on the category you select, the attribute is displayed on the <strong>Business Attributes</strong> step, the <strong>Technical Attributes</strong> step, or the</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
**Organization Attributes** step of the Create New Application wizard.  
**Note:** If your Fortify Software Security Center instance is integrated with Fortify WebInspect, the list also includes the **Dynamic Scan Request** category.

| Scope | Select the value that indicates whether the attribute applies only to application versions, runtime applications, or to both. |

| Type | Select one of the following control types:  
- To create a check box for the attribute, select **Boolean**.  
- To create a calendar selection control for the attribute, select **Date**.  
  
  **Note:** This type is not available for a Dynamic Scan Request attribute.  
- To create a list from which a user can select only a single value for the attribute, select **List of Values - Single Selection**.  
  
  **Note:** If you create a single-select type attribute, users can select it from the **Group by** and **Aggregate by** lists on the Dashboard to customize the data they view.  
- To create a list from which a user can select multiple values for the attribute, select **List of Values - Multiple Selection**.  
- To create a field that accepts an integer value, select **Integer**.  
- To create a text field into which a user can type a single line of text, select **Text - Single Line**.  
- To create a text field into which a user can type multiple lines of text, select **Text - Multiple Lines**.  
  
  **Note:** If you select one of the **List of Values** types, additional fields are displayed in which you add the values and their descriptions, and specify whether or not they are hidden. |

6. Click **Save**.  
The new attribute is available the next time a user uses the Create New Application wizard.
For instructions on how to specify custom attributes in existing application versions, see “Specifying New Custom Attributes in Existing Application Versions” below.

**See Also**

"Application Version Attributes" on page 183

**Specifying New Custom Attributes in Existing Application Versions**

To apply a new custom attribute to existing application versions:

2. On the Applications page, select the application version for which you want to specify a new attribute.
   Fortify Software Security Center displays the Audit page for that version.
3. On the application version toolbar, select Profile.
   The Application Profile - `<application_name>` window opens to the Advanced Options section.
4. Click Application Settings.
5. In the Version Settings section, click the edit icon.
   The Edit Version wizard opens to Step 1. General.
6. Click Next Step.
7. On Step 2. Define Attributes and Risk, select the attribute category (Technical Attributes, Organization Attributes, or Business Risk Attributes), and then select the value or values for the custom attribute.
8. Navigate to Step 4 of the wizard, and then click Finish.

**See Also**

"Creating Custom Attributes" on page 184

"Editing Application Version Details" on page 195

**About Issue Templates**

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

An issue template contains the following settings:

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

Fortify Software Security Center comes with pre-designed issue templates that you can either use as they are, or modify (from Fortify Audit Workbench) to suit your application needs.

To see descriptions of these out-of-the-box issue templates:
1. On the Hewlett Packard Enterprise header, select **Administration**.
2. In the left panel, select **Templates**, and then select **Issue**.

The Issue page lists the issue templates and their descriptions.

You can import a Fortify Software Security Center issue template into Fortify Audit Workbench, modify it, save it with a new name, and then import it into Fortify Software Security Center. You can also create a new issue template from scratch in Fortify Audit Workbench. For instructions on how to modify or create an issue template in Fortify Audit Workbench, see the *HPE Security Fortify Audit Workbench User Guide*. For instructions on how to import a new or modified issue template into Fortify Software Security Center, see "Adding Issue Templates to the System" below.

**Adding Issue Templates to the System**

To add an issue template that was created or modified in Fortify Audit Workbench to Fortify Software Security Center:

1. Log in to Fortify Software Security Center as an administrator.
2. On the Hewlett Packard Enterprise header, click **Administration**.
3. In the panel on the left, select **Templates**, and then select **Issue**.
   Fortify Software Security Center lists the system issue templates in a table to the right.
4. Click **New**.
   The Create New Issue Template dialog box opens.
5. In the **Name** box, type the template name.
6. Click **Browse**, and then locate and select the new or modified template.
7. (Optional) In the **Description** box, type a description that lets users know how to use the template.
8. Click **Save**.

**See Also**

"About Issue Templates" on the previous page

**Template Selection**

Fortify Software Security Center issue templates provide Fortify client and server products an optimal means of categorizing, summarizing, and reporting application data. Issue templates also enable the use of customized application settings at the enterprise level and not just at the application level.

Although you can change the issue template for an application after you finish creating the application, your security team must carefully consider its choice of template before completing the application creation process.
Creating the First Version of a New Application

A Fortify Software Security Center application version consists of the data and attributes for a given variant of the application code base. The following procedure describes how to create the first version of a new application.

To create a new application:

1. Log in to Fortify Software Security Center as either an Administrator or a Security Lead.
2. In the toolbar, click + New Application.
   The Create New Application wizard opens to Step 1. General.
3. In the Application Setup section, do the following:
   a. In the Application Name box, type a name for the new application.
   b. (Optional) in the Application Description box, type a description.
4. In the Version Setup section, provide the information described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version Name</td>
<td>Type a name for the version. The wizard uses the application name and appends the version name to it automatically.</td>
</tr>
<tr>
<td>Version Description</td>
<td>(Optional)</td>
</tr>
<tr>
<td>Use Existing Application Version</td>
<td>a. To use the settings of an existing application version, select this check box. Otherwise, proceed to step 5.</td>
</tr>
<tr>
<td></td>
<td>b. To open the Select Application Version dialog box, click Browse.</td>
</tr>
<tr>
<td></td>
<td>c. From the Applications list, select the application.</td>
</tr>
<tr>
<td></td>
<td>d. From the Versions list, select the row that displays the version name you want, and then click Done.</td>
</tr>
<tr>
<td></td>
<td>By default, Fortify Software Security Center includes all settings of the selected application version.</td>
</tr>
<tr>
<td></td>
<td>e. To exclude some of the settings, clear one or more of the following check boxes:</td>
</tr>
<tr>
<td></td>
<td>○ Version Attributes</td>
</tr>
<tr>
<td></td>
<td>○ Custom Tags</td>
</tr>
<tr>
<td></td>
<td>○ Analysis Processing Rules</td>
</tr>
<tr>
<td></td>
<td>○ User Access Settings</td>
</tr>
<tr>
<td></td>
<td>○ Bug Tracker Settings</td>
</tr>
</tbody>
</table>
5. To advance to **Step 2. Define Attributes and Risk**, click **Next Step**.

6. In the **Technical Attributes** section, provide the information described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development Phase</td>
<td>Leave <strong>New</strong> selected.</td>
</tr>
<tr>
<td>Development Strategy</td>
<td>Select the strategy used to develop the application version.</td>
</tr>
<tr>
<td>Accessibility</td>
<td>Select the value that specifies how the application is to be accessed.</td>
</tr>
<tr>
<td>Application Type</td>
<td>Select the application type.</td>
</tr>
<tr>
<td>Target Deployment Platform</td>
<td>Select the target deployment platform.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Select the check boxes for the interfaces available to access the application.</td>
</tr>
<tr>
<td>Development Languages</td>
<td>Select the check boxes for the languages used to develop the application version.</td>
</tr>
<tr>
<td>Authentication System</td>
<td>Select the check boxes for the authentication systems used to access the application.</td>
</tr>
</tbody>
</table>

7. Click **Organization Attributes**, and then provide the information described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Unit</td>
<td>Select the business unit for which the application version is being developed.</td>
</tr>
<tr>
<td>Industry</td>
<td>Select the industry sector to which the application version applies.</td>
</tr>
<tr>
<td>Region</td>
<td>Select the region for which the application version is being developed.</td>
</tr>
</tbody>
</table>

8. Click **Business Risk Attributes**, and then provide the information described in the following
table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known Compliance Obligations</td>
<td>Select the check boxes for all of the known compliance obligations that the application version must meet.</td>
</tr>
<tr>
<td>Data Classification</td>
<td>Select the check boxes for all of the data classifications that apply to the application version.</td>
</tr>
<tr>
<td>Application Classification</td>
<td>Select the check boxes for all of the application classifications that apply to this application version.</td>
</tr>
</tbody>
</table>

9. Click **Next Step**.
10. In the **Issue Template** section, select the check box for a template to set the minimum thresholds for issue detection. To see a description of each template, select its check box.

   A thumbs-up icon (👍) is displayed next to the issue template that Fortify recommends based on your selections.

11. To advance to **Step 4. Assign Responsibilities and Team** section, click **Next Step**.
12. In the **Assign Responsibilities** section, click **Project Manager**, **Security Manager**, **Development Manager**, or **Team**.
13. In the **Assign Team** section, do one of the following:
   a. To assign a user from the Fortify Software Security Center database, leave **Local** selected.
   b. Select the check box for the team member or members you want to assign.

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

   Alternatively,
   a. To assign a user from the LDAP directory (if LDAP authentication is configured for your Fortify Software Security Center server), click **LDAP**, and then, from the **View by** list, select the attribute to use to display LDAP entities.
   b. Select the check box for the team member or members you want to assign.

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

14. Click **Finish**.

   Fortify Software Security Center indicates that the application was successfully created and adds the new application version to the application versions list.
Adding a New Version to an Application

A version consists of the data and attributes for a given variant of the application code base. The following procedure describes how to create a new version of an existing application.

To create a new version of an existing application:

1. Log in to Fortify Software Security Center as either an Administrator or Security Lead.
2. On the Hewlett Packard Enterprise header, click Applications.
3. On the Applications page, select a version of the application for which you want to create a new version.
   Fortify Software Security Center displays the Audit page for that version.
   The Create New Version wizard opens to Step 1. General.
5. In the Version Setup section, do the following:
   a. In the Version Name box, type a name for the new version.
      The wizard uses the application name and appends the version name to it automatically.
   b. In the Version Description box, type a description of the new version.
   c. If you prefer to specify all of the attributes of the new version manually, proceed to apply the setting of an existing application version to the new version:
      i. Select the Use Existing Application Version check box.
      ii. Click Browse, and then navigate to and select the application version with the attribute settings you want to apply to the new version.
      iii. Clear any of the following check boxes for the settings that you do not want to apply to this version:
         - Version Attributes
         - Custom Tags
         - Analysis Processing Rules
         - User Access Settings
         - Bug Tracker Settings
6. To advance to Step 2. Define Attributes and Risk, click Next Step.
7. From the Business Risk Rating list, select the level of risk that this application version poses to the organization's business goals.
8. In the Technical Attributes section, provide the information described in the following table.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development Phase</td>
<td>From this list, select the current development phase of the new version.</td>
</tr>
<tr>
<td>Development Strategy</td>
<td>Select the strategy used to develop the application version.</td>
</tr>
<tr>
<td>Accessibility</td>
<td>Select the value that specifies how the application is to be accessed.</td>
</tr>
<tr>
<td>Application Type</td>
<td>Select the application type.</td>
</tr>
<tr>
<td>Target Deployment Platform</td>
<td>Select the target deployment platform.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Select the check boxes for the interfaces available to access the application.</td>
</tr>
<tr>
<td>Development Languages</td>
<td>Select the check boxes for the languages used to develop the application version.</td>
</tr>
<tr>
<td>Authentication System</td>
<td>Select the check boxes for the authentication systems used to access the application.</td>
</tr>
</tbody>
</table>

9. Click **Organization Attributes**, and then provide the information described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Unit</td>
<td>Select the business unit for which the application version is being developed.</td>
</tr>
<tr>
<td>Industry</td>
<td>Select the industry sector to which the application version applies.</td>
</tr>
<tr>
<td>Region</td>
<td>Select the region for which the application version is being developed.</td>
</tr>
</tbody>
</table>
10. Click **Business Risk Attributes**, and then provide the information described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known Compliance Obligations</td>
<td>Select the check boxes for all of the known compliance obligations that the application version must meet.</td>
</tr>
<tr>
<td>Data Classification</td>
<td>Select the check boxes for all of the data classifications that apply to the application version.</td>
</tr>
<tr>
<td>Application Classification</td>
<td>Select the check boxes for all of the application classifications that apply to this application version.</td>
</tr>
</tbody>
</table>

11. To advance to **Step 3. Choose Templates**, click **Next Step**.

12. In the **Issue Template** section, select the check box for a template to set the minimum thresholds for issue detection. To see a description of each template, select its check box. A thumbs-up icon is displayed next to the issue template that Fortify recommends based on your selections. (Also see "Template Selection" on page 188.)

13. To advance to **Step 4. Assign Responsibilities and Team** section, click **Next Step**.

14. In the **Assign Responsibilities** section, select one or more of the following roles:
   - Project Manager
   - Security Manager
   - Development Manager
   - Team

15. In the **Assign Team** section, do one of the following:
   - To assign a user from the Fortify Software Security Center database, leave **Local** selected, and then select the check box for the team member or members you want to assign.

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

   Or,
   a. To assign a user from the LDAP directory (if LDAP authentication is configured for your Fortify Software Security Center server), click **LDAP**, and then, from the **View by** list, select the attribute to use to display LDAP entities.
   b. Select the check box for the team member or members you want to assign.

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

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

**Searching Applications and Application Versions from the Applications View**

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

1. In the **Search Apps and Versions** box above the **Applications** table, type at least part of the application name or version name for the application or version you want to find.
2. Click **Find**. The **Applications** table lists all application versions that match your search string.
3. To return to the complete **Applications** table, clear the text in the search box.

**See Also**

"Searching Globally in Fortify Software Security Center" on page 270

**Updating the Application Overview Page**

If an application version has pending audit information, its **Overview** page heading displays the "more information" icon.

To recalculate the metrics for the application:

- Click the icon, and then, in the Refresh application metrics dialog box, click **Refresh now**.

The metrics refresh may take some time, depending on current system activity. After the refresh is complete, the **Overview** page displays the latest data for the application.

**Note:** Metrics are also refreshed automatically according to the system schedule.

**Editing Application Version Details**

To edit the details of an application version:

1. From the Dashboard, click **Applications**.
2. In the **Applications** table, select the version you want to edit.
3. To the right of the Overview heading, click the pencil icon. The Edit Version wizard opens.
4. Edit values in any of the fields described in "Adding a New Version to an Application" on
5. After you make your changes, advance to Step 4, and then click Finish.

See Also

"Changing the Template Associated with an Application Version" on page 205

About Deleting Application Versions

You cannot directly delete an application in Fortify Software Security Center. Fortify Software Security Center removes an application automatically after all of its versions are deleted.

If you are assigned the Administrator role in Fortify Software Security Center, you can delete any application version. If you are in the Security Lead or Manager role, then you can delete any application version to which you are assigned.

If you would rather not delete a version, but prefer instead to remove it from display on the Dashboard and Applications pages, you can deactivate it. For instructions on how to deactivate an application version, see "Deactivating Application Versions" below.

See Also

"Deleting an Application Version" on page 198

Deactivating Application Versions

Deactivating an application version hides that version on the Applications page. If you delete all versions of an application, Fortify Software Security Center automatically deletes the application.

To deactivate a Fortify Software Security Center application version:

1. From the Applications view, select the version name for the application version you want to deactivate.
   Fortify Software Security Center opens the Overview page for the selected version.
2. On the application version toolbar, click Profile.
3. In the Application Profile dialog box, click Application Settings.
4. In the Version Settings panel, click Deactivate.
   Fortify Software Security Center prompts you to confirm that you want to deactivate the version.
5. Click OK.
   The Deactivate button is now the Activate button. If you need to, you can re-activate the version later.
6. Close the Application Profile dialog box.

See Also

"Deleting an Application Version" on page 198
Reactivating Application Versions

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

If the deactivated application version was the only version of the application that exists, you can do one of the following to access and reactivate it:

- Return to the legacy user interface and reactivate it there. (For instructions, see the *HP Fortify Software Security Center User Guide* for version 4.30.
- Create a new version of the deactivated application, and then follow the procedure described below.

To reactivate an application version when another version of the application exists:

1. On the Hewlett Packard Enterprise header, click **Applications**.
2. In the Applications view, select the **Show inactive versions** check box.
3. In the table, click the deactivated application version name. The Overview page for the selected application version opens.
4. On the application version toolbar, click **Profile**. The Application Profile dialog box opens.
5. Click **Application Settings**.

6. In the **Other Versions** section, next to the inactive version you want to reactivate, click **Activate**.
Fortify Software Security Center prompts you to confirm the activation.

7. Click **OK**.

8. Close the Application Profile dialog box.

The application version is again represented on the Fortify Software Security Center Dashboard and in the Applications view.

**Deleting an Application Version**

If you would rather not delete an application version, but prefer instead to remove it from display on the Fortify Software Security Center Dashboard and in the Applications view, see “Deactivating Application Versions” on page 196

---

**Important:** If you delete all versions of an application, Fortify Software Security Center automatically deletes the application.

To delete a Fortify Software Security Center application version:

1. From the Applications view, select the name of the application version you want to delete.
   Fortify Software Security Center opens the Overview page for the selected version.

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

3. In the Application Profile dialog box, click **Application Settings**.

4. In the **Version Settings** panel, click **Delete**.
   Fortify Software Security Center prompts you to confirm that you want to delete the version.

5. Click **OK**.
   Fortify Software Security Center removes the version from the database.

---

**Using Bug Tracking Systems to Help Manage Security Vulnerabilities**

Developers fixing software defects often use a bug tracking system to help manage their workload. Security vulnerabilities are a type of bug, and getting vulnerability information into the bug tracking system helps developers take appropriate remediation measures, in line with other development activities. The result is more security awareness and faster remediation of security issues.

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

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

- Details that describe the type of issue uncovered
- Remediation guidance, with instructions on the action to take
- A link back to Software Security Center for complete issue details
Topics covered in this section:

Bug Tracker Configuration ................................................................. 199
Velocity Templates for Bug Filing ......................................................... 199
Submitting a Bug for One or More Issues ............................................. 203

Bug Tracker Configuration

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

If you are a security lead or development manager, you can enable team access to your bug tracking system as follows:

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

See Also

“Velocity Templates for Bug Filing" below

Velocity Templates for Bug Filing

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

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

Note: The velocity templates feature is only available for bugs that you file from the HTML interface. This feature is not available in the legacy user interface.

This section contains the following topics:

“Adding Velocity Templates to Bug Tracker Plugins" on the next page
“Editing Velocity Templates for Bug Tracker Plugins" on page 202
“Deleting Velocity Templates" on page 202
Adding Velocity Templates to Bug Tracker Plugins

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

**Important:** Before you add a new template or edit an existing one, make sure that you review the pre-defined templates carefully to understand how to correctly reference variables within the template.

As you create (or edit) a template, keep the following in mind:

- To avoid runtime errors, Fortify strongly recommends that you validate variables in your template before you render them. (See the pre-defined templates for examples of how to use a macro.)

- Use conditionals if you want to render content differently for a single-issue bug (as opposed to a bug that includes multiple issues).

To add a Velocity template to a bug tracker plugin:

1. On the Hewlett Packard Enterprise header, select **Administration**.
2. In the left panel of the Bug Filing page, select **Templates**, and then select **Bug Filing**.
3. In the table, click the name of 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**.

   ![Add field button]

5. Click **Add field**.
   - The Add template dialog box opens.
6. In the **Mapped field** box, type the name of the field to map, as it appears in the bug tracker plugin dialog box.

   **Note:** You can map only text-based fields.
The following screen capture shows an example of a bug filing dialog box with a couple of mapped fields.

7. In the **Template** box, type your Velocity Template Language (VTL) statement for the mapping.

   (To access 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 available variables, click **Show variables**.)

   **Note:** Not all variables are available for all issues. In particular, verbose content such as “ATTRIBUTE_COMMENTS,” “ISSUE_DETAIL,” and “ISSUE_RECOMMENDATION” are available only if you are filing a bug for a single issue.

8. Click **Apply**.

9. To add another template, repeat steps 5 through 8.

10. Click **Save**.

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

**See Also**

"Bug Tracker Configuration" on page 199

"Velocity Templates for Bug Filing" on page 199

"Editing Velocity Templates for Bug Tracker Plugins" on the next page

"Deleting Velocity Templates" on the next page
Editing Velocity Templates for Bug Tracker Plugins

To edit the Velocity template for a bug tracker plugin:

1. On the Hewlett Packard Enterprise header, select Administration.
2. In the left panel of the Bug Filing page, select Templates, and then select Bug Filing.
3. In the table, click the name of 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.
   - To the right of the template you want to modify, click the Edit field icon.
     The Edit template dialog box opens.
     (To access 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 available variables, click Show variables.)
5. Make any necessary changes to the content in the Mapped field and Template boxes.
6. Click Apply.
7. Click Save.

On the Bug Filing page, the details for the bug tracker plugin now include your changes.

See Also

"Velocity Templates for Bug Filing" on page 199
"Adding Velocity Templates to Bug Tracker Plugins" on page 200
"Deleting Velocity Templates" below

Deleting Velocity Templates

If a bug tracker plugin is not associated with any application versions, you can delete its velocity templates.

To delete the velocity templates group associated with a bug tracker plugin:

1. On the Hewlett Packard Enterprise header, select Administration.
2. In the left panel of the Bug Filing page, select Templates, and then select Bug Filing.
3. In the table, click the name of your bug tracker plugin.
   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 **Delete**.
   Fortify Software Security Center prompts you to confirm that you want to delete the template group.

   **Caution:** Fortify strongly recommends that you not delete the pre-defined template groups.

5. To continue with the deletion click **OK**.
   The Bug Filing page no longer lists the velocity templates for the bug tracker plugin.

**See Also**

"Velocity Templates for Bug Filing" on page 199

"Adding Velocity Templates to Bug Tracker Plugins" on page 200

"Editing Velocity Templates for Bug Tracker Plugins" on the previous page

**Submitting a Bug for One or More Issues**

If a bug tracking plugin has been specified for an application version O, you can submit bugs that cover one or multiple issues.

To submit a single bug that covers multiple issues:

1. From the Fortify Software Security Center Dashboard, click **Applications**.
2. In the **Version** column of the **Applications** table, click the application version of interest.
   Fortify Software Security Center displays the Overview page for the application version.
3. On the Overview page toolbar, click **Audit**.
   The Audit page opens.
4. To filter the issues listed:
   a. From the **Group by** list, select the attribute to use to group the issues in the issues table.
   b. From the **Filter by** list, select the attributes to use to filter the issues for display in the issues table.
      Note that you can select multiple attributes from this list.
   c. To refine the issues table further, click **Advanced**, and then select one or more additional filter categories from the **Advanced Issue Filters** list.
5. After you review the issues, select the check boxes for one or more issues tagged as exploitable and that you want to submit in a single bug.
6. Click **file issues**.

   **Note:** If, after you select one or more check boxes, **file issues** is not enabled, you first need to set up a bug tracker for the application version. (See.)

   The File Issues dialog box opens.
7. Provide your credentials for your bug tracking system, and then click **LOGIN**.

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

   After Fortify Software Security Center connects to the bug tracking server, the File Issues dialog box displays the required bug tracker plugin fields.

8. Provide the required information, and then click **Submit**.

**See Also**

"Viewing Bugs Submitted for Issues" on page 258

**Bug State Management**

Bug state management enables Fortify Software Security Center to make specific updates to bugs as the states of the issues within those bugs change. Fortify Software Security Center checks new security scans to determine whether filed bugs are to remain open, or can be closed.

If scan results indicate that one of more security issues associated with a previously submitted bug persist (and match the selection criteria), Fortify Software Security Center checks the bug tracking system to ensure that the bug is in a valid open state and, if necessary, reopens the bug.

If all issues associated with a bug are removed (either because the issues were remediated or no longer match the selection criteria), Fortify Software Security Center updates the bug to indicate that stakeholders may resolve or close this ticket. To enable auditing and traceability, Fortify Software Security Center does not automatically resolve or close bugs.

For instructions on how enable bug state management for an application version, see.
Changing the Template Associated with an Application Version

You can modify many settings for an existing application version, including its issue template. However, keep in mind that assigning a different issue template to an application version or updating an issue template on the server results in loss of synchronization between the database cache and existing audit sessions.

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

To change the template associated with an application version:

1. Log in to Fortify Software Security Center as either an Administrator or Security Lead.
2. Click the Applications tab.
3. From the list of application versions, select the version you want to modify.
4. On the application version toolbar, click Profile.
   - The Application Profile <application_version> dialog box opens.
5. Click Application Settings.

6. In the Version Settings section, click the edit icon 🖊.
The Edit Version wizard opens.

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

7. Advance to **Step 3. Choose Templates** (use **Next Step**).

   ![Template List](template_list.png)

    In the templates list, the currently assigned template is marked as selected (with a green check mark). A thumbs-up icon is displayed next to the template that Fortify recommends based on your application settings. 🌟

8. Select the check box for the template you prefer to use for the application version.
9. Click **Next Step**, and then click **Finish**.

After you change the template, Fortify Software Security Center invalidates any auditing session of the affected application version (for example, by a different user) and displays an error message to advise you that the application version audit session must be restarted.

**Note:** A Fortify Audit Workbench user auditing the affected application version does not see this information.

### Setting Analysis Result Processing Rules for Application Versions

Analysis results processing rules enable management approval and oversight of code scans. You can configure the rules to be followed when analysis results for an application version are processed during scan artifact uploads.

To configure the analysis results processing rules for an application version:

1. Log in to Fortify Software Security Center as an administrator, and then click the **Applications** tab.
2. Click the application version for which you want to configure the analysis results processing rules.
   
   The Overview page for the application version opens.
3. On the application version toolbar, click **Profile**.
   
   The Application Profile dialog box opens and displays the default processing rules for the application version.
4. Select the **Processing Rules** tab.
5. Review the listed processing rules.
6. Select or clear the check boxes for the rules described in the following table, and then click **Apply**.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require approval if the Build Project is different between scans</td>
<td>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.</td>
</tr>
<tr>
<td>Check external metadata file versions in scan against versions on server</td>
<td>Fortify Software Security Center checks the <em>externalmetadata.xml</em> files in the Fortify Static Code Analyzer and Fortify Software Security Center installations to determine whether they are the same. If they are identical, the data that an Audit WorkBench user sees on a Fortify Static Code Analyzer installation matches the data for the same output file results viewed in Fortify Software Security Center.</td>
</tr>
<tr>
<td>Require approval if file count differs by more than 10%</td>
<td>Fortify Software Security Center compares the file count for the scan and the scan that preceded it. If the count differs by more than ten percent, management approval is required before the scan can be uploaded.</td>
</tr>
<tr>
<td>Require approval if result has Fortify Java Annotations</td>
<td>Fortify Software Security Center checks the results to determine whether they include Fortify Java annotations. If Fortify Software Security Center finds any of the annotations, management approval is required before the scan can be uploaded.</td>
</tr>
<tr>
<td>Require approval if line count differs by more than 10%</td>
<td>Fortify Software Security Center compares the line count for the scan and the scan that preceded it. If the count differs by more than ten percent, management approval is required before the scan can be uploaded.</td>
</tr>
<tr>
<td>Automatically perform Instance ID migration on upload</td>
<td>A newer version of Fortify Static Code Analyzer or a Rulepack can change an instance ID from an instance ID created in a previous scan by an older version of Fortify Static Code Analyzer or a Rulepack. In reality, both instance</td>
</tr>
<tr>
<td>Rule</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>IDs identify the same issue. When enabled, this rule automatically migrates old instance IDs to the corresponding new instance IDs to preserve the history of the issues. It is sometimes useful to disable this rule as a troubleshooting measure for customer support.</td>
</tr>
<tr>
<td>Require approval if the engine version of a scan is newer than the engine version of the previous scan</td>
<td>Fortify Software Security Center checks to determine whether any scan engine (Fortify Static Code Analyzer, Fortify WebInspect, Fortify WebInspect Agent) version is newer than the one already used in the application. If it detects newer versions, it flags the upload for management approval.</td>
</tr>
<tr>
<td>Ignore Fortify SCA scans performed in Quick Scan mode</td>
<td>Blocks the processing of Fortify Static Code Analyzer scans done in Quick Scan Mode, which searches for high-confidence, high-severity issues.</td>
</tr>
<tr>
<td>Require approval if the Rulepacks used in the scan do not match the Rulepacks used in the previous scan</td>
<td>Fortify Software Security Center checks to determine whether you have added or removed a Rulepack, and whether a Rulepack version has changed. If it detects that a Rulepack has been added, removed, or updated, it flags the upload for management approval.</td>
</tr>
<tr>
<td>Require approval if Fortify SCA or Fortify WebInspect Agent scan does not have valid certification</td>
<td>Fortify Software Security Center checks to see that a Fortify Static Code Analyzer or WebInspect Agent scan has valid certification. If the certification is not valid, then someone may have tampered with the results in the upload. If the certification is missing, it is not possible to detect tampering. If certification is missing or is not valid, the rule requires management approval.</td>
</tr>
<tr>
<td>Require approval if result has analysis warnings</td>
<td>Fortify Software Security Center checks to see whether a Fortify Static Code Analyzer or Fortify WebInspect Agent scan contains analysis warnings. If it detects analysis warnings, the rule requires management approval.</td>
</tr>
</tbody>
</table>

**Note:** This rule applies only to the first upload of a given results file, and does not apply to subsequent uploads of the file. For example, if audit Information is...
<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>added to a previously-uploaded FPR file that contains analysis warnings, Fortify Software Security Center does not require management approval when the changed file is again uploaded.</td>
<td></td>
</tr>
<tr>
<td>Warn if audit information includes unknown custom tag</td>
<td>If audit information includes an unknown custom tag, the rule requires management approval.</td>
</tr>
<tr>
<td>Disallow upload of analysis results if there is one pending approval</td>
<td>If an analysis result still requires approval, this rule blocks its upload.</td>
</tr>
</tbody>
</table>

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

7. Click **OK**.

**See Also**

"Uploading Scan Artifacts" on page 229

**Custom Tags**

To audit code in Fortify Software Security Center, the security team examines analysis results (FPR) and assigns values to “tags” that are associated with application issues. The development team can then use these tag values to determine which issues to address and in what order.

Fortify Software Security Center provides a single default tag named “Analysis” to enable application auditing out of the box. Valid values for the Analysis tag are Exploitable, Not an Issue, Suspicious, Reliability Issue, and Bad Practice. You can modify the Analysis tag attributes, revise the tag values, or add new tag values based on your auditing needs.

To refine your auditing process, you can define your own custom tags. Like the Analysis tag, your custom tag definitions are stored in an issue template that you can associate with a Fortify Software Security Center application version. For example, you could create a custom tag used to track the sign-off process for an issue. After a developer audits his own issues, a security expert can review those same issues and mark each as “approved” or “not approved.”

**Note:** Fortify Audit Workbench users can add custom tags to their projects as they audit them. However, if these custom tags are not defined in Fortify Software Security Center for the issue template associated with the corresponding application version, then the new custom tags are lost after the Audit Workbench user uploads an FPR file to Fortify Software Security Center.
Topics covered in this section:

- Adding Custom Tags to the System ................................................................. 210
- Modifying Custom Tag Attributes ............................................................... 212
- Globally Hiding Custom Tags ........................................................................ 213
- Deleting Custom Tags ..................................................................................... 213
- Adding Custom Tag Values ............................................................................. 214
- Editing Custom Tags ....................................................................................... 214
- Deleting Custom Tag Values ........................................................................... 214
- Associating Custom Tags with Issue Templates .......................................... 215
- Viewing the Custom Tags Associated with an Issue Template ...................... 216
- Removing Custom Tags from Issue Templates ............................................. 216
- Assigning Custom Tags to Application Versions ....................................... 217
- Disassociating a Custom Tag from an Application Version ....................... 218
- Managing Custom Tags Through Issue Templates ...................................... 219
- Managing Custom Tags Through an Issue Template in an FPR File ............. 219

Adding Custom Tags to the System

If you are a Fortify Software Security Center administrator, you can add custom tags to the system. The following topics describe how to add each of the supported custom tag types to Fortify Software Security Center.

**Note:** You can filter issues based on the values for custom tags you create and assign to an application version. For information, see “Filtering Issues for Display on the Overview and Audit Pages” on page 249.

To add a custom tag:

1. On the Hewlett Packard Enterprise header, click **Administration**.
2. In the left panel of the Administration view, select **Templates**, and then select **Custom Tags**.
   The Custom Tags page opens.
3. In the Custom Tags page header, click **New**.
   The Create New Custom Tags dialog box opens.
4. In the **Name** box, type a name for the new tag.
   **Important:** Make sure that the name you specify for a custom tag is *not* a database reserved word.
5. (Optional) In the **Description** box, type content that describes how to use the custom tag.
6. From the **Type** list, select one of the following tag types:
   - **Date**—Accepts a calendar date in the format `yyyy-mm-dd`
   - **Decimal**—Accepts a number with a precision of up to 18 (up to 9 decimal places)
   - **List**—Accepts a selection from the list of values that you specify for the tag
   - **Text**—Accepts a string with up to 500 characters (HTML/XML tags and newlines are not allowed)

7. Select one or both of the following optional tag features:
   - To allow only users with specific permission (managers, security leads, administrators) to modify the tag, select the **Restricted** check box.
   - To prevent the display of the tag in the Assign dialog box or in Audit Workbench, select the **Hidden** check box.

8. If your new custom tag is a date-, decimal-, or text-type tag, click **Save**. If your new custom tag is a list-type tag, continue.
   
   A list-type custom tag can be **extensible**, which means that auditors can add values to it as they audit issues.

9. If you are adding a list-type tag, and you want to enable users to add new values to the tag during audits, select the **Extensible** check box.

10. To specify a value for the new tag:
    a. **Click + Add value.**
       The Add Value dialog box opens.
    b. In the **Name** box, type a value.
       A value can be a discrete attribute for the issue that this tag addresses. For example, you might specify that this custom tag addresses a due date or server quality issue.
    c. (Optional) In the **Description** box, type a description of what the value represents.
    d. To prevent the tag from being displayed in the Assign dialog box or in Audit Workbench, select the **Hidden** check box.
    e. **Click Apply.**
    f. Repeat the previous step until you have defined all of the values you need for the new custom tag.

    If the custom tag has a default value, then issues with no value set for the tag acquire that default value. If no default value is defined, then the tag value becomes “Not Set.”

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

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

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

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

13. Click **Save**.

**Note:** To use a new custom tag to audit application version issues, you must first assign the tag to the application version. For instructions, see *Assigning Custom Tags to Application Versions* on page 217.

See Also

- "Custom Tags" on page 209
- "Editing Custom Tags" on page 214
- "Globally Hiding Custom Tags" on the next page
- "Associating Custom Tags with Issue Templates" on page 215
- "Managing Custom Tags Through Issue Templates" on page 219
- "Managing Custom Tags Through an Issue Template in an FPR File" on page 219
- "Deleting Custom Tags" on the next page

Modifying Custom Tag Attributes

To modify the attributes of a custom tag:

1. From the left panel in the **Administration** page, click **Templates**, and then click **Custom Tags**.
2. On the **Custom Tags** page, click the row that displays the tag you want to modify.
   
   The row expands to reveal the details.
3. Click **Edit**.
4. Modify the tag attributes and save your changes.

**Important:** Make sure that the name you specify for a custom tag is not a database reserved word.
Globally Hiding Custom Tags

To globally hide a custom tag:

1. From the left panel in the Administration view, click Templates, and then select Custom Tags.
   The Custom Tags page opens and lists all existing custom tags.
2. Click the row for the tag you want to hide.
   The row expands to display the details for the tag.
3. Click Edit.
4. Under the Description box, select Hidden.
5. Click Save.
The custom tag no longer appears on the Audit page or in Audit Workbench.

Deleting Custom Tags

If you are an Administrator or a Security Lead, you can delete custom tags.

**Note:** You cannot delete a custom tag if:
- The tag is currently set as the primary tag.
- The tag is currently associated with an application version or issue template.
- If an issue has been audited using the custom tag.
You can never delete the Analysis tag.

To delete custom tags:

1. From the left panel in the Administration page, click Templates, and then click Custom Tags.
   The Custom Tags page opens. Existing custom tags are listed on the right.
2. Select the check boxes for the custom tags you want to delete.
3. In the Custom Tags toolbar, click Delete.
4. When prompted to confirm that you want to delete the tag (or tags), click OK.

Adding Custom Tag Values

If you are a Fortify Software Security Center administrator, you can add values to the list-type custom tags in the system.

**Note:** If a custom tag is assigned the Extensible attribute, then you can add values to it as you audit issues.
To add a value to a list-type custom tag:

1. From the left panel in the Administration page, click Templates, and then click Custom Tags.
   
The Custom Tags page opens. Existing custom tags are listed on the right.
2. Click the row for the tag to which you want to add a value.
   
The row expands to display the details for the tag.
3. Below the table of values, click Edit.
4. Above the table of values, click + Add value.
5. In the Add Value dialog box, type a name and, optionally, a description for the new value.
6. To make the value unavailable in the Audit page and in Fortify Audit Workbench, select the Hidden check box.
7. Click Apply.
8. On the Custom Tags page, click Save.

See Also

*Adding Custom Tags to the System* on page 210

*Assigning Custom Tags to Application Versions* on page 217

*Editing Custom Tags* below

*Deleting Custom Tag Values* below

Editing Custom Tags

If you are an Administrator-level user, you can modify custom tags in the system.

To edit a custom tag:

1. From the left panel in the Administration view, click Templates, and then select Custom Tags.
   
The Custom Tags page opens and lists all custom tags in the system.
2. Click the row for the tag you want to edit to expand it and display the details.
3. Below the table of values, click Edit.
4. Edit the values for any of the displayed fields, and then click Save.
   
   For information about the displayed fields, see *Adding Custom Tags to the System* on page 210.

See Also

*Deleting Custom Tag Values* below

*Assigning Custom Tags to Application Versions* on page 217

Deleting Custom Tag Values

If you are an administrator or a security lead, you can delete custom tag values.
To delete a value for a custom tag:

**Note:** You cannot delete a custom tag value that is currently associated with an application version, issue template, or if an issue is audited using the value.

1. From the left panel in the Administration view, click Templates, and then click Custom Tags.
   The Custom Tags page opens and lists all custom tags in the system.
2. Click the row for the tag from which you want to delete a value.
   The row expands to display the details for the tag.
3. Below the table of values, click Edit.
4. In the table of values, click the Remove value icon in the row for the value you want to delete.
5. Click Save.

**See Also**

"Adding Custom Tags to the System" on page 210
"Adding Custom Tag Values" on page 213
"Editing Custom Tags" on the previous page

**Associating Custom Tags with Issue Templates**

After you first create an issue template and upload an issue template file, the custom tags defined in that issue template file are the custom tags that are initially associated with the issue template. Updates to existing custom tags are ignored because tags are designed to be updated using the procedures described in previous sections, but newly-defined custom tags in that issue template file are added to the system and associated with the issue template.

**Note:** The custom tags associated with an issue template are the default tag set assigned to an application version when it is first created using that issue template.

To associate a custom tag with an issue template:

1. From the left panel in the Administration page, click Templates, and then select Issue.
   The table on the right lists all of the issue templates in the system.
2. Click the row that displays the issue template to associate with the custom tag.
   The row expands to reveal the issue template detail.
3. Click Edit.
   The editable fields of the details section become writable and the + Add Custom Tag button is now visible.
4. Click + Add Custom Tag.
   The Add Custom Tag dialog box opens.
5. Select the check box for the custom tag to associate with the issue template, and then click
Add

6. Click **Save**.

**See Also**

"Disassociating a Custom Tag from an Application Version" on page 218

**Viewing the Custom Tags Associated with an Issue Template**

To see which custom tags are associated with an issue template:

1. On the Hewlett Packard Enterprise header, click **Administration**.
2. In the left panel of the Administration view, click **Templates**, and then select **Issue**.
   The Issue page lists all issue templates.
3. Click the row for the project template of interest.
   The row expands to reveal
4. Click **View Details**.
5. Click the **Custom Tags** tab.

You can also edit or delete a custom tag from this project template from the **Custom Tags** tab.

**Removing Custom Tags from Issue Templates**

To remove a custom tag from an issue template:

1. From the left panel in the **Administration** page, click **Templates**, and then select **Issue**.
   The table on the right lists all of the issue templates in the system.
2. Click the row that displays the issue template associated with the custom tag you want to remove.
   The row expands to reveal the issue template details. The **Custom Tags** section lists the custom tags associated with the template.
3. Scroll to the bottom of the expanded row and click **Edit**.

4. In the last column, click the remove icon 🗑️ for the custom tag that you want to remove from the template.

5. Click **Save**.

**See Also**

"Custom Tags" on page 209

### Assigning Custom Tags to Application Versions

To use a new custom tag to audit application version issues, you must first assign the tag to the application version.

To assign a custom tag to an application version:

1. From the Applications view, select the version name for the application version you plan to audit.
   
   Fortify Software Security Center opens the Audit page for the selected version.

2. In the application version toolbar, click **Profile**.

3. In the Application Profile dialog box, click **Custom Tags**.

4. Click **Assign / Remove**.
   
   The Assign Custom Tags dialog box opens and lists the tags available for auditing issues.

5. Select the check box for the custom tag you want to assign to the application version, and then click **Done**.
To successfully complete the audit of an issue in Fortify Software Security Center, you must specify a value for the custom tag that is designated as the *primary tag*. By default, the Analysis tag is the primary tag.

During an audit, the primary tag is listed first. If custom tags other than Analysis exist in your Fortify Software Security Center instance and are assigned to the application version, you can select one of these (instead of Analysis) as the primary tag.

6. (Optional) To assign a tag other than the current primary tag as primary:

   **Note:** You can only assign list-type custom tags as primary tags.

   a. Click **Select Primary**.

      The Select Primary Tag dialog box opens.

   b. From the **Select Primary Tag** list, select the tag to set as the primary custom tag.

      **Note:** If you use Audit Assistant, and you have not provided Audit Assistant guidance information, make sure that you edit the tag to include that information. For information about how to provide Audit Assistant guidance, see "Adding Custom Tags to the System" on page 210. For information about how to edit a custom tag, see "Editing Custom Tags" on page 214.

   c. Click **Done**.

7. Close the Application Profile dialog box.

   The assigned custom tag will be available the next time a team member audits issues for the application version.

**See Also**

"Adding Custom Tags to the System" on page 210

"Adding Custom Tag Values" on page 213

"Auditing Issues" on page 244

"Editing Custom Tags" on page 214

**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 Hewlett Packard Enterprise header, click **Applications**.

2. Click the application version name to which the custom tag is assigned.

   The Overview page opens.

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

   The Application Profile window opens.

4. Select **Custom Tags**.
5. Click **Assign/Remove**.
   The Assign Custom Tags dialog box opens.

6. Clear the check box for the custom tag that you want to remove, and then click **Done**.

**See Also**

"Adding Custom Tags to the System" on page 210

"Assigning Custom Tags to Application Versions" on page 217

**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 Hewlett Packard Enterprise header, select **Administration**.
2. In the left panel of the Administration page, select **Templates**, and then select **Custom Tags**.
3. Complete the update.

You can add a new custom tag through an issue template upload. This could, for example, allow a member of a security team who is not part of a software audit to define the issue template and the custom tags in the issue template.

**Managing Custom Tags Through an Issue Template in an FPR File**

FPR files typically contain an issue template. If an FPR file uploaded to Fortify Software Security Center contains an issue template with a custom tag that has been set as editable, you can add a value to the tag.
Chapter 13: Variables, Performance Indicators, and Alerts

Fortify Software Security Center lets you store measured values and event conditions for application versions as variables. A Fortify Software Security Center variable is a definition of a metric that is to be evaluated periodically for each application version. Variables count issues, conditions, and other categories of numeric data.

Performance indicators combine variables into metrics that are normalized across application version boundaries, and that can represent complex higher-level abstractions such as monetary costs. Fortify Software Security Center variables and performance indicators provide the building blocks that you can use to create customized metrics, which you can then incorporate into customized alert definitions. You can use the values of variables to trigger alerts, which Fortify Software Security Center then displays on the dashboards of users specified as recipients in alert definitions. Fortify Software Security Center can also email alert notifications to members of an application version team.

This section contains the following topics:

Working with Variables ................................................................. 220
Performance Indicators ................................................................. 222
Alert Definitions ............................................................................ 223
Viewing and Marking Alerts ............................................................ 227

Working with Variables

If you are a Security Lead or an Administrator, you can define variables for your applications. The following topics provide information about Fortify Software Security Center variable syntax and search strings, and include instructions on how to create variables.

Creating Variables

To create a Fortify Software Security Center variable:

1. Log in as a Security Lead or an Administrator, and then click Administration.

   **Note:** Users who have Developer accounts cannot create Fortify Software Security Center variables.

2. In the Administration panel on the left, under Metrics & Tracking, select Variables.
3. In the Variables toolbar, click New.

   The Create New Variable dialog box opens.
4. Provide the information described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a variable name that begins with a letter (a-z, A-Z), and that contains only letters, numerals (0-9), and the underscore character (_).</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Type a description so that other users can understand how to use the variable.</td>
</tr>
<tr>
<td>Search String</td>
<td>Type a valid Fortify Software Security Center variable search string. (For information about how to construct search strings, see “Variable Syntax” below.)</td>
</tr>
<tr>
<td>Folder</td>
<td>From this list, select a folder from the default filter set to associate with the variable. The Folder list displays the unique folder names associated with all available issue templates. The variable value is calculated if the folder name is associated with the issue template for the application version.</td>
</tr>
</tbody>
</table>

5. Click **Validate**.

Fortify Software Security Center displays the variable validation result.

6. After Fortify Software Security Center validates the variable, click **Save**.

The Variables table now lists your new variable.

### Variable Syntax

The Fortify Software Security Center variable format is `modifier:searchstring`.

**Example:** `[Fortify Priority Order]:critical audited:false`

To search for an exact match of the string, enclose the string in quotation marks (" "). To search for a string without qualifications, type the string without quotation marks.

The following table lists the Fortify Software Security Center relational operators.

<table>
<thead>
<tr>
<th>Relational Operator</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number range</td>
<td>A comma-separated pair of numbers used to specify the beginning and end of a range of numbers. Use a left or right bracket (&quot;[&quot;]&quot;) to specify that the range includes the adjoining number.</td>
<td>(2, 4] Indicates a range of greater than two, and less than or equal to four</td>
</tr>
</tbody>
</table>
### Relational Operator

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a begin or end parenthesis (&quot;(&quot;) to specify that the range excludes (is greater than or less than) the adjoining number.</td>
<td>! (not equal) Negate a modifier with an exclamation character (!).</td>
<td>!file:Main.java Returns all issues that are not in Main.java.</td>
</tr>
</tbody>
</table>

### Performance Indicators

Fortify Software Security Center performance indicators enable you to combine variables into metrics that are normalized across application version boundaries, and that can represent complex, high-level abstractions such as monetary costs. This section provides information about performance indicator syntax and instructions on how to create performance indicators.

The general format for a Fortify Software Security Center performance indicator formula is as follows:

```
Variable[operator]Variable
```

where `operator` is a standard mathematical operator (+, -, *, /).

For instructions on how to create performance indicators, see "Creating Performance Indicators" below.

**See Also**

"Key Performance Indicators Report" on page 288

### Creating Performance Indicators

To create a Fortify Software Security Center performance indicator:

1. Log in to Fortify Software Security Center as a Security Lead, and then click the **Administration** tab.

   **Note:** Users who have Manager and Developer accounts cannot create Fortify Software Security Center performance indicators.

2. In the panel on the left, select **Metrics & Tracking**, and then select **Performance Indicators**.

   The table to the right lists existing **Performance Indicators**.

3. Click **New**.

   The Create New Performance Indicator dialog box opens.
4. Provide the information described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a performance indicator name.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a description of this performance indicator.</td>
</tr>
<tr>
<td>Equation</td>
<td>Type a valid Fortify Software Security Center performance indicator equation.</td>
</tr>
<tr>
<td></td>
<td>The format for a performance indicator formula is as follows:</td>
</tr>
<tr>
<td></td>
<td>Variable[operator]Variable where operator is a standard mathematical operator (+, -, *, /).</td>
</tr>
<tr>
<td>Return Type</td>
<td>From this list, select the value type to return.</td>
</tr>
</tbody>
</table>

5. After you configure and successfully validate the new performance indicator, click **Save**. The **Performance Indicators** table lists your new indicator.

### Alert Definitions

Alert definitions can include variables or performance indicators to determine when Fortify Software Security Center is to generate an alert notification in the **Todo List** on the Dashboard.

**Note:** This functionality is available only if a Fortify Software Security Center administrator has enabled email notifications from the legacy user interface. For information about how to access the legacy user interface, see "Switching Between the New User Interface and the Legacy User Interface" on page 24. For instructions on how to enable email notifications from the legacy UI, see the **HP Fortify Software Security Center Installation and Configuration Guide** for version 4.30.

You can configure alert notifications to send email messages about one or more alert notifications to members of a given application version.

**Next**

"Creating Alerts" below

**See Also**

"Configuring Email Alert Notification Settings" on page 91

"Deleting Alerts" on page 226

**Creating Alerts**

You can define alerts for any application versions to which you have been granted access.
To create a Fortify Software Security Center alert:

1. On the Hewlett Packard Enterprise header, click Administration.
2. In the panel on the left, click Templates, and then select Alerts.
   The Alerts page displays any alerts defined to date.
3. In the Alerts toolbar, click New.
   The Create New Alert dialog box opens.
4. In the Name box, type a name for the alert.
5. (Optional) In the Description box, type text that describes what the alert is for.
6. Next to Type, select the type of alert you want to create.

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

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

### Performance indicator

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>From the Alert when list, select a performance indicator.</td>
</tr>
<tr>
<td>b.</td>
<td>From the list of operators, select an operator.</td>
</tr>
<tr>
<td>c.</td>
<td>Type a numeric value. The type of performance indicator selected determines whether the value represents an integer or a percentage.</td>
</tr>
<tr>
<td></td>
<td>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 &lt; 50 is triggered only once, even if many new critical issues are uncovered in subsequent scans.</td>
</tr>
<tr>
<td>d.</td>
<td>To have Fortify Software Security Center reset your alert after each new artifact upload, select the Reset after triggering check box.</td>
</tr>
</tbody>
</table>

### Variable

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>From the Alert when list, select a variable.</td>
</tr>
<tr>
<td>b.</td>
<td>From the list of operators, select the appropriate operator.</td>
</tr>
<tr>
<td>c.</td>
<td>Type a numeric value. The type of variable you selected determines whether the value represents an integer or a percentage.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>d.</td>
<td>To have Fortify Software Security Center reset your alert after each new artifact upload, select the Reset after triggering check box.</td>
</tr>
</tbody>
</table>
upload, select the **Reset after triggering** check box.

### System event

- From the **Alert when** list, select the Fortify Software Security Center system event to trigger the alert.

### Scheduled alert (Administrators only)

Under **Alert when**, do the following:

a. Use the calendar control to specify the date on which Fortify Software Security Center is to send the alert.
b. In the two boxes to the right, type the hour and minute (hh:mm) at which to send the alert.
c. Toggle between AM and PM to determine whether the alert is sent in the morning or afternoon.
d. From the list of countries and regions, select the country or region to which your time and date settings apply.
e. From the time zone list, select the time zone to which your time and date settings apply.

8. If you are creating a performance indicator alert or variable alert, do one of the following:

- To use this alert for all application versions to which you have been granted access, select the **Monitor All Applications** check box.

Otherwise, to use this alert for specific application versions:

a. Click **Add**.

   The Select Application Version dialog box opens.
b. In the **Application** list, select an application for which you want to use the alert.
c. To include inactive versions of the application in the **Versions** list, select the **Show inactive versions** check box.
d. To use the alert for all application versions, select the check box next to **Versions**. Otherwise, in the **Versions** list, select the check boxes for the versions for which you want to use the alert.
e. Click **Done**.

9. In the **Recipients** section, select one of the following recipient preferences:

   Regardless of the option you select, you will receive the notification.
To have the notification sent only to you, select **Me Only**.

To have the notification sent to all Fortify Software Security Center users who have access to the application versions you specified (in the Select Application Version dialog box), select **Version assignees**.

If you are creating a scheduled alert, to have the notification sent to all Fortify Software Security Center users, select **All system users**.

10. To create the alert without enabling it, clear the **Enabled Alert** check box. To enable this alert, leave the check box selected.

11. In the **Message** box, type a message to tell recipients why they have received the alert.

   **Note**: If you are creating a scheduled alert, **message text is required**.

12. Click **Save**.

   If you selected **Version assignees** as recipients, Fortify Software Security Center displays the following alert:

   "Are you sure you want to notify all application versions users? This could potentially notify a large amount of users every time the alert triggers."

13. To proceed, click **OK**. Otherwise, click **Cancel**, and then select **Me Only** as a recipient.

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

**Editing Alerts**

To edit a Fortify Software Security Center alert:

1. Log in to Fortify Software Security Center as an Administrator, and then click the **Administration** tab.

2. In the panel on the left, click **Templates**, and then select **Alerts**.

   The Alerts page displays all alerts you have defined.

3. In the **Alerts** table, locate and select the row for the alert you want to edit.

   The row expands to reveal the alert settings.

4. Click **Edit**.

5. Make the necessary changes and then click **Save**.

**Deleting Alerts**

To delete a Fortify Software Security Center alert:

1. Log in to Fortify Software Security Center as an Administrator, and then click the **Administration** tab.

2. In the panel on the left, click **Templates**, and then select **Alerts**.

   The Alerts page displays all alerts you have defined.

3. In the **Alerts** table, select the check box to the left of the alert you want to delete.
4. In the **Alerts** toolbar, click **Delete**.
   Fortify Software Security Center prompts you to confirm that you want to proceed with the deletion.
5. Click **OK**.

**See Also**

*Alert Definitions* on page 223

*Creating Alerts* on page 223

**Viewing and Marking Alerts**

Fortify Software Security Center flags any unread alerts that either you or another user has set up for you to receive. These flags are visible in the collapsible panel on the right of the Dashboard, and on the right end of the Hewlett Packard Enterprise header in every view.

**To view your unread alerts, do one of the following:**

- At the right end of the Hewlett Packard Enterprise header, click the red circle that shows the number of unread alerts for you.
- On the Dashboard, in the **Todo List** section of the collapsible panel, click the red circle that shows the number of unread alerts for you.

The Alerts window opens and lists your unread alerts.

**To mark an alert as having been read:**

- In the Alerts window, select the check box to the left of the alert name, and then click **Mark as Read**.

**To view alerts that you have already read:**

- From the **View** list, select **Read**.

**To mark an alert you have read as unread:**

- Select the check box to the left of the alert name, and then click **Mark as Unread**.

**To view all of your alerts (read and unread):**

- From the **View** list, select **All**.
If you have marked all of your alerts as read, the read alert flag is no longer displayed. To see these alerts, go to the Dashboard and, in the **Todo List** section of the collapsible panel, click **Show all alert notifications**.

![Todo List](image)
Chapter 14: About Working with Scan Artifacts

This section contains the following topics:

- Uploading Scan Artifacts ................................................................. 229
- Uploading SAP NetWeaver Data to an Application Version .................. 231
- Viewing Scan Errors ................................................................. 233
- Downloading Scan Artifacts ....................................................... 234
- Approving Scan Artifacts .......................................................... 235
- Viewing High-Level Summary Results ......................................... 235
- Displaying Additional Application Versions on the Dashboard ............... 238
- Viewing Issue Metadata .......................................................... 239
- Mapping Scan Results to External Lists ........................................ 239
- Purging Scan Artifacts .............................................................. 240
- Deleting Artifacts ................................................................. 241

Uploading Scan Artifacts

The following procedure describes how to upload your scan artifacts to the Fortify Software Security Center database. For information about how to submit training metadata to Fortify Audit Assistant, see "Submitting Training Data to Audit Assistant" on page 266.

**Important:** The files you upload to Fortify Software Security Center must be no larger than 2GB.

**Note:** If a scan artifact requires approval based on analysis result processing rules, it must be approved before it can be processed. For information, see "Approving Scan Artifacts" on page 235.

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

1. On the Hewlett Packard Enterprise header, click **Applications**.
2. On the **Applications** page, click the link for the application version associated with the artifact you want to upload.
3. On the application version toolbar, click **Artifacts**.
   - The **Artifacts History** table lists all scan artifacts uploaded for the application.
4. Click **Upload Artifact**.
   - The Upload Artifact dialog box opens.
5. Click **Add Files**.
6. Navigate to and select one or more artifact files to upload.

The Upload Artifact dialog box lists the selected files.

7. To remove a file from the list, click the trash icon for that file.

8. To remove all of the listed files, click Clear.

9. After you select all of the files that you want to upload, click **Start upload**. The dialog box displays a green progress bar as each file is uploaded.

10. After your files are successfully uploaded, click **Close**.
Viewing File Processing Errors

If there was an error in processing an uploaded artifact, the **Status** column of the **Scan History** table displays **Error Processing**, along with a circled number that indicates the number of processing rules violated.

<table>
<thead>
<tr>
<th>Scan History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Upload Date</strong></td>
</tr>
<tr>
<td>10/07/2015 3:28:24 PM</td>
</tr>
</tbody>
</table>

To view information about the processing rules violated:

- Click the circled number.

The **Artifact Processing Messages** box opens to display details about problems encountered during the upload.

**See Also**

- "Using an Application Identifier to Upload FPR Files" on page 304
- "Using an Application Name and Version to Upload FPR Files" on page 305
- "Downloading Scan Artifacts" on page 234
- "Deleting Artifacts" on page 241
- "Setting Analysis Result Processing Rules for Application Versions" on page 206
- "About Auditing" on page 242

Uploading SAP NetWeaver Data to an Application Version

If your organization uses SAP NetWeaver Code Vulnerability Analyzer (CVA) to search for vulnerabilities in ABAP source code, you can use the NetWeaver plugin to map your CVA scans to a Fortify Software Security Center application version, and then import the results for investigation from Fortify Software Security Center.

If your Fortify Software Security Center administrator has configured a connection with NetWeaver, you can download NetWeaver results to a Fortify Software Security Center application version.

To download NetWeaver CVA results to a Fortify Software Security Center application version:

1. To determine the display ID for the NetWeaver CVA run that produced the results you want to download:
a. From SAP NetWeaver, open the ABAP Test Cockpit (ATC).

b. Under **Personal Results**, right-click the result, and then select **Header Information** from the shortcut menu.

The Result Header Information dialog box lists the display ID under **Technical Details**.

2. Create a file with the NWV extension, open your `<file_name>.nwv` file in a text editor, and then add the following line:

   `resultDisplayId=<display_ID>`

   where `<display_ID>` is the display ID you found in step 1.

3. From the Dashboard, open the Overview page for the application version for which you want to upload the NetWeaver data.
4. On the Overview toolbar, click **Artifacts**.
5. On the Artifact History page, click **Upload Artifact**.
   The Upload Artifact dialog box opens.

![Upload Artifact dialog box](image)

6. Click **+ Add Files**.
7. Browse to and select your `<file_name>.nwv` file.

![Upload Artifact dialog box with file selected](image)

8. In the Upload Artifact dialog box, click **Start Upload**.
   After a successful upload, Fortify Software Security Center displays the individual CVA findings, and identifies their source code file names and line numbers, assigns each a Fortify Priority Order, and displays them in the Fortify Software Security Center user interface for auditing.

**Viewing Scan Errors**

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

To view scan errors:

1. On the Hewlett Packard Enterprise header, click **Applications**.
2. On the **Applications** page, click the link for the application version you are interested in.
3. On the application version toolbar, click **Artifacts**.

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

4. To open the Scan Errors window and view detailed information about the errors that occurred, click the number in the red circle.

   **See Also**

   "Purging Scan Artifacts" on page 240

**Downloading Scan Artifacts**

From the Artifact History page, you can download the latest merged FPR file for an application version or you can download FPR files that result from individual scans.

**Downloading the Merged FPR File for an Application Version**

To download the latest merged scan results for an application version in FPR format:

1. On the Hewlett Packard Enterprise header, click **Applications**.
2. On the **Applications** page, click the link for the application version you are interested in.
3. On the application version toolbar, click **Artifacts**.

   The **Artifact History** table lists all scan artifacts uploaded for the application.

4. Click **Download Application File**.
5. In the Opening `<file_name>` dialog box, do one of the following:
   - Note the file name, leave **Save** selected, and then click **OK**.
   - Select **Open with**, browse to the program with which to open the file, and then click **OK**.
     (If you do not select a program, Fortify Software Security Center tries to open the file in Fortify Audit Workbench, which is the default program).
Downloading Individual Scan Results

2. On the Applications page, click the link for the application version you are interested in.
3. On the application version toolbar, click Artifacts.
   - The Artifact History table lists all artifacts uploaded for the application.
4. Click the row that displays the artifact you want to download.
   - The row expands to reveal detailed information about the scan.
5. Click Download.
6. Save the file, and then open the saved file from Fortify Audit Workbench or other application.

See Also

*Uploading Scan Artifacts* on page 229
*Deleting Artifacts* on page 241
*Viewing Scan Errors* on page 233

Approving Scan Artifacts

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

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

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

See Also

*Setting Analysis Result Processing Rules for Application Versions* on page 206

Viewing High-Level Summary Results

Fortify Software Security Center offers several ways to view high-level summary results for application versions from the Fortify Software Security Center Dashboard or from the Overview page.
Viewing Summary Metrics on the Issue Stats Page

To view summary metrics for application versions (individually and collectively) from the Issue Stats page:

- On the Hewlett Packard Enterprise header, select Dashboard. The following three portlets on the Issue Stats page (the default Dashboard view in Fortify Software Security Center) display consolidated metrics for all of the applications to which you have access:
  - The Issues Remediated portlet shows the total number of issues remediated to date, the average number of days it took to review them, and the average number of days required to remediate them.
  - The Issues Pending Review portlet shows the total number of open issues, and the number of these that have been reviewed.
  - The Application Versions portlet shows the total number of application versions to which you have access the number of files scanned and the number of lines of code scanned for those application versions.

The table on the Issue Stats page displays summary metrics for each of the application versions to which you have access. If you click an application version listed in the table, Fortify Software Security Center takes you directly to the Audit page for that application version.

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

Viewing Summary Metrics on the Chart Page

You can view a graphical representation of summary metrics for individual application versions from the Charts page.

To view summary metrics for application versions from the Charts page:

2. In the list of application versions, move your cursor to a colored bar for an application
Fortify Software Security Center shows the summary findings for the version. In the example shown here, the pie chart of the left shows the security ratings for the 32% of findings (54 of 171) that have been audited to date for this application version. The chart on the right shows the percentage of findings audited (32) and the percentage of the total that has yet to be audited (68).

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

**Viewing Summary Metrics on the Overview Page**

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

1. On the Hewlett Packard Enterprise header, click **Applications**.
2. On the **Applications** page, click the link for the version you are interested in.
3. On the **Overview** page, if the panel on the right is collapsed, expand it.
The **Version Progress** section displays summary information with trending arrows.

4. To display a metric other than Fortify Security Rating, click the edit icon 🏗, and then select a different metric to display from the list.

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

**See Also**

"Auditing Issues" on page 244

### Displaying Additional Application Versions on the Dashboard

To display up to five more application versions on the Application Dashboard:

**See Also**
Viewing Issue Metadata

To view metadata for an issue:

1. Navigate to the Audit page for the application version of interest.
2. In the issues table, if you have selected a grouping, expand a group to view issues it contains.
3. Click the row that displays the issue name.
   
   The Code tab displays an overview of the issue, the Analysis value (if set), the stack trace, and the section of code in which the issue was uncovered.
4. At the bottom of the issue details section, click Metadata.

   The Metadata box displays the unique issue identifier (Instance ID), the unique identifier for the rule that generated the issue (Primary Rule ID), priority metadata values, and legacy priority metadata values.

5. To go to the website that provides detailed information about software security errors, select the HPE Security Fortify Taxonomy: Software Security errors link.

Mapping Scan Results to External Lists

Fortify distributes an external metadata document with Rulepacks. This document includes mappings from the Fortify categories to alternative categories (such as OWASP 2010, PCI DSS 3.2, or CWE). Security leads can customize this mapping or create their own files to map issues to different taxonomies, such as internal application security standards or additional compliance obligations.
**Note:** For detailed information about external metadata, see the *HPE Security Fortify Static Code Analyzer Custom Rules Guide.*

You can either modify the existing external metadata document (externalmetadata.xml), or create your own document (recommended). The existing mapping file is located in the `<sca_install_dir>\Core\config\ExternalMetadata` directory of Fortify Static Code Analyzer.

Use any XML editor to make your changes or create a new document. Fortify recommends that you save your new or modified document to the `<sca_install_dir>\Core\config\CustomExternalMetadata` directory with a new name so that your changes are not lost during security content updates.

To validate your modified or new mapping, use the `externalmetadata.xsd` file, which is located in the `<sca_install_dir>\Core\config\schemas` directory.

To apply the modified or new external metadata document across all applications, you must first import it into Fortify Software Security Center.

To import a new or modified external metadata document into Fortify Software Security Center:

1. Log in as Administrator, and then click the **Administration** tab.
2. In the **Administration** panel, under **Metrics & Tracking**, click **Rulepacks**.
3. In the **Rulepacks** panel on the right, click **Import**.
   - The Import Rulepack dialog box opens.
4. Click **+Add Files**.
5. Navigate to and select your document, and then click **Start Upload**.

If you are conducting a collaborative audit between Fortify Software Security Center and Audit Workbench, you can import the changed mapping document to Fortify Software Security Center, and then open the FPR file in Audit Workbench to see how the mapping works with the scan results.

**Purging Scan Artifacts**

Purging an artifact recovers space from the Fortify Software Security Center database by removing the uploaded artifact, the temporary results of artifact processing, and the cross-reference information for source files.

Before you purge artifacts for an application version, consider the following:

- After the purge, neither the purged artifacts, nor the earliest artifact not purged, can be deleted.
- Purging does not affect any issue-base metrics in the system.
- If you have custom reports, consult HPE Security Technical Support first to determine whether an artifact purge will affect them.

To purge a scan artifact from the Fortify Software Security Center database:
1. From the <application_version> Overview page, click Artifacts.
   The Artifact History table lists all scan artifacts uploaded for the application version.
2. Click the row that displays the artifact you want to purge from the database.
   The table expands to show the details for the selected artifact.
3. Below the artifact details, click Purge.
   Fortify Software Security Center prompts you to confirm that you intend to purge the artifact.
4. Click OK.

Deleting Artifacts

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

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

2. On the Applications page, click the link for the version you are interested in.
3. On the application version toolbar, click Artifacts.
   The Artifact History table lists all artifacts uploaded for the application.
4. Click the row that displays the scan artifact you want to delete.
   The table expands to show the details for the selected artifact.
5. Below the artifact details, click Delete.
   Fortify Software Security Center prompts you to confirm that you want to delete the artifact.
6. Click OK.
Chapter 15: Collaborative Auditing

Fortify Software Security Center provides a web-based collaborative environment for auditing issues associated with Fortify Software Security Center applications. The following sections provide an overview of the auditing process and instructions on how to display and use the auditing interface.

The information in these topics is presented based on the assumption that you know how to create and configure Fortify Software Security Center application versions. (For information about Fortify Software Security Center applications and application versions, see “Applications and Application Versions” on page 180.

This section contains the following topics:

- About Auditing ................................................................. 242
- Auditing Issues ............................................................... 244
- About Audit Assistant .................................................... 258
- Setting Issue Viewing Preferences .................................. 269
- Searching Globally in Fortify Software Security Center ............ 270
- Fortify Software Security Center and WebInspect Enterprise Integration .................. 272

About Auditing

When Fortify Static Code Analyzer scans source code, all of its discoveries are presented as potential vulnerabilities, not actual vulnerabilities. Because every application is unique and all functionality runs within a particular context understood best by the development team, no technology can fully determine if a suspect behavior should be considered a vulnerability without direct developer confirmation.

Issue audits, whether performed in Fortify Software Security Center or Fortify Audit Workbench, or by Audit Assistant, accomplish the following:

- Condense and focus application information
- Enable the security team to collaboratively decide which issues represent real vulnerabilities
- Enable the security team to collaboratively prioritize issues based on vulnerability

Fortify Software Security Center uses issue templates to categorize and display issues.

About Current Issues State

Fortify Software Security Center keeps track of which analysis engine (analyzer) uncovers each issue in an application version and merges any new information into the existing body of results for the application version. After new audit information is uploaded to the server or entered on the Audit page, Fortify Software Security Center merges that information into any existing audit
information for a given issue. Fortify Software Security Center also marks an issue as removed after the analysis engine no longer finds the issue.

Whenever new scan results are uploaded, Fortify Software Security Center checks every issue to determine whether it was uncovered in a previous scan.

**Setting the Strategy for Resolving Issue Audit Conflicts**

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

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

**Example of the default strategy for resolving audit conflicts:**

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

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

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

On a different 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. Log in to Fortify Software Security Center as an administrator.
2. On the Hewlett Packard Enterprise header, select **Administration**.
3. In the left panel, select **Configuration**, and then select **Issue Audit**.
The Issue Audit page opens.

4. From the **Issue Audit** list, select one of the following:
   - Conflicts are resolved in favor of the SSC changes
   - Conflicts are resolved in favor of the most recent changes

5. Click **Save**.

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

**See Also**

"About Current Issues State" on page 242

**Auditing Issues**

To display the issues you want to audit:

1. Upload scan results for the application version you want to audit. For instructions, see "Uploading Scan Artifacts" on page 229.

2. Open the **Audit** page for the application version of interest. (For instructions, see "Accessing the Audit Page from the Issue Stats Page of the Dashboard" on page 249 or "Accessing the Audit Page from the Applications View" on page 249.)

3. To selectively display the issues you want to audit, apply filters to the issues list. (See "Filtering Issues for Display on the Overview and Audit Pages" on page 249.)

4. In the issues table, if you have selected a grouping, expand a group to view the issues it contains.
To audit displayed issues:

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

![Image of Code tab displaying an issue in Fortify Software Security Center]

**Note:** This screen capture shows the details for an issue uncovered during a Fortify Static Code Analyzer scan. For information about viewing Fortify WebInspect results, see "Viewing Fortify WebInspect Scan Results in Fortify Software Security Center" on page 272.

In the left panel of the **Code** tab, the **Overview** section displays a summary of the issue, the analysis value (if set), and the analysis trace. The panel on the right displays the primary section of code in which the issue was discovered.
2. To see view summary details about a step along the course that tainted data has taken, in **Analysis Trace** section, move your cursor to that step. To view code associated with that step, click the step in the **Analysis Trace** section.

3. To search for a specific string in the code associated with the issue, click the **Search in source code** icon, type the character string, and then use the next \( \rightarrow \) and previous \( \leftarrow \) icons to move through the results.

4. To view the issue history and any comments related to the issue, click **Comments & History**.

5. To add a comment, type it into the **Comments** box, and then click **Post Comment**. You can mark an issue as **suppressed** to exclude it from display either because it is not of high priority or of immediate concern. This might include issues that you know to be fixed, or issues that you plan not to fix.

6. (Optional) To mark the issue as suppressed, click **Suppress**.
You can attach an image file to an issue. The image file must be smaller than 3MB, and in JPG, JPEG, BMP, PNG, or GIF format.

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

7. To attach an image file to the issue:
   a. Select **Attachments**.
   b. Select **Click here to add**.
   c. In the Upload Attachment dialog box, click **Browse**, and then navigate to and select the image file (JPG, JPEG, BMP, PNG, or GIF) to upload.

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

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

8. Do one of the following:
   - At the bottom of the issue details section, click **Assign**.

   Alternatively,
   - In the left panel, to the right of the **Analysis** field, click the **Assign Issue** icon.
9. From the **Analysis** list in the left panel, select a value that reflects your assessment of this issue.

10. If additional custom tags are associated with the application version, specify the values for these tags.

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

   **Note:** If Audit Assistant assessed the issues, the Assign dialog box displays additional fields **AA_Prediction**, **AA_Confidence**, and **AA_Training**. For information about how to use these fields, see “Reviewing Audit Assistant Results” on page 267.

11. To locate a user to assign to the issue, in the **Find user** box, type part or all of a user's name, and then click **Find**. Alternatively, to list all users in the system, click **Find all users**.

12. In the list of returned names, click the name of the user to assign to the issue.

   The Assigned section now displays the selected user name and avatar (if available).

13. (Optional) In the text box at the bottom of the right panel, you can type a comment about this issue audit.

14. Click **Apply**.
15. To collapse the issue details view, click the row again.

See Also
"About Auditing" on page 242

Accessing the Audit Page from the Issue Stats Page of the Dashboard

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

1. On the Hewlett Packard Enterprise header, click **Dashboard**.
2. In the application version summary table, select the link to the application version of interest.

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

Next
"Auditing Issues" on page 244

See Also
"Accessing the Audit Page from the Applications View" below

Accessing the Audit Page from the Applications View

To access the Audit page from the **Applications** view:

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

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

Next
"Auditing Issues" on page 244

See Also
"Accessing the Audit Page from the Issue Stats Page of the Dashboard" above

Filtering Issues for Display on the Overview and Audit Pages

Use the following steps to filter issues for display for an application version from either the Overview page or from the Audit page.

Note: You can also select a filter set to change the issues displayed on the Overview and Audit pages. For information and instructions, see "Changing Displayed Issues Using Filter Sets" on page 257.
To filter issues for display on the **Overview** or **Audit** page:

1. From the **Group by** list, select the attribute to use to group the issues in the issues table.
2. From the **Filter by** list, select the attributes to use to filter the issues for display in the issues table. You can select multiple attributes from this list. However, you must select them one at a time.
3. To filter issues based on values for a custom tag other than Analysis, or based on risks related to OWASP, WASC, or other security threat classifications:
   a. Click **Advanced**.
      The **Advanced Issue Filters** window opens.
   b. From the **Select filter category** list, select a category.
      The **Select filters** list is populated with the filters available for the selected category.
   c. To refine the **Select filters** list further, type a text string in the text box.
      The **Select filters** list displays the filters that contain the text that matches the text you typed.
   d. In the **Select filters** list, click each of the filters you want to add to the **Selected filters** list to the right.
   e. To add filters for another filter category, repeat these steps.
   f. Click **Apply**.
The Filter by box now displays all of the filters you have selected.

4. To remove one of the filters, click the close symbol to its left.

5. To clear all selected filters, click the Clear all icon.

See Also

"Searching Issues" on the next page

"Searching Globally in Fortify Software Security Center" on page 270

Viewing Issues Assigned to You

To view all issues assigned to you:

2. In the Applications view, select the My assigned issues check box.

The Applications view lists the application versions and shows the number of issues for each that are assigned to you. If Fortify Software Security Center finds no issues assigned to you, it displays a message to let you know.

See Also

"Viewing Removed Issues" on page 269
Searching Issues

You can create search queries to refine the list of issues displayed for an application version. To indicate the type of comparison to perform, wrap search terms with delimiters.

To create a query to search issues:

1. Access the Audit page for the application version. (See "Accessing the Audit Page from the Applications View" on page 249 or "Accessing the Audit Page from the Issue Stats Page of the Dashboard" on page 249.)

2. In the Search Issues box, type search query using the following syntax:

<table>
<thead>
<tr>
<th>Comparison</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>contains</td>
<td>Searches for a term without any special qualifying delimiters</td>
</tr>
<tr>
<td>equals</td>
<td>Searches for an exact match if the term is enclosed in quotation marks (&quot;&quot;)</td>
</tr>
<tr>
<td>number range</td>
<td>Uses standard mathematical syntax, such as &quot;(&quot; and &quot;)&quot; for exclusive range and &quot;[&quot; and &quot;]&quot; for inclusive range where (2,4] means greater than two less than or equal to four</td>
</tr>
<tr>
<td>not equal</td>
<td>Excludes issues specified by the string by preceding the string with an exclamation character (!) Example: file:!Main.java returns all issues that are not in Main.java</td>
</tr>
</tbody>
</table>

**Note:** to See example search strings, click the Syntax Guide link.

You can further qualify your search terms with modifiers using the syntax modifier:<search_term>. (See "Search Modifiers" on the next page.)

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

DateCustomTag: yyyy-mm-dd.

A search string can contain multiple modifiers and search terms. If you specify more than one modifier, Fortify Software Security Center returns only issues that match all of the modified search terms. For example, file:ApplicationContext.java category:SQL Injection returns only SQL injection issues found in ApplicationContext.java.

If you use the same modifier more than once in a search string, then the search terms qualified by those modifiers are treated as an OR comparison. For example, file:ApplicationContext.java category:SQL Injection category:Cross-
Site Scripting returns SQL injection issues and cross-site scripting issues found in ApplicationContext.java.

For complex searches, you can also insert the AND or the OR keyword between your search queries. Note that AND and OR operations have the same priority in searches.

3. Click **Find**.

   SSC lists all issues that match your search string.

4. To return to the complete issues list, clear the text in the search box.

**See Also**

"Filtering Issues for Display on the Overview and Audit Pages" on page 249

"Search Query Examples" on page 256

"Searching Globally in Fortify Software Security Center" on page 270

**Search Modifiers**

You can use a search modifier to specify which attribute of an issue the search term should apply to. To use a modifier that contains a space in the name, such as the name of the custom tag, you must delimit the modifier with brackets. For example, to search for issues that are new, enter [issue age]:new.

A search that you do not qualify using a modifier matches the search string based on the following attributes: kingdom, primary rule id, analyzer, filename, severity, class name, function name, instance id, package, confidence, type, subtype, taint flags, category, sink, and source.

To apply the search to all modifiers, enter a string such as control flow. This searches all modifiers and returns any result that contains the specified string.

To apply the search to a specific modifier, type the modifier name and the string as follows: analyzer:control flow. This returns all results whose analyzer is control flow.

The following table lists the search modifiers. A few of these have a shortened names, which are indicated in parentheses. You can use either modifier string.

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[issue age]</td>
<td>Searches for the issue age, which is new, updated, reintroduced, or removed.</td>
</tr>
<tr>
<td>&lt;custom_tagname&gt;</td>
<td>Searches the specified custom tag. Note that tag names that contain spaces must be delimited by square brackets. Example: [my tag]:value</td>
</tr>
<tr>
<td>analysis</td>
<td>Searches for issues that have the specified audit analysis value (such as exploitable, not an issue, and so on).</td>
</tr>
<tr>
<td>Modifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>analyzer</td>
<td>Searches the issues for the specified analyzer</td>
</tr>
<tr>
<td>audience</td>
<td>Searches for issues by intended audience. Valid values are targeted, medium, and broad.</td>
</tr>
<tr>
<td>audited</td>
<td>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.</td>
</tr>
<tr>
<td>category (cat)</td>
<td>Searches for the given category or category substring.</td>
</tr>
<tr>
<td>comments (com)</td>
<td>Searches for issues that contain the search term in the comments that have been submitted on the issue.</td>
</tr>
<tr>
<td>commentuser</td>
<td>Searches for issues with comments from the specified user.</td>
</tr>
<tr>
<td>confidence (con)</td>
<td>Searches for issues that have the specified confidence value. Fortify Static Code Analyzer calculates the confidence value based on the number of assumptions made in code analysis. The more assumptions made, the lower the confidence value.</td>
</tr>
<tr>
<td>file</td>
<td>Searches for issues where the primary location or sink node function call occurs in the specified file.</td>
</tr>
<tr>
<td>[fortify priority order]</td>
<td>Searches for issues that have a priority level that matches the specified priority determined by Fortify Static Code Analyzer. Valid values are critical, high, medium, and low, based on the expected impact and likelihood of exploitation. The impact value indicates the potential damage that might result if an issue is successfully exploited. The likelihood value is a combination of confidence, accuracy of the rule, and probability that the issue can be exploited.</td>
</tr>
<tr>
<td>historyuser</td>
<td>Searches for issues that have audit data modified by the specified user.</td>
</tr>
<tr>
<td>kingdom</td>
<td>Searches for all issues in the specified kingdom.</td>
</tr>
<tr>
<td>maxconf</td>
<td>Searches for all issues that have a confidence value equal to</td>
</tr>
<tr>
<td>Modifier</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>&lt;metadata_listname&gt;</td>
<td>Searches the specified metadata external list. Metadata external lists include [OWASP Top 10 2013], [SANS Top 25 2011], and [PCI 3.2], and others. Square braces delimit field names that include spaces.</td>
</tr>
<tr>
<td>minconf</td>
<td>Searches for all issues that have a confidence value equal to or greater than the number specified as the search term.</td>
</tr>
<tr>
<td>package</td>
<td>Searches for issues where the primary location occurs in the specified package or namespace. For dataflow issues, the primary location is the sink function.</td>
</tr>
<tr>
<td>[primary context]</td>
<td>Searches for issues where the primary location or sink node function call occurs in the specified code context. Also see sink and [source context].</td>
</tr>
<tr>
<td>primaryrule (rule)</td>
<td>Searches for all issues related to the specified sink rule.</td>
</tr>
<tr>
<td>sink</td>
<td>Searches for issues that have the specified sink function name. Also see [primary context].</td>
</tr>
<tr>
<td>source</td>
<td>Searches for dataflow issues that have the specified source function name. Also see [source context].</td>
</tr>
<tr>
<td>[source context]</td>
<td>Searches for dataflow issues that have the source function call contained in the specified code context. Also see source and [primary context].</td>
</tr>
<tr>
<td>sourcefile</td>
<td>Searches for dataflow issues with the source function call that the specified file contains. Also see file.</td>
</tr>
<tr>
<td>status</td>
<td>Searches issues that have the status reviewed, not reviewed, or under review.</td>
</tr>
<tr>
<td>suppressed</td>
<td>Searches for suppressed issues.</td>
</tr>
<tr>
<td>taint</td>
<td>Searches for issues that have the specified taint flag.</td>
</tr>
</tbody>
</table>

For examples of search queries that use modifiers, see "Search Query Examples" on the next page.
See Also

"Searching Issues" on page 252

Search Query Examples

The following are search query examples that use search modifiers.

- To search for all privacy violations in file names that contain jsp with getSSN() as a source, type:
  
  category: "privacy violation" source: getssn file: jsp

- To search for all file names that contain com/fortify/ssc, type:
  
  file: com/fortify/ssc

- To search for all paths that contain traces with mydbcode.sqlcleanse as part of the name, type:
  
  trace: mydbcode.sqlcleanse

- To search for all paths that contain traces with cleanse as part of the name, type:
  
  trace: cleanse

- To search for all issues that contain cleanse as part of any modifier, type:
  
  cleanse

- To search for all audited issues that have the [my tag] assigned and set to P1, type:
  
  [my tag]: P1

- To search for all suppressed vulnerabilities with asdf in the comments, type:
  
  suppressed: true comments: asdf

- To search for all categories except for SQL Injection, type:
  
  category: !SQL Injection

- To search for all issues in file names that contain either java or jsp, type:
  
  filename: java OR filename: jsp

- To search for all issues in file names that contain java and that occur on line number 12, type:
  
  filename: java AND line: 12

See Also

"Searching Issues" on page 252

"Search Modifiers" on page 253

About Suppressed, Removed, and Hidden Issues

You can control whether the issues panel lists the following types of issues:

**Suppressed issues**

As you assess successive scans of an application version, you might want to completely suppress some exposed issues. It is useful to mark an issue as suppressed if you are sure that the specific
vulnerability is not, and will never be, an issue of concern. You might also want to suppress warnings for specific types of issues that might not be high priority or of immediate concern. For example, you can suppress issues that are fixed, or issues that you plan not to fix. Suppressed issues are not included in the Total Issues value shown in the Version Progress section of the expandable panel on the Audit page. For information about how to suppress an issue, see “Auditing Issues” on page 244.

**Removed issues**

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

**Hidden issues**

In Fortify Audit Workbench, users typically hide a group of issues temporarily so that they can focus on other issues. For example, you might hide all issues except those assigned to you.

**Changing Displayed Issues Using Filter Sets**

Fortify Software Security Center provides the following filter sets for changing the display of application version issues on the Overview and Audit pages:

- **Quick View**
  
  The Quick View filter set provides a view only of issues in the Critical folder (these have a potentially high impact and a high likelihood of occurring) and the High folder (these have a potentially high impact and a low likelihood of occurring). The Quick View filter set provides a useful first look at results that enables you to quickly address the most pressing issues.

- **Security Auditor View**
  
  This view reveals a broad set of security issues to be audited. The Security Auditor View filter contains no visibility filters, so all issues are shown.

- **PCI Auditor View**
  
  This view is defined for individuals responsible for auditing an application with respect to its compliance with Payment Card Industry Security Standards.
Viewing Bugs Submitted for Issues

The issues table on the Audit page includes a “Bug submitted” column 🗿 that shows whether a bug has been submitted against a listed issue.

To view the bug, click the View bug icon 🗿, and log in to the assigned bug tracking application.

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

About Audit Assistant

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

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

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

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

The workflow for using Audit Assistant is as follows:

1. Obtain a Fortify Scan Analytics account, as follows:
   b. Click Need an Account?
   c. Complete the fields on the Request a Fortify Scan Analytics Tenant form, and then click Request Now.
      Fortify sends an email with information about how to connect to Fortify Scan Analytics.

2. From Fortify Scan Analytics, create one or more classifiers.
3. From Fortify Scan Analytics, create one or more policies.
4. (Optional) Choose to share anonymous metadata.
5. Obtain a Fortify Scan Analytics token.
6. From Fortify Software Security Center, configure and test the connection to Fortify Scan Analytics.
7. From Fortify Software Security Center, open an application version, and submit the latest completely audited scan to Audit Assistant. This step is referred to as training.
8. From Fortify Software Security Center, open an application version and submit its Fortify Static Code Analyzer scan results to Audit Assistant.
9. After Audit Assistant completes its assessment, view those results and, if necessary, adjust them.
10. Submit corrected results to Audit Assistant.

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

See Also
“Configuring Audit Assistant” on page 83
“About Classifiers and Prediction Policies” below
“Defining Classifiers” below
“Defining a Catch-All Classifier” on page 264
“Defining Prediction Policies” on page 264
“Enabling Metadata Sharing” on page 266
“Submitting Training Data to Audit Assistant” on page 266
“Reviewing Audit Assistant Results” on page 267

About Classifiers and Prediction Policies
To use Audit Assistant to process your scan results, you must first define classifiers and prediction policies in Fortify Scan Analytics.

Audit Assistant uses classifiers to classify issues and predict whether the issues represent true vulnerabilities. To define a classifier, you specify the criteria (issue attributes) that are to determine which Fortify Software Security Center issue training metadata to pull into Fortify Scan Analytics.

You must also define at least one prediction policy to map issue attributes to different classifiers. For example, you can establish a prediction policy that directs all .NET issues to Classifier_A, and all Java issues to Classifier_B, all cross-site scripting issues to Classifier_C, and so on.

When you submit a new scan to Audit Assistant for prediction, each Issue can go to different classifiers, based on the prediction policy you specify in Fortify Software Security Center.

Next
“Defining Classifiers” below

See Also
“Defining Prediction Policies” on page 264

Defining Classifiers
Audit Assistant uses classifiers to classify issues and predict whether or not they represent true vulnerabilities. To define classifiers, you specify the criteria (issue attributes) that determine which Fortify Software Security Center issue training metadata to pull into Fortify Scan Analytics.

Fortify recommends that you define at least two classifiers: one that filters for certain criteria, and a catch-all classifier that specifies no filters. Using a catch-all classifier with a prediction policy
ensures that issues that do not match any training criteria of other classifiers are still assessed. For information about how to use a catch-all classifier, see “Defining Prediction Policies” on page 264.

**Note:** If you submit no training data and you do not enable metadata sharing, then the underlying classifier is not created and all issues end up “Not Predicted.”

To define a classifier:

1. Log in to Fortify Scan Analytics ([https://analytics.fortify.com](https://analytics.fortify.com)).
   The Classifiers page opens.
2. Click **+Add**.
   The Classifiers | Add page opens.
3. Under **Details**, type the classifier name and (optionally) description.
   Next, you specify the training criteria for the classifier to use by building a set of one or more AND / OR statements.
4. Under **Training Filter Criteria**, use the lists and combo boxes to build your training filter criteria (groupings of ANDs and ORs) for the classifier.
   The following screen capture shows example training filter criteria for a classifier.
If you specify the value by selecting from a list of known values, as is true for attributes such as file type and language, then an **Override** check box is available under the list.

5. To specify a value that is not listed, select **Override**, and then type a value in the box.
6. To see the code for the filter you created, click **[preview]**.
7. Close the Training Filter Criteria box.

8. To delete an element (either a group, or a child of a group), click the red minus character (-) to the right of the element.

   In addition to the training data you submit to Audit Assistant, you can use the Fortify Community Intelligence data set. This is a large pool of anonymous data that Fortify customers have contributed for their training purposes.

9. To globally enable the use of (and contribute your metadata to) the Fortify Community Intelligence data set, follow the instructions provided in "Enabling Metadata Sharing" on page 266.

10. To use this classifier with only the training data that you submit from Fortify Software Security Center, leave the Limit to tenant training data check box selected. To use this classifier with your training data and the Fortify Community Intelligence data set, clear this check box.

    **Note:** The Limit to tenant training data check box is disabled if you have not enabled data sharing.

11. Click **Save**.

    For information about how to associate your classifiers to prediction policies, see "Defining Prediction Policies" on the next page.

**See Also**

"Configuring Audit Assistant" on page 83

"About Classifiers and Prediction Policies" on page 260
Defining a Catch-All Classifier

In addition to the classifiers you define to filter issues based on training criteria, Fortify strongly recommends that you create a catch-all classifier, for which you specify no training criteria. Using a catch-all classifier with a prediction policy ensures that issues that do not match any training criteria of other classifiers are still assessed.

To define a catch-all classifier:

1. Log in to Fortify Scan Analytics (https://analytics.fortify.com).
   The Classifiers page opens.
2. Click +Add.
   The Classifiers | Add page opens.
3. Under Details, type the classifier name and (optionally) description.
4. Click Save.

For information about how to associate your classifiers to prediction policies, see "Defining Prediction Policies" below.

See Also

"Defining Classifiers" on page 260

Defining Prediction Policies

Audit Assistant uses prediction policies to map issues to your classifiers.

To define a prediction policy:

1. Log in to Fortify Scan Analytics (https://analytics.fortify.com).
   The Prediction Policies | Add page opens.
2. In the left panel, select Prediction Policies.
3. Click +Add.
   The Prediction Policies | Add page opens.
4. In the Prediction Policy Name box, type a name for the policy.
   The Prediction Policies | Add page contains two confidence threshold settings. You use these to configure which issues Audit Assistant treats as indeterminate - that is, neither a true issue nor a non-issue.

Audit Assistant results include the following:

- The AA_Prediction value shows how each issue was assessed. Possible values are Exploitable, Not an issue, and Not Predicted.
- The AA_Confidence value (percentage value that ranges from 0.00 to 1.00) shows Audit Assistant's level of confidence in the AA_Prediction value.
If the **AA_Confidence** value falls below either of the confidence thresholds you set here for the prediction policy, then Audit Assistant treats the issue as indeterminate, and assigns it the **AA_Prediction** value **Not Predicted**.

5. Set the **Confidence Threshold - Not an Issue** and the **Confidence Threshold - Exploitable** sliders to an acceptable level for the applications on Fortify Software Security Center.

   **Note:** The higher you set the threshold values, the less likely it is that the Audit Assistant results contain false negatives. (Tests using the default 80% threshold values result in false negative occurrence of less than one percent.)

6. (Optional) In the **Description** box, type a policy description.

7. To associate a classifier with the prediction policy:
   a. Under **Classifiers**, from **Classifier Name** list, select a classifier name.
   b. Click **+Add**.

      The Prediction Policies | Add page imports the training criteria specified for the selected classifier as the mapping.

      In the following screen capture, the added classifier Java_JS specifies that, for this prediction policy, issues in either the Java or JavaScript language are to be sent to classifier Java_JS.

![Classifiers](image)

You can either use the classifier as is, or you can override the classifier for this prediction policy. The training criteria that determine what the classifier "learns" from, does not change.

   c. To override the classifier training criteria for this prediction policy:
      i. To the right of the training criteria, click the override icon 🆕.
      ii. In the Override Classifier Prediction Filter dialog box, modify the training criteria (just as you would if you were creating a classifier), and then click **OK**.

8. To associate another classifier with the prediction policy, repeat "To associate a classifier with the prediction policy." above.

   Audit Assistant filters issues based on the order in which you list the classifiers for the prediction policy, starting from the top.

9. To change the order of a classifier in the List, use the up and down arrows ⬆️ ⬇️ to the left of the classifier name.
Audit Assistant does not assess issues that do not match the filter criteria that the added classifiers specify. However, you can add a catch-all classifier to make sure that issues that do not meet the listed training criteria still get assessed.

10. To ensure that Audit Assistant assesses all issues, add your catch-all classifier as the last classifier. For information about how to create a catch-all classifier, see "Defining a Catch-All Classifier" on page 264.

11. To remove a classifier, click the red minus character (−) to the right of its name.

12. Click **Save**.

**See Also**

"About Classifiers and Prediction Policies" on page 260

"Defining Classifiers" on page 260

"Configuring Audit Assistant" on page 83

**Enabling Metadata Sharing**

You can contribute your audit metadata to the Fortify Community Intelligence data set (pool of anonymous auditing metadata from Fortify users). If you do, you can take advantage of the Fortify Community Intelligence data pool to assess your own data. Otherwise, Audit Assistant restricts the metadata it uses to assess your issues to just the training metadata you submit.

**Note:** If you submit no training data and you do not enable metadata sharing, then the underlying classifier is not created and Audit Assistant assesses no issues.

To enable data sharing:

1. Log in to Fortify Scan Analytics (https://analytics.fortify.com).
2. In the left panel, select **Settings**.
3. Select the **Share anonymous issue metrics** check box.
4. Click **Save**.

**See Also**

"About Classifiers and Prediction Policies" on page 260

"Defining Classifiers" on page 260

"Configuring Audit Assistant" on page 83

**Submitting Training Data to Audit Assistant**

The following procedure describes how to submit training data to Audit Assistant for assessment. Keep in mind that all data transferred from the Fortify Software Security Center environment is anonymized and contains no sensitive information.
To submit training data to Audit Assistant:

1. From the Dashboard, open a page (Overview, Artifact, Audit or Trend) for the application version of interest.
2. On the application version toolbar, click Profile.
3. In the Application Profile dialog box, click the Audit Assistant Training tab.

   **Note:** The Audit Assistant Training tab is visible only if Audit Assistant is configured. For information about Audit Assistant configuration, see "Configuring Audit Assistant" on page 83.

   The Data last sent for training field shows the date and time training data for the application version was last submitted.

4. To submit new training data, click Send for Training.
   
   The Data last sent for training field displays the Sending status.

5. After the Data last sent for training field is refreshed with the updated date and time, close the Application Profile dialog box.

6. On the application version toolbar, click Artifacts, and then check to see whether the Status field for your upload is Processing Complete.

After processing is completed, you can view the results from the Audit page. For instructions, see "Reviewing Audit Assistant Results" below.

**See Also**

"About Audit Assistant" on page 258

### Reviewing Audit Assistant Results

After you submit scan results to Audit Assistant and Audit Assistant finishes its assessment of the issues, you can examine the results.

To view Audit Assistant results:

1. Navigate to the Audit page for the application version.
2. Use the Group by list and Filter by lists.
3. To selectively display the issues you want to audit, apply filters to the issues list. (See "Filtering Issues for Display on the Overview and Audit Pages" on page 249.)
4. In the issues table, if you have selected a grouping, expand a group to view the issues it contains.
5. To expand an issue and view its details, click its row in the table.
6. In the lower right corner of the details section, click Assign.
The Assign dialog box opens.

In addition to the Analysis tag and any other custom tags associated with the application version, the left panel displays:

- **AA_Prediction** - Exploitability level that Audit Assistant assigned to the issue.
- **AA_Confidence** - Audit Assistant's level of confidence in the accuracy of its AA_Prediction value. This is a percentage, expressed in values that range from 0.000 to 1.000. For example, the value 0.982 indicates a confidence level of 98.2 percent.

7. If your exploitability assessment agrees with the AA_Prediction value displayed, you can select the same value from the Analysis list. Otherwise, select a different Analysis value.

8. To specify whether to include the issue in or exclude it from Audit Assistant training, from the AA_Training list, select either Include (the default) or Exclude.

   If the value you select from the Analysis list differs from the AA_Prediction value, and you select Include from the AA_Training list, then the next time you submit data for this application version to Audit Assistant, Audit Assistant updates the classifier based on your clarification.

9. Click **Apply**.

**See Also**

* "About Audit Assistant" on page 258
* "Auditing Issues" on page 244
Setting Issue Viewing Preferences

You can set certain viewing preferences for individual application versions from the Application Profile dialog box.

Viewing Suppressed Issues

To view the suppressed issues associated with an application version:

1. From the Applications view, select the version name for the application version you are interested in.
   Fortify Software Security Center opens the Overview page for the selected version.
2. On the application version toolbar, click **Profile**.
   The Application Profile dialog box opens to the **Advanced Options** tab.
   The number in parentheses (N) next to **Show suppressed issues** represents the total number of suppressed issues in the database associated with the selected application version.

   **Note:** The filter set you have selected does not affect the number of suppressed issues shown. For example, if a suppressed issue is hidden in the selected filter set, it is still included in the count of suppressed issues.

3. Select the **Show suppressed issues (N)** check box.
4. Click **Apply**.

See Also

"Viewing Removed Issues" below

Viewing Removed Issues

When Fortify Software Security Center merges uploaded scan results, it removes issues that were uncovered in the previous analysis but are no longer evident in the most recent results.

To view the issues that were removed for an application version:

1. From the Applications view, select the version name for the application version you are interested in.
   Fortify Software Security Center opens the Overview page for the selected version.
2. On the application version toolbar, click **Profile**.
   The Application Profile dialog box opens to the **Advanced Options** tab.
   The number in parentheses (N) next to **Show removed issues** represents the total number of removed issues in the database associated with the selected application version.

   **Note:** The filter set you have selected does not affect the number of removed issues shown. For example, if a suppressed issue is hidden in the selected filter set, it is still included in the count of removed issues.
3. Select the **Show removed issues (N)** check box.
4. Click **Apply**.

**See Also**

"Viewing Hidden Issues" below

"Viewing Suppressed Issues" on the previous page

**Viewing Hidden Issues**

In Fortify Software Security Center, hidden issues are the issues that are not shown because of the filter set rules currently in effect.

To reveal any hidden issues associated with an application version:

1. From the Applications view, select the version name for the application version you are interested in.
   Fortify Software Security Center opens the Overview page for the selected version.
2. On the application version toolbar, click **Profile**.
   The Application Profile dialog box opens to the **Advanced Options** tab.
   The number in parentheses (N) next to **Show hidden issues** represents the total number of hidden issues in the database associated with the selected application version.
3. Select the **Show hidden issues (N)** check box.
4. Click **Apply**.

**Searching Globally in Fortify Software Security Center**

Regardless of where you are in the Fortify Software Security Center user interface, you have access to the global **Search** field in the Hewlett Packard Enterprise header. Any search string you type here is applied across all application versions, issues, reports, comments, and users.
To use the global **Search** field:

1. From any view, type a search string into the **Search** box.

   ![Search field example](Image)

   Fortify Software Security Center displays the first several items that match your search string, grouped by category.

2. To go to a specific item listed, click the item.

   Fortify Software Security Center opens the user interface where you can view or work on the item.

3. To see a list of all search results, click **See All Results**.

**Example: Finding issues**

![Search field example](Image)

After you select a single issue from the listed results, Fortify Software Security Center takes you to the corresponding version page with the issue expanded to full view.
If you select **See All Results**, Fortify Software Security Center takes you to the **Search Results** page. From here, you can open the first match with the issue expanded to full view. From there, you can use the next and previous buttons to page through all of the findings.

**Example: Finding users**

![Search results for Simpson](image)

After you select a single user from the listed results, assuming you have the required permission, Fortify Software Security Center takes you to the details for the user account in the Administration view.

If you select **See All Results**, Fortify Software Security Center takes you to the **Search Results** page.

**See Also**

"Searching Applications and Application Versions from the Applications View" on page 195

**Fortify Software Security Center and WebInspect Enterprise Integration**

Fortify Software Security Center and Fortify WebInspect are closely integrated and can share scan results. Administrators can also submit requests for WebInspect dynamic scans from the Fortify Software Security Center interface. This section describes how to view WebInspect results in Fortify Software Security Center and provides instructions for Fortify Software Security Center users on how to request scans.

**Viewing Fortify WebInspect Scan Results in Fortify Software Security Center**

Fortify WebInspect saves scan results (results data and audit data) in FPR format, which you can upload to Fortify Software Security Center. (See "Uploading Scan Artifacts" on page 229.) Fortify WebInspect issue details differ somewhat from those shown for issues uncovered by other analyzers, such as Fortify Static Code Analyzer.

The screen capture on the following page shows the details displayed on Fortify Software Security Center Audit page for an issue uncovered during a Fortify WebInspect scan.
In the left panel of the **Code** tab, the **Overview** section displays summary information about the finding, the analysis value (if set), and the **Implications** section. The **Additional References** section lists any pertinent references available.

The panel on the right 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. (See previous screen capture.)

As the following screen capture shows, responses that contain binary data or a large volume of data (more than 50 KB) to display are not highlighted. To download responses such as these in a text file, click **Download Response**.
Note: The **Steps** tab is available only if the steps are included in the WebInspect results file.

Viewing Additional Details and Recommendations

To view additional details and recommendations for the issue, on the issue toolbar, click one of the following:

- **Open in new tab**
- **Expand to full screen**

On the right, the **Detailed Advice** panel opens to the **Details** section, which provides suggestions on what to look for in this issue.
To view recommendations and tips on how to address the issue, from the Details list, select Recommendations.

For information about how to audit the issue, see "Auditing Issues" on page 244.

WebInspect Audit Data

In addition to screen shots, the following types of audit data are transferred from WebInspect to Fortify Software Security Center:

- **Vulnerability Notes.** Vulnerability notes in WebInspect are transferred to Fortify Software Security Center as issue comments.
- **Ignored Vulnerabilities.** Vulnerabilities marked as “ignored” in WebInspect are marked “Suppressed” upon transfer to Fortify Software Security Center.
- **False Positives.**

False Positives

Fortify Software Security Center does not have a direct equivalent of the Fortify WebInspect “false positive” status. If a Fortify WebInspect user marks a vulnerability as a false positive, the vulnerability is hidden from the vulnerability lists and is removed from the vulnerability counts.

To emulate the false positive status in Fortify Software Security Center, you can use the default Analysis custom tag. A Fortify WebInspect false positive is assigned the Analysis value “Not an Issue” in Fortify Software Security Center. To emulate the Fortify WebInspect behavior of hiding the issue from lists and counts, the issue is marked as **Suppressed.**

Note: If the selected value for Analysis has changed from “Not an Issue” or is missing, or if the Analysis list has been removed from your application version, then the false positive status of the issue is lost. The issue is marked as “Suppressed.”

See Also

"Viewing Suppressed Issues" on page 269
Chapter 16: Integrating with Fortify CloudScan

If Fortify Software Security Center is configured to communicate with Fortify CloudScan, then the Fortify Software Security Center user interface includes the Scans view, which contains the CloudScan Scan Requests, Sensors, Controller and Sensor Pools pages. The following sections describe these pages and their functionality. For information about how to configure the connection between Fortify Software Security Center and CloudScan, see “Configuring CloudScan Monitoring in Fortify Software Security Center” on page 86.

This section contains the following topics:

CloudScan Permissions ................................................................. 276
Viewing CloudScan Scan Request Details ..................................... 277
Exporting CloudScan Scan Request Details ................................... 278
Canceling CloudScan Scan Requests ........................................... 278
Viewing CloudScan Sensor Information ....................................... 279
Viewing CloudScan Controller Information ................................... 280
About Fortify CloudScan Sensor Pools ......................................... 281
Creating CloudScan Sensor Pools .................................................. 282

CloudScan Permissions

The following table shows which Fortify Software Security Center roles have permission to perform which CloudScan-related tasks.

<table>
<thead>
<tr>
<th>Roles</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developer</td>
<td>View information on the Scan Requests, Sensors, and Sensor Pools pages</td>
</tr>
<tr>
<td></td>
<td><strong>Restrictions:</strong></td>
</tr>
<tr>
<td></td>
<td>• Users see only the scan requests for application versions to which they are assigned</td>
</tr>
<tr>
<td></td>
<td>• Users see only sensor pool assignment for the application versions to which they are assigned</td>
</tr>
<tr>
<td>Administrator</td>
<td>View information on the Scan Requests, Sensors, and Sensor Pools pages</td>
</tr>
</tbody>
</table>

Page 276 of 322
Security Lead Manager

Performing all tasks that involve changes to sensor pool
Cancel scan requests
Assign sensors and application versions to sensor pools.

Restrictions:
- Users can cancel only those scan requests for application versions to which they are assigned
- Users can assign only application versions to which they are assigned to sensor pools

To see what actions each Fortify Software Security Center role can perform:

1. On the Hewlett Packard Enterprise header, select Administration.
2. In the left panel, select Users, and then select Roles.
   The Roles table lists all of the roles to which you can assign users.
3. To see all of the actions a user in a given role can perform, click the row for the role.

Viewing CloudScan Scan Request Details

To view details on CloudScan scan requests:

1. On the Hewlett Packard Enterprise header, click Scans.
   The Scans view opens to the Scan Requests page, which lists all scan requests and details for each, including the job token for the request, the build ID, status, application version, and more.
2. To filter the displayed requests based on current state, from the Filter by list, select a state.
3. To expand a row and see more detail about a given scan, click the row.
4. To update the data displayed, click Refresh Table.

See Also
Exporting CloudScan Scan Request Details

To export the details related to a CloudScan scan request:

1. On the Hewlett Packard Enterprise header, click **Scans**.
   
   The Scans view opens to the Scan Requests page, which lists all scan requests and the details for each, including the job token for the request, the build ID, status, application version, and more.

2. To filter the displayed requests based on current state, from the **Filter by** list, select a state.

3. To see the details for a scan, click its row.

4. Do one of the following:
   
   - If the scan was completed and you want to export the resulting FPR file, click **Export**, select **FPR**, and then specify the directory to which you want to save the file.
   
   - To export the log for the scan (with any status except for Scan Faulted), click **Export**, select **Log**, and then specify the directory to which you want to save the file.

See Also

- "Viewing CloudScan Sensor Information" on the next page
- "Viewing CloudScan Controller Information" on page 280

Canceling CloudScan Scan Requests

To cancel a prepared CloudScan scan request:

1. On the Hewlett Packard Enterprise header, click **Scans**.

2. To cancel a scan, click its row and then select **Cancel**.
1. On the Hewlett Packard Enterprise header, click **Scans**.
   The Scans view opens to the Scan Requests page, on which a table lists all scan requests and the details for each.
2. To filter the displayed requests based on current state, from the **Filter by** list, select a state.
3. Expand the row for the prepared scan request that you want to cancel.
4. At the bottom right, click **Cancel Scan**.
   Fortify Software Security Center prompts you to confirm that you want to cancel the request.
5. Confirm the cancellation.
6. To update the data displayed on the Scan Requests page, click **Refresh Table**.

**See Also**

"Exporting CloudScan Scan Request Details" on the previous page

**Viewing CloudScan Sensor Information**

To view current information about CloudScan sensor states and activities:

1. On the Hewlett Packard Enterprise header, click **Scans**.
   The Scans view opens to the Scan Requests page, on which a table lists all sensors and the details for each.
2. In the left panel, select **CloudScan**, and then select **Sensors**.
   
   ![Sensors Panel](image)

   A sensor can be in the active, inactive, or stale state.
3. To filter the displayed sensors based on current state (**Active**, **Inactive**, or **Stale**) from the **Filter by** list, select a state. (**All States** is the default.)
4. To expand a row and see more detail about a sensor, click the row.

See Also

"Viewing CloudScan Scan Request Details" on page 277
"Canceling CloudScan Scan Requests" on page 278

Viewing CloudScan Controller Information

To view CloudScan Controller information:

1. On the Hewlett Packard Enterprise header, click **Scans**.
   The Scans view opens to the Scan Requests page, on which a table lists all scan requests and the details for each.

2. In the left panel, select **CloudScan**, and then select **Controller**.
3. For descriptions of the information displayed, click the information icons.

See Also

"Viewing CloudScan Scan Request Details" on page 277
"Canceling CloudScan Scan Requests" on page 278
"Viewing CloudScan Sensor Information" on page 279

About Fortify CloudScan Sensor Pools

If your Fortify Software Security Center server is integrated with Fortify CloudScan, and you are an Administrator, Manager, or Security Lead, you can create groups of sensors, or sensor pools, based on any criteria, which you can then target for scan requests.

Sensor pools give you more control over what sensors are used for scan requests. Here are a couple of examples of how you might use sensor pools:

- Create pools based of sensor computing power (size of physical memory) and assign scan requests that require a lot of memory to those pools.
- Create pools based on teams or business units in your organization, so that your resources are distributed no team can consume all sensors and block scan requests submitted by others teams.

If a scan request is associated with an application version, the CloudScan Controller queries Fortify Software Security Center for available sensor pools. If the scan request is not associated with an application version, Fortify CloudScan clients can request a specific sensor pool for a scan request.

Pre-defined Sensor Pools

Fortify Software Security Center provides two pre-defined sensor pools: the unassigned sensor pool and the default pool. The unassigned sensor pool, which contains all newly-registered sensors, serves as a shared sensor pool for other pools. The default sensor pool uses sensors from the unassigned sensor pool. It contains scan requests that were not assigned to a specific sensor pool.

See Also
Creating CloudScan Sensor Pools

If your Fortify Software Security Center server is integrated with CloudScan, you can create CloudScan sensor pools, which you can then target for scan requests.

To create a new sensor pool:

1. On the Hewlett Packard Enterprise header, select **Scans**.
   The Scan Requests view opens to the Scan Requests page for CloudScan.

2. In the left panel, select **Sensor Pools**.
   The Sensor Pools page opens to **Sensor Pools** tab, which lists the Default Pool and any other sensor pools that were created.

   **Note:** The Default Pool is a pool of all application versions that have not been assigned to a sensor pool.

3. On the Sensor Pools page header, click **+New Pool**.
   The Create New Pool wizard opens.

4. On **Step 1. Assign Versions**, do the following:
   a. In the **Name** box, type a name for the new pool. Note that the first character of the pool name must be a Unicode alphanumeric character (lower or upper case a through z, or 0 through 9).
   b. In the **Description** box, type a description of the new pool (its properties or purpose).
   c. Under **Add Version**, from the list, select an application, the versions of which you want to assign to this pool.
The wizard lists all active versions of the selected application.

d. To have the wizard to list inactive and active versions of the selected application, select the Show inactive versions check box.

e. To assign all of the listed versions to the new pool, select the check box next to the application name. Otherwise, to assign only a subset of the application versions, select the check boxes next to the version names.

On the right, the wizard lists your selections under Selected Versions.

f. To assign versions of another application to this pool, repeat steps c through f.

g. To remove an application version form the Selected Versions list, click the trash icon next to its name.

5. Click Next.

6. On Step 2. Assign Sensors, do the following:

a. To locate a specific sensor, type part or all of its host's name in the search box, and then click Find.

The wizard lists all sensor hosts that include the specified text. The lock icon (🔒) next to the hostname indicates that the sensor is already assigned to a pool.

To see which pool the sensor is in, in the Sensor Hostname list, select the hostname, and then, in the Sensor information section, check the Assigned to value.

b. To see which pool the sensor is in, in the Sensor Hostname list, select the hostname, and then, in the Sensor information section, check the Assigned to value.

The Sensor information section also displays the sensor state, the host IP address, available memory, and the Fortify Static Code Analyzer version installed.

c. Select the check boxes for the sensors that you want to include in the pool.

The wizard lists your selections in the Selected Sensors list.

d. To add another sensor, repeat steps a through c.

e. To remove a sensor from the Selected Sensors list, either click the trash icon ( удален) next to its name, or clear the check box for the sensor in the Sensors list.

7. Click Finish.

The Sensor Pools table now lists your new pool. The Pool column in the table on the Sensors page also lists the new pool name for the sensors included.

You can edit or delete the pool at any time.

See Also

"Viewing CloudScan Sensor Information" on page 279

"Deleting CloudScan Pools" on the next page
Deleting CloudScan Pools

To delete a CloudScan pool:

On the Hewlett Packard Enterprise header, select **Scans**.

The Scan Requests view opens to the Scan Requests page for CloudScan.

2. In the left panel, select **Sensor Pools**.

The Sensor Pools page opens to **Sensor Pools** tab, which lists all existing pools. The last column of the table displays a **Delete Pool** icon for each pool. If the icon is blue 📌, you can delete the pool. If the icon is gray 📌, you cannot delete the pool.

3. Click the **Delete Pool** icon 📌 that corresponds to the pool you want to delete.

Fortify Software Security Center removes the pool from the list and adds all sensors assigned to the deleted pool to the **Unassigned Sensors** tab.

### See Also

- "Viewing CloudScan Sensor Information" on page 279
- "Creating CloudScan Sensor Pools" on page 282
Chapter 17: BIRT Reports

Fortify Software Security Center reports are based on the Business Intelligence and Reporting Technology (BIRT) system. BIRT is an open source reporting system based on Eclipse.

**Note:** Fortify Software Security Center cannot run reports with WebSphere Application Server (WAS) JRE while SSL is enabled. An external process such as BIRT ReportRunner does not have WebSphere SSL libraries on its classpath. SSL with IBM JRE works only for web applications deployed to WAS—not for standalone applications.

For information about BIRT, see the following page on the Eclipse website:

http://www.eclipse.org/birt/phoenix/intro

This section contains the following topics:

- Issue Reports ................................................................. 285
- Portfolio Reports ............................................................ 287
- Application Summary Report ............................................ 288
- Generating and Viewing Reports ...................................... 288
- Preventing Destructive Libraries and Templates from Being Uploaded .............................................................. 291
- BIRT Libraries ................................................................ 291
- Importing Report Libraries ............................................. 291
- Customizing Fortify Software Security Center BIRT Reports .............................................................. 292
- Acquiring the BIRT Report Designer ................................ 292
- Downloading Report Definitions ...................................... 293
- Importing Report Definitions ........................................... 293

**Issue Reports**

The Issue report group summarizes the presence of specific vulnerability categories in a single Fortify Software Security Center application version.

**CWE/SANS Top 25 Reports**

The CWE/SANS Top 25 reports detail findings related to the CWE/SANS top 25 most dangerous programming errors uncovered for an application version, and provide information about where and how to address the findings.
**Developer Workbook Report**

The Developer Workbook report, which is targeted at project managers and developers, contains all of the information needed to understand and fix issues discovered during an application version audit.

**DISA STIG Reports**

The DISA STIG reports, which are targeted at project managers, security auditors, and developers, address DISA compliance through violations found in an application version. They provide information about where and how to fix the issues, and details about the technical risks posed by unremediated violations. The reports also include an estimate of the effort required to fix, verify, and test the findings.

**FISMA Compliance: FIPS - 200 Report**

The FISMA Compliance: FIPS - 200 report, which is targeted at project managers, security auditors, and developers, addresses FISMA compliance through FIPS-200 violations detected in an application version. It provides information about where and how to fix the issues, as well as details about the technical risks posed by unremediated violations. The report also includes an estimate of the effort required to fix, verify, and test the findings.

**OWASP Mobile Top 10 Reports**

The OWASP Mobile Top 10 reports, which are targeted at project managers, security auditors, and software developers, detail the top ten OWASP mobile-related findings for an application version. They provide information on where and how to fix specific issues and on the technical risk posed by the unremediated findings discovered during analysis. The reports also provide estimates of the effort required to fix, verify, and test the findings.

**OWASP Top 10 Reports**

The OWASP reports, which are targeted at project managers, security auditors, and developers, detail the top ten OWASP-related findings for an application version. They include information about where and how to fix the issues, as well as details about the technical risks posed by unremediated violations. The reports also provide estimates of the effort required to fix, verify, and test the findings.

**PCI DSS Compliance: Application Security Report**

The PCI Compliance: Application Security Requirements report is targeted at project managers, security auditors, and compliance auditors. It summarizes the application security portions of PCI DSS. Software Security Center tests for 21 application security-related requirements across sections 3, 4, 6, 7, 8, and 10 of PCI DSS and reports on whether each requirement is either “in place” or “not in place.”
Penetration Testing Correlation Report

Use the Penetration Testing Correlation Report to correlate results from third-party penetration testing tools with issues detected by WebInspect Agent, Runtime Application Protection, and Static Source Code Analyzer issues for a Software Security Center application version.

Seven Pernicious Kingdoms Report

The Seven Pernicious Kingdoms Report is directed at project managers, security auditors, and developers. This report summarizes the findings related to the presence of several Fortify-defined issues (see https://vulncat.fortify.com) in an application version. It includes information about where and how to fix the issues, and details about the technical risks posed by unremediated issues. The report also provides estimates of the effort required to fix, verify, and test the findings.

Vulnerability Report

The Vulnerability Report provides an analysis of the security risk posed by an application version’s current status. It presents the vulnerability category and severity level distributions across the entire application. The report data enable managers to evaluate the security posture of an application and prioritize outstanding issues that require immediate attention.

Portfolio Reports

The Portfolio report group contains reports that enable you to compare issues trends and indicators across multiple Fortify Software Security Center application versions.

Hierarchical Summary Report

The Hierarchical Summary Report presents a three-level, hierarchical summary for all applications you select to include in the report. It provides the following information:

- Overview statistics for all selected applications
- A specific application attribute
- Applications grouped by owner

You can choose to exclude the project summary and owner details from the report.

Issue Trending Report

Use the Issue Trending Report to create an historical summary of issues by:

- Application version
- Issue categorization (Fortify Priority Order, Kingdom, or OWASP 2004, 2007, 2010, or 2013)
- Date range
The charts in this report show the number of issues found in each application you selected to include. They display the total number of issues, as well as a breakdown of High Priority and Critical Exposure issues per application.

**Key Performance Indicators Report**

The Key Performance Indicators Report summarizes multiple security performance indicators based on application attributes. Project managers and security officers can use this view of the application portfolio to perform basic comparisons between attribute groupings. This report permits indicators to be grouped by application type or other cross-application categories.

**Security at a Glance Report**

Use the Security at a Glance Report to produce a high-level overview of the security of your application portfolio. The data included in the report directs portfolio owners towards the top risk concerns within the portfolio. These concerns are presented in the form of riskiest applications and the most pervasive vulnerability types found.

Combined with the enterprise business risk data, this information helps you prioritize resources in your remediation efforts. The information is presented so that it is most useful for security officers and project managers.

**Application Summary Report**

Use the Application Summary report to summarize a single version of an application. This report includes a high-level look at the outstanding issues associated with the application version and detailed information related to its risk profile. It also includes a summary of the user activities.

**Generating and Viewing Reports**

To generate and view a Fortify Software Security Center report:

1. On the Hewlett Packard Enterprise header, click Reports.
   The Reports page opens.
3. To see a description of the report that results from a listed template, move your cursor to the report listing, and then move it to the information icon.

4. Navigate to and select the report template you want to use.
   The panels on the right display the configuration fields for the template you select.

5. Specify the required report settings, including the report name, output format, and application versions to include in the report.
   Depending on the report type, additional settings might be required or available.

6. If multiple editions of a report template are available, from the Options list, select the edition you want to generate.

7. Click Generate.
Fortify Software Security Center adds the report to the **Reports** table, which lists all reports, based on category. After the report generation is completed, the **Status** field displays the value **Processing Complete**.

**Note:** If you typed content in the **Notes** box when you configured the report, the **Notes** column displays a note icon for the report.

8. To view the report, move your cursor to the report name, and then click **Download**.

9. Save or open the report.
Preventing Destructive Libraries and Templates from Being Uploaded

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

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

- Make sure to assign these permissions only to trusted users.
- Make sure to check all custom templates for arbitrary SQL queries and commands before uploading them to Fortify Software Security Center.

**BIRT Libraries**

With BIRT Libraries, commonly required functions and report items can be encapsulated. These libraries can then be imported into any number of BIRT reports for reuse. In addition, the concept of libraries helps segment report development tasks, as opposed to requiring a single report developer to create all components for each report by himself.

**Note:** Before you use the BIRT report libraries, you must acquire the BIRT Report Designer. For instructions, see "Acquiring the BIRT Report Designer" on the next page.

Reports that reference libraries are automatically updated during report execution. This is useful in cases where business or technical changes would otherwise require report rework. For example, if a library component such as a corporate logo is used in a large number of report designs, then a change to the logo would only require a change to the library. All referencing reports would reflect the change automatically.

**Importing Report Libraries**

If you are an Administrator-level user, you can add report libraries to the Fortify Software Security Center server.

To add a report library:

1. In the left panel of the Administration view, select **Templates**, and then select **Report Libraries**.
   The **Report Libraries** page lists all of the report libraries in the system.
2. In the **Report Libraries** toolbar, click **Import**.
The Import New Library Template dialog box opens.

3. (Optional) In the **Description** box, type a description of the library you are importing.

4. Click **Browse**, and then navigate to and select the report library resource.

5. Click **Save**.

The **Report Libraries** list now includes the library you added.

### Customizing Fortify Software Security Center BIRT Reports

Customizing BIRT reports is not a beginner-level activity. Customizing Fortify Software Security Center reports requires an understanding of database operation and design, SQL syntax, and report design.

To customize a Fortify Software Security Center BIRT report:

1. Acquire a supported version of Eclipse BIRT Report Designer (**Report Designer**).
   For information about the BIRT Report Designer versions supported for Fortify Software Security Center reports, see the *HPE Security Fortify Software System Requirements* document.
   For information about downloading Eclipse BIRT Report Designer, see "Acquiring the BIRT Report Designer" below.

   You typically first export a report definition from Fortify Software Security Center, and then upload that report definition into Report Designer. For information about how to export a Fortify Software Security Center report definition, see "Downloading Report Definitions" on the next page.

   Connecting Report Designer to the Fortify Software Security Center database enables you to load and verify the database queries you add to a BIRT report.

4. Use the Report Designer to add report design elements to the report definition, and add database queries to those design elements.

5. Use a local instance of Fortify Software Security Center to test the operation of a customized BIRT report.

6. Import the customized report definition into Fortify Software Security Center.
   For information about importing report definitions into Fortify Software Security Center, see "Importing Report Definitions" on the next page.

### Acquiring the BIRT Report Designer

To customize Fortify Software Security Center reports, you must use a supported version of the Eclipse BIRT Report Designer (**Report Designer**). For information about supported versions, see the *HPE Security Fortify Software System Requirements* document.
To download the Eclipse BIRT Report Designer:

1. Open a web browser window and go to the following download page:
2. Download the Report Designer Full Eclipse Install for your operating system.

**Downloading Report Definitions**

To download a Fortify Software Security Center report definition:

1. On the Hewlett Packard Enterprise header, click **Reports**.
2. In the **Reports** table, select the report.
   - The row expands to display the report description, category, and document type.
   - Fortify Software Security Center displays the Reports Definition page, which lists all defined reports.
3. Click **Download**.
   - The Opening <Report_File_Name> dialog box opens.
4. Click **Save**, and then click **OK**.

Fortify Software Security Center exports the report to your **Downloads** folder.

**Importing Report Definitions**

Fortify Software Security Center reports are based on the open-source Business Intelligence and Reporting Tools (BIRT) system. A BIRT report definition provides the Fortify Software Security Center report engine the information it needs to generate a report. This includes information such as the report name, report parameters, and the name of the report template file.

BIRT enables you to add import report definitions files to Fortify Software Security Center. To do this, you need a Fortify Software Security Center BIRT definition (with the **rptdesign** filename extension).

To import a report definition:

1. On the Hewlett Packard Enterprise header, click **Administration**.
2. In the left panel, select **Templates**, and then select **Reports**.
   - The **Reports** table lists existing report templates, along with the report template types and descriptions.
3. Click **Import**.
   - The Import New Report Template dialog Box opens.
4. Configure the new report definition as follows:
   - Type or choose the **Name, Description, Report Engine, and Category** settings.
   - In the **Template** area, browse to the Fortify Software Security Center BIRT definition (with the **rptdesign** filename extension).
5. Add one or more optional parameters to the new report definition.
   - In the Parameters area, click **Add**.
   - Type or choose the **Name**, **Description**, **Identifier**, and **Data Type** settings that correspond to those values in the BIRT template you are uploading.

6. To add the new report definition to the list of definitions, click **Save**.
Chapter 18: Authentication Tokens

Authentication tokens are unique keys that enable users to automate actions within Fortify Software Security Center without using passwords. The user requests a token, authenticates to the Fortify Software Security Center server, and receives back a string that is permissioned for a small set of time-limited actions.

For example, the AnalysisUploadToken token does not allow the user to log in to the interface or view results.

Common actions include uploading scan results and downloading reports.

Generating Authentication Tokens

To generate a token, run the following command:

```
fortifyclient token -gettoken <token_name> -url SSC_URL -user USERNAME -password
```

The following table lists the available `token_name` options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnalysisUploadToken</td>
<td>Upload scan results to Fortify Software Security Center and list applications</td>
</tr>
<tr>
<td>AuditToken</td>
<td>Load details about current security issues and apply analysis tags</td>
</tr>
<tr>
<td>AnalysisDownloadToken</td>
<td>Download merged result files</td>
</tr>
<tr>
<td>JenkinsToken</td>
<td>Authorizes the web service requests that the Jenkins plugin uses</td>
</tr>
<tr>
<td>ReportToken</td>
<td>Enables users to:</td>
</tr>
<tr>
<td></td>
<td>Request list of saved reports</td>
</tr>
<tr>
<td></td>
<td>Request saved report based on the report ID</td>
</tr>
<tr>
<td></td>
<td>Delete saved reports</td>
</tr>
<tr>
<td></td>
<td>Return list of saved reports associated with a specific application version</td>
</tr>
<tr>
<td></td>
<td>Generate new reports</td>
</tr>
</tbody>
</table>

Authentication tokens are defined at runtime in WEB-INF/internal/serviceContext.xml.
See Also

"Specifying DaysToLive for fortifyclient Authentication Tokens" on page 301.
Appendix A: LDAP Configuration Property Descriptions

The `ldap.properties` file contains parameters for a single specific LDAP server. The LDAP server parameters are listed in the following table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Property Name from the Legacy (4.30) ldap.properties File</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Server Usage Flag</td>
<td>ldap.enabled</td>
</tr>
<tr>
<td>Cache Usage Flag</td>
<td>ldap.cache</td>
</tr>
<tr>
<td>URL</td>
<td>ldap.url</td>
</tr>
<tr>
<td>Base Domain Name</td>
<td>ldap.base.dn</td>
</tr>
<tr>
<td>LDAP User Name</td>
<td>ldap.user.dn</td>
</tr>
<tr>
<td>LDAP Password</td>
<td>ldap.user.password</td>
</tr>
<tr>
<td>Search Domain Name</td>
<td>ldap.search.dns</td>
</tr>
<tr>
<td>User Class</td>
<td>ldap.class.user</td>
</tr>
<tr>
<td>User Name</td>
<td>ldap.attribute.username</td>
</tr>
<tr>
<td>First Name</td>
<td>ldap.attribute.firstname</td>
</tr>
<tr>
<td>Last Name</td>
<td>ldap.attribute.lastname</td>
</tr>
<tr>
<td>E-mail</td>
<td>ldap.attribute.email</td>
</tr>
<tr>
<td>Group Class</td>
<td>ldap.class.group</td>
</tr>
<tr>
<td>Group Name</td>
<td>ldap.attribute.groupname</td>
</tr>
<tr>
<td>Group Member</td>
<td>ldap.attribute.member</td>
</tr>
<tr>
<td>Org Unit Name</td>
<td>ldap.attribute.orgunitname</td>
</tr>
<tr>
<td>Org Unit Class</td>
<td>ldap.class.orgunit</td>
</tr>
<tr>
<td>Object Class</td>
<td>ldap.attribute.objectclass</td>
</tr>
<tr>
<td>Parameter</td>
<td>Property Name from the Legacy (4.30) ldap.properties File</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>Distinguished name</td>
<td>ldap.attribute.distinguishedname</td>
</tr>
<tr>
<td>Nested Group Usage Flag</td>
<td>ldap.nestedgroups</td>
</tr>
<tr>
<td>Max Thread Number</td>
<td>ldap.cache.max.threads.per.cache</td>
</tr>
<tr>
<td>Pool Size</td>
<td>ldap.cache.executor.pool.size</td>
</tr>
<tr>
<td>Max Pool Size</td>
<td>ldap.cache.executor.pool.size.max</td>
</tr>
</tbody>
</table>
Appendix B: Using the fortifyclient Utility

The topics in this section provide information about the Fortify Software Security Center fortifyclient command-line utility (on Windows systems, this is fortifyclient.bat) that you can use to securely transfer objects to and from Fortify Software Security Center.

Note: Throughout this section, <ssc_install_dir> represents the directory into which you extracted the HPE_Security_Fortify_<version>_Server_WAR_<application server>.zip file.

This section contains the following topics:

- fortifyclient Requirements .......................................................... 299
- Listing fortifyclient Options and Parameters .................................. 300
- About Uploading Authentication Tokens ........................................... 300
- Listing fortifyclient Authentication Tokens ...................................... 302
- Invalidating Tokens ........................................................................ 302
- Listing Application Versions ............................................................ 303
- Purging Application Versions ............................................................ 303
- About Uploading FPRs .................................................................... 304
- About Downloading FPRs ............................................................... 305
- Importing Content Bundles ............................................................... 307
- Downloading Audit Attachment Files ................................................ 308
- About Archiving and Restoring Runtime Events ................................. 308

fortifyclient Requirements

To use fortifyclient to upload scan results (FPR files), you must know the URL for your Fortify Software Security Center instance and have one the following:

- A user account on the Fortify Software Security Center server with privileges sufficient to perform the operation specified by the fortifyclient command-line utility
- A fortifyclient authentication token

Topics covered in this section:

- About Specifying the Fortify Software Security Center URL .................. 300
- fortifyclient Authentication Tokens .................................................. 300
About Specifying the Fortify Software Security Center URL

Most fortifyclient commands include the Fortify Software Security Center URL. The Fortify Software Security Center URL passed to fortifyclient must include both the port number and the context path /ssc/. The correct format for the Fortify Software Security Center URL is as follows:

```
http://<hostname>:<port>/ssc/
```

For example:

- For non-root applications: http://www.company.com/ssc
- For root applications: http://ssc.company.com

**Note:** In code examples in this guide, `<ssc_url>` represents a correctly formatted Fortify Software Security Center URL as described in this topic.

fortifyclient Authentication Tokens

fortifyclient authentication tokens enable scripted processes to perform operations without revealing Fortify Software Security Center user names and passwords. You can use the credentials for any existing Fortify Software Security Center user account to create an authentication token.

An authentication token inherits the privileges of the account type (Administrator, Security Lead, Manager, or Developer) of the user who creates the token. When fortifyclient uses an authentication token to perform an operation, Fortify Software Security Center logs the operation under the account name used to create the token.

Listing fortifyclient Options and Parameters

To list fortifyclient commands and parameters:

1. From the command line, navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. At the command prompt, type `fortifyclient`. (On a Windows system, type `fortifyclient.bat`)

In Fortify Software Security Center, command and option names are case-sensitive.

About Uploading Authentication Tokens

fortifyclient upload authentication tokens enable the concealment of account and password information as FPRs are uploaded to Fortify Software Security Center.
Topics covered in this section:

**Acquiring an Upload Authentication Token** ................................................................. 301
**Specifying DaysToLive for fortifyclient Authentication Tokens** ................................. 301

### Acquiring an Upload Authentication Token

To use `fortifyclient` to acquire an analysis upload token, you must have the following:

- Your Fortify Software Security Center URL (see "About Specifying the Fortify Software Security Center URL" on the previous page)
- A Fortify Software Security Center user account with privileges that enable you to use the `fortifyclient` access token

To use `fortifyclient` to acquire an analysis upload token:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory, and run the following:

   ```bash
   fortifyclient -url <ssc_url> token -gettoken AnalysisUploadToken -user <account_name>
   ```

   where `AnalysisUploadToken` is the case-sensitive `fortifyclient` upload token specifier. You are prompted for a password.

2. Type the password for `<account_name>`.
   - `fortifyclient` displays a token of the general form:
     ```
     cb79c492-0a78-44e3-b26c-65c14df52e86
     ```

3. Copy the returned token into a text file.
   
   The ability of `fortifyclient` to use the token to read or write information to or from Fortify Software Security Center depends on the privileges of the user account specified by the `-user` parameter.

### Specifying DaysToLive for fortifyclient Authentication Tokens

As described in "About Uploading Authentication Tokens" on the previous page, `fortifyclient` supports tokens that enable the administration to conceal user account information.

You can use the `-daysToLive` parameter to configure `fortifyclient` tokens to expire after a specified number of days. The following example command illustrates the use of the `-daysToLive` parameter to acquire a token that expires after two days:

```bash
fortifyclient -url <ssc_url> token -gettoken AnalysisUploadToken -user admin -daysToLive 2
```

where `<ssc_url>` represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on the previous page).

You must type the case-sensitive `daysToLive` parameter exactly as shown in the example above.
Listing fortifyclient Authentication Tokens

Fortify Software Security Center administrators can use fortifyclient to list all existing access tokens for all Fortify Software Security Center user accounts. The fortifyclient utility does not support filtering the list of tokens by Fortify Software Security Center account name or account privilege level.

To list all access tokens:

1. Navigate to the <ssc_install_dir>/Tools/fortifyclient/bin directory, and run the following:

   ```
   fortifyclient -url <ssc_url> listtokens -user <admin_account_name>
   ```

   where <ssc_url> represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 300) and <admin_account_name> is the name of a Fortify Software Security Center Administrator-level user account.

2. When prompted, type the password for the administrator-level user account. A list showing the ID, owner, creation date, expiration date, and creation IP address for all fortifyclient authentication tokens is returned.

Invalidating Tokens

To invalidate an existing authentication token:

1. Navigate to the <ssc_install_dir>/Tools/fortifyclient/bin directory.
2. Run the following:

   ```
   fortifyclient -url <ssc_url> invalidatetoken [ -invalidateByID <token_ID> | -invalidateForUser <owner> | -invalidate <token> ]
   ```

   where

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ssc_url&gt;</td>
<td>represents the URL of the Fortify Software Security Center instance (see &quot;About Specifying the Fortify Software Security Center URL&quot; on page 300)</td>
</tr>
<tr>
<td>&lt;token_ID&gt;</td>
<td>represents the ID of the token to invalidate</td>
</tr>
<tr>
<td>&lt;owner&gt;</td>
<td>represents the user for whom the token is to be invalid</td>
</tr>
<tr>
<td>&lt;token&gt;</td>
<td>represents the name of the token to invalidate</td>
</tr>
</tbody>
</table>
Listing Application Versions

You can use `fortifyclient` to list the Fortify Software Security Center application versions accessible by the account that was used to create a particular access token.

**Note:** Administrator-level users can view all application versions. Security Lead users can view all application versions they created or to which they have been granted access. Manager and Developer account users can view application versions to which they have been granted access.

To perform the command in this section, you must first obtain an upload authentication token. (See "About Uploading Authentication Tokens" on page 300.)

To retrieve a list of application identifiers, application names, and application versions:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

   ```bash
   fortifyclient -url <ssc_url> -authtoken <token> listApplicationVersions
   ```

   where `<ssc_url>` represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 300) and `<token>` is a valid `fortifyclient` authentication token. You can also use the `-user` and `-password` parameters to specify user account credentials.

   For all application versions accessible to the user account that created the token, the `fortifyclient` utility lists the application version ID, name, and number.

Purging Application Versions

To purge all artifacts in an application version that was scanned before a given date:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

   ```bash
   fortifyclient -url <ssc_url> purgeApplicationVersion <app_identifier>
                  -scanDate <MMDDYYYY>
   ```

   where `<ssc_url>` represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 300) and `<app_identifier>` represents the `-application` `<app_name>`, `-version` `<version_name>`, or `-applicationVersionID` `<id>`. 
About Uploading FPRs

Users periodically upload application analysis results files (in FPR format) to Fortify Software Security Center. To do this, you can use an authentication token or a username and password. The topics in this section describe how to upload FPRs using an authentication token. For examples of how to use a username and password, see “About Downloading FPRs” on the next page.

Fortifyclient upload access tokens support the use of the AccessUploadToken token to conceal user credentials when using scripts to upload FPRs to Fortify Software Security Center. To provide additional security, you can also use an access token’s DaysToLive parameter.

**Note:** To perform the procedures described in this section, you must first obtain an authentication token. (See “About Uploading Authentication Tokens” on page 300.)

You can upload FPR files using one of the methods described in the following topics:

- Using an Application Identifier to Upload FPR Files ......................................................... 304
- Using an Application Name and Version to Upload FPR Files ........................................... 305

Using an Application Identifier to Upload FPR Files

To upload an FPR into Fortify Software Security Center using an application identifier:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

   ```
   fortifyclient -url <ssc_url> -authtoken <token> uploadFPR -file <fpr_name> -applicationVersionID <id>
   ```

where

<table>
<thead>
<tr>
<th><code>&lt;ssc_url&gt;</code></th>
<th>represents the URL of the Fortify Software Security Center instance (see &quot;About Specifying the Fortify Software Security Center URL&quot; on page 300)</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;token&gt;</code></td>
<td>represents a valid fortifyclient authentication token</td>
</tr>
<tr>
<td><code>&lt;fpr_name&gt;</code></td>
<td>represents the full path and name of the FPR file with its extension</td>
</tr>
<tr>
<td><code>&lt;id&gt;</code></td>
<td>represents the Fortify Software Security Center application version identifier</td>
</tr>
</tbody>
</table>

For information about how to acquire Fortify Software Security Center application identifiers, see “Listing Application Versions” on the previous page.
Using an Application Name and Version to Upload FPR Files

To upload an FPR into a Fortify Software Security Center application version using the application name and version:

1. Navigate to the `ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

   ```bash
   fortifyclient -url <ssc_url> -authtoken <token> uploadFPR -file <fpr_name>
   -project <app_name> -version <app_version>
   ``

   where

   - `<ssc_url>` represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 300)
   - `<token>` represents a valid fortifyclient authentication token
   - `<fpr_name>` represents the full path and name of the FPR file with its extension
   - `<app_name>` represents the Fortify Software Security Center application name
   - `<app_version>` represents the Fortify Software Security Center application version that corresponds to the specified application name

About Downloading FPRs

You can use `fortifyclient` to download FPRs by specifying either the Fortify Software Security Center identifier or the application version. This section provides the procedures to download FPRs using both methods.

You can download FPRs using an authentication token or username and password. The topics in this section describe downloading FPRs using a username and password. For examples using an authentication token, see "About Uploading FPRs" on the previous page.

Topics covered in this section:

- Downloading an FPR Using an Application Identifier .......................................................... 306
- Downloading an FPR Using an Application Name and Version ............................................ 306
Downloading an FPR Using an Application Identifier

To use `fortifyclient` to download an FPR file to Fortify Software Security Center using an application identifier:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

   ```
   fortifyclient -url <ssc_url> -user <Username> -password <password> downloadFPR -file <FPRname> -applicationVersionID <id>
   ```

   where

   | `<ssc_url>` | represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 300) |
   | `<Username>` | represents the user name for a Developer-level (or higher) Software Security Center account with access to the application version that contains the FPR file |
   | `<password>` | represents the password for the Developer-level (or higher) Software Security Center account with access to the application version that contains the FPR file |
   | `<FPRname>` | represents the full path and name of the FPR file with its extension |
   | `<id>` | represents the Fortify Software Security Center application version identifier |

For more information about how to acquire Fortify Software Security Center application identifiers, see "Listing Application Versions" on page 303.

Downloading an FPR Using an Application Name and Version

To download an FPR into a Fortify Software Security Center application version using the application name and version:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

   ```
   fortifyclient -url <ssc_url> -user <username> -password <password> downloadFPR -file <fpr_name> -project <app_name> -version <app_version>
   ```

   where
Importing Content Bundles

As part of its ongoing support for Fortify Software Security Center, Fortify periodically provides content bundles (.zip filename extension) that contain one or more issue templates or report definitions.

**Note:** Fortify Software Security Center does not support the use of authentication tokens to import content bundles.

To import a content bundle into Fortify Software Security Center:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

```
fortifyclient -url `<ssc_url>` -user `<username>` -password `<password>`
import -bundle `<bundle_name>`
```

where

| `<ssc_url>` | represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 300) |
| `<username>` | represents the user name for a Developer-level (or higher) Fortify Software Security Center account with access to the application version that contains the fpr file |
| `<password>` | represents the password for the Developer-level (or higher) Fortify Software Security Center account with access to the application version that contains the fpr file |
| `<fpr_name>` | represents the full path and name of the FPR file with its extension |
| `<app_name>` | represents the Fortify Software Security Center application name |
| `<app_version>` | represents the Fortify Software Security Center application version that corresponds to the named application |
Downloading Audit Attachment Files

To download an audit attachment file:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

   ```
   fortifyclient -url <ssc_url> downloadAttachment -file <destination_file>
   -attachmentId <Attachment_Id>
   ```

   where

<table>
<thead>
<tr>
<th><code>&lt;ssc_url&gt;</code></th>
<th>represents the URL of the Fortify Software Security Center instance (see &quot;About Specifying the Fortify Software Security Center URL&quot; on page 300)</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;destination_file&gt;</code></td>
<td>represents the full path for the downloaded fpr file</td>
</tr>
<tr>
<td><code>&lt;Attachment_Id&gt;</code></td>
<td>represents the id of the attachment to download</td>
</tr>
</tbody>
</table>

About Archiving and Restoring Runtime Events

You can use the `fortifyclient` command-line utility to archive and restore Fortify Runtime Application Protection events. The legacy Fortify Software Security Center user interface includes a `Runtime` tab, which provides access to Runtime Console tools and features that you can use to manage one or more instances of Fortify Runtime Application Protection running in Federated mode. The `fortifyclient` utility includes a set of features to support the Runtime Console.

**Note:** For information about the `Runtime` tab, see the *HPE Security Fortify Runtime Application* User Guide.
Protection Operator Guide.

Topics covered in this section:

- Archived Runtime Events .................................................. 309
- Listing Runtime Applications ............................................... 309
- Archiving Runtime Events .................................................. 310
- About Restored Runtime Events ......................................... 311
- Restoring Runtime Events .................................................. 311
- Listing Runtime Archives .................................................. 311
- Uploading a Source Archive to an Application Version ............... 312
- Downloading Runtime Event Archive Files ............................ 313

Archived Runtime Events

Fortify Software Security Center stores runtime event archives in its database. You can download stored archives for external storage or for data mining. Archived events are removed from Fortify Software Security Center charts and lists.

Listing Runtime Applications

The fortifyclient command-line utility returns a list of numeric runtime application IDs and names.

Before you can archive events for a given runtime application, you must use fortifyclient to obtain its numeric identifier.

To obtain a list of all runtime application identifiers:

1. Navigate to the <ssc_install_dir>/Tools/fortifyclient/bin directory.
2. Run the following:

   ```
   fortifyclient -url <ssc_url> -user <account_name> -password <password> listRuntimeApplications
   ```

   where

<table>
<thead>
<tr>
<th>&lt;ssc_url&gt;</th>
<th>represents the URL of the Fortify Software Security Center instance (see &quot;About Specifying the Fortify Software Security Center URL&quot; on page 300)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;account_name&gt;</td>
<td>represents the user name for a Manager, Security Lead, or Administrator account with access to the Fortify Software Security Center runtime application</td>
</tr>
</tbody>
</table>
Archiving Runtime Events

You can archive the events for a runtime application. This action stores the runtime events in zipped format in the Fortify Software Security Center database.

Before you can archive events for a given runtime application, you must use fortifyclient to obtain its numeric identifier. For more information, see "Listing Runtime Applications" on the previous page.

To archive the events for a runtime application:

1. Navigate to the <ssc_install_dir>/Tools/fortifyclient/bin directory.
2. Run the following:

   ```
   fortifyclient -url <ssc_url> -user <account_name> -password <password> 
   archiveRuntimeEvents -startDate <mmddyyyy> -endDate <mmddyyyy> 
   -runtimeApplicationIds <AppID1,AppID2,...>
   ```

where

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;password&gt;</td>
<td>represents the password that corresponds to the &lt;account_name&gt; specified for the Manager, Security Lead, or Administrator account that has access to the runtime application</td>
</tr>
<tr>
<td>&lt;ssc_url&gt;</td>
<td>represents the URL of the Fortify Software Security Center instance (see &quot;About Specifying the Fortify Software Security Center URL&quot; on page 300)</td>
</tr>
<tr>
<td>&lt;account_name&gt;</td>
<td>represents the user name for a Manager, Security Lead, or Administrator account that has access to the Fortify Software Security Center runtime application</td>
</tr>
<tr>
<td>&lt;password&gt;</td>
<td>represents the password that corresponds to the &lt;account_name&gt; specified for the Manager, Security Lead, or Administrator account with access to the runtime application</td>
</tr>
<tr>
<td>&lt;mmddyyyy&gt;</td>
<td>represents the date of the first and last runtime events to include in the archive</td>
</tr>
<tr>
<td>&lt;AppID1,AppID2,....&gt;</td>
<td>represents the numeric identifiers of the runtime applications to archive</td>
</tr>
</tbody>
</table>
About Restored Runtime Events

Fortify Software Security Center reassigns all restored events to Runtime applications on the basis of the Runtime Console’s current set of application assignment rules.

For information about Runtime Console application assignment rules, see the HPE Security Fortify Runtime Application Protection: Java Designer Guide.

Restoring Runtime Events

To restore an archived set of runtime events:

1. Navigate to the <ssc_install_dir>/Tools/fortifyclient/bin directory.
2. Run the following:

   ```bash
   fortifyclient -url <ssc_url> -user <account_name> -password <password> restoreRuntimeEventArchive -archiveId <archiveID1,archiveID2,...>
   ```

   where

   - `<ssc_url>` represents the URL of the Fortify Software Security Center instance (see "About Specifying the Fortify Software Security Center URL" on page 300)
   - `<account_name>` represents the name associated with the Manager, Security Lead, or Administrator account that has access to the Fortify Software Security Center runtime application
   - `<password>` represents the password that corresponds to the specified `<account_name>`
   - `<archiveID1,archiveID2,...>` represents the numeric identifiers of one or more runtime archives to restore

Listing Runtime Archives

The `fortifyclient` command-line utility returns a list of numeric archive IDs, runtime application names, start dates, end dates, and restored status values (true or false).

To use `fortifyclient` to list the runtime event archives contained in the Fortify Software Security Center database:
1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

```sh
fortifyclient -url <ssc_url> -user <account_name> -password <password> listRuntimeEventArchives
```

where

<table>
<thead>
<tr>
<th><strong>&lt;ssc_url&gt;</strong></th>
<th>represents the URL of the Fortify Software Security Center instance (see &quot;About Specifying the Fortify Software Security Center URL&quot; on page 300)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>&lt;account_name&gt;</strong></td>
<td>represents the name of the Manager, Security Lead, or Administrator account that has access to the Fortify Software Security Center runtime application</td>
</tr>
<tr>
<td><strong>&lt;password&gt;</strong></td>
<td>represents the password that corresponds to the specified <code>&lt;account_name&gt;</code></td>
</tr>
</tbody>
</table>

### Uploading a Source Archive to an Application Version

To upload a source archive to an application:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin` directory.
2. Run the following:

```sh
fortifyclient -url <ssc_url> uploadSource -file <source_file_name> -application <app_name> -version <app_version> -user <ssc_user> -password <password>
```

where

<table>
<thead>
<tr>
<th><strong>&lt;ssc_url&gt;</strong></th>
<th>represents the URL for the Fortify Software Security Center instance (see &quot;About Specifying the Fortify Software Security Center URL&quot; on page 300)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>&lt;source_file_name&gt;</strong></td>
<td>represents the name of the source file to upload</td>
</tr>
<tr>
<td><strong>&lt;app_name&gt;</strong></td>
<td>represents the application name</td>
</tr>
<tr>
<td><strong>&lt;app_version&gt;</strong></td>
<td>represents the application version that corresponds to the named application</td>
</tr>
</tbody>
</table>
Downloading Runtime Event Archive Files

Follow the instructions in this topic to download a zipped runtime event archive file. You can extract the file to see the events that it contains.

To download a runtime event archive file:

1. Navigate to the `<ssc_install_dir>/Tools/fortifyclient/bin directory.
2. Run the following:

   ```
   fortifyclient -url <ssc_url> -user <account_name> -password <password> 
   downloadRuntimeEventArchive -file <destination_file> -archiveId <archive_ID>
   ```

where

<table>
<thead>
<tr>
<th><code>&lt;ssc_url&gt;</code></th>
<th>represents the URL of the Fortify Software Security Center instance (see &quot;About Specifying the Fortify Software Security Center URL&quot; on page 300)</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;account_name&gt;</code></td>
<td>represents the name associated with the Manager, Security Lead, or Administrator account that has access to the Fortify Software Security Center runtime application</td>
</tr>
<tr>
<td><code>&lt;password&gt;</code></td>
<td>represents the password that corresponds to the specified <code>&lt;account_name&gt;</code></td>
</tr>
<tr>
<td><code>&lt;destination_file&gt;</code></td>
<td>represents the full path for the downloaded RTA file</td>
</tr>
<tr>
<td><code>&lt;archive_ID&gt;</code></td>
<td>represents the id of the event archive file</td>
</tr>
</tbody>
</table>
Appendix C: Authoring Bug Tracker Plugins

Fortify Software Security Center supports integration with external bug tracking systems. This integration allows Fortify Software Security Center users to log bugs for issues as they audit them in Fortify Software Security Center. As delivered, the system can integrate with JIRA, Bugzilla, ALM, and TFS/VSTS. (For specific versions supported, see the HPE Security Fortify Software System Requirements document.) If your company uses a different bug tracker system, you can author a new plugin for it. This section provides information about how to author and deploy a new bug tracker plugin.

Note: In this guide and in the Fortify Software Security Center user interface, the terms bug and defect are used interchangeably.

Important! Fortify strongly recommends that you inspect the delivered plugin samples before you author your own plugin. You can find the samples in the following directory:

<ssc_install_dir>/Samples/<BugTrackerPlugin_Name>

This section contains the following topics:

Use Case ................................................................. 314
Application Setup ..................................................... 315
Implementation ....................................................... 315
Plugin Methods and Method Calls ................................. 316
Plugin Helper .......................................................... 319
Error Handling ......................................................... 319
Almost Stateless ....................................................... 319
Debugging a Bug Tracker Plugin ................................. 320
Deploying a Customized Bug Tracker Plugin .................. 320

Use Case

As the Fortify Software Security Center administrator, you can configure an external bug tracking system to use with a given application version, as described in "About Bug Tracker Integration" on page 127. Fortify Software Security Center displays the required configuration parameter fields for the bug tracker you select, and you set the values for these just one time for the application version. After you test the bug tracker configuration parameter values for validity (optional), you save them to the database for use whenever a user logs a defect for the application version.
A user who submits a bug against an application version logs on to the bug tracker, and then completes the required fields that the bug tracker supplies for the bug parameters. Required parameter information can include such items as summary, description, severity level, component, and so on.

The plugin framework supports a dynamic aspect to bug-tracking parameters. Whenever a user changes a parameter value, the plugin detects the change and an updated list of bug parameters with new list selections becomes available.

When a bug is filed, the bug ID is saved in the database against the issue. The user can then navigate to the bug using an external bug link, which the plugin supplies.

The credentials accepted from the user filing the bug are saved in the server session, and are reused for bugs subsequently submitted against the application during the same session.

**Application Setup**

The bug tracker plugin can be an independent application that you can write using your preferred IDE.

Configure a bug tracker plugin with the following dependencies:

- fortify-public-17.20.jar (required)
- Apache Commons Logging (optional)
- Apache Commons Lang (optional)

You can use your preferred build system to build your application distributable.

**Implementation**

All plugins must implement the `com.fortify.pub.bugtracker.plugin.BugTrackerPlugin` interface. Fortify strongly recommends that your implementation class extend `com.fortify.pub.bugtracker.plugin.AbstractBugTrackerPlugin` so that you can take advantage of any backward-compatibility support that becomes available in future releases. Also, you must annotate the implementation class with `@BugTrackerPluginImplementation`.

The BugTracker plugin interface is as follows:

```java
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,
```
Plugin Methods and Method Calls

The following table lists the methods and calls to use with your plugin.

<table>
<thead>
<tr>
<th>Method or Call</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>requiresAuthentication</td>
<td>This method is expected to return <code>true</code> if it requires the framework to request credentials from the user for any bug-tracking operation. This almost always returns <code>true</code>, except in cases where the plugin gets its credentials using a different mechanism, perhaps from the credential store or if the plugin interacts with the bug-tracking system asynchronously and not in real time. If the method returns <code>false</code>, the system passes null for all the UserAuthenticationStore parameters of the plugin methods.</td>
</tr>
<tr>
<td>getConfiguration</td>
<td>The plugin framework uses the <code>getConfiguration</code> method to get metadata about the questions to be presented to the user during plugin configuration. The return value is a list of BugTrackerConfig objects that provide required information about the configuration item. Each item corresponds to a text box in the user interface. The value field of each item is used to specify the default value for the text box.</td>
</tr>
<tr>
<td>setConfiguration (call)</td>
<td>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.</td>
</tr>
<tr>
<td>testConfiguration (call)</td>
<td>The plugin framework uses the <code>testConfiguration</code> call to test the configuration previously set using the <code>setConfiguration</code> call. This</td>
</tr>
</tbody>
</table>
**Method or Call** | **Description**
--- | ---
| | 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.

**getShortDisplay** | **getShortDisplay** method is used to return a short display name for the plugin. This string is used to populate the list of available bug tracker plugins. **Important:** If you customize the sample bug-trackers code that Fortify Software Security Center provides, but you use the same plugin classname, do not change the short display name of the plugin. (For consistency, also avoid changing the long display name.) If you do change the name of the main implementation class, then you must also change the display name(s) for the plugin.

**getLongDisplay** | **getLongDisplay** method is used to return a value that includes additional identification of the bug tracking system obtained from the configuration. This method is used, for example, when the user is prompted to provide credentials for a bug-tracking system. **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 do change the name of the main implementation class, then you must also change the display name(s) for the plugin.

**getBugParameters** | **getBugParameters** method returns metadata about the bug parameters to present to users. Fortify Software Security Center supports the following three bug parameter types:

- **BugParamText** translates to a text box.
- **BugParamTextArea** translates to a multiple-line text box and is typically used for bug descriptions.
- **BugParamChoice** translates to a list.
- **The issueDetail** object encompasses the details of the issue for which the user is attempting to log a bug. This defaults to various bug parameters such as the description and summary, which can be extracted from this object. The pluginHelper protected member has a
<table>
<thead>
<tr>
<th>Method or Call</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>helper method</strong> to build a suggested default bug description. (See “Plugin Helper” on the next page.)</td>
<td></td>
</tr>
<tr>
<td><strong>onParameterChange</strong></td>
<td>The plugin framework calls the onParameterChange method whenever the value for a bug parameter marked as hasDependentParams (see BugParamChoice class javadoc) changes. This method can take action and return a new list of bug parameters to display.</td>
</tr>
<tr>
<td></td>
<td>Keep the following guidelines in mind:</td>
</tr>
<tr>
<td></td>
<td>• Act on each bug parameter that has dependent parameters</td>
</tr>
<tr>
<td></td>
<td>• Do not forget handling case when parameter value changes to null (no selection made)</td>
</tr>
<tr>
<td></td>
<td>• Do not forget to set the parameter value in a return list to null when its selections change</td>
</tr>
<tr>
<td></td>
<td>• Before you add a new parameter, check the return list to make sure that it does not already include the parameter</td>
</tr>
<tr>
<td></td>
<td>• Return null if there is no change</td>
</tr>
<tr>
<td></td>
<td>• Use one of the following strategies:</td>
</tr>
<tr>
<td></td>
<td>• Modify the currentValues parameter and return it</td>
</tr>
<tr>
<td></td>
<td>• Construct the return value from raw parameters maintained. Set values and choice lists before returning.</td>
</tr>
<tr>
<td><strong>fileBug</strong></td>
<td>This method files a bug on the external bug-tracking system. The BugSubmission object passed encompasses all bug details.</td>
</tr>
<tr>
<td></td>
<td>Make sure that you correctly differentiate between the bug.getIssueDetail() object and the bug.getParams() object. The bug.getIssueDetail() object returns details of the issue, whereas the bug.getParams() object returns the bug parameter values that the user provides.</td>
</tr>
<tr>
<td></td>
<td>If you added Bug Description as a user-editable bug parameter, then fetch the bug description from the bug.getParams() object instead of from the bug.getIssueDetail() object. The return value of the fileBug object must be a bugId, which can be used to fetch the bug with the fetchBug method and formulate the deep link with the getBugDeepLink method.</td>
</tr>
<tr>
<td></td>
<td>Use fields in BugSubmission.getIssueDetail(), namely</td>
</tr>
</tbody>
</table>
### User Guide

**Appendix C: Authoring Bug Tracker Plugins**

<table>
<thead>
<tr>
<th>Method or Call</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>getLastBuildWithoutIssue(), getDetectedInBuild(), and getFileName()</td>
<td>To perform changeset discovery if you have access to your repository.</td>
</tr>
<tr>
<td>fetchBug</td>
<td>This method is used to fetch the current bug status.</td>
</tr>
<tr>
<td>getBugDeepLink</td>
<td>This method is used to formulate a deep link to the bug. If the bug tracker does not support a deep link, return null.</td>
</tr>
</tbody>
</table>

For a detailed explanation of each parameter and other supporting classes, see the public API javadoc.

## Plugin Helper

If your bug tracker plugin class extended from the class `AbstractBugTrackerPlugin` provided, you will find a protected member `BugTrackerPluginHelper` available. This helper object can be used to perform frequently used plugin operations for locating parameters, loading default values, and so on. Please consult the javadoc for more details. Also look at its usage in the plugin samples.

## Error Handling

For proper error handling and reporting, use the following strategy across all plugin methods to throw exceptions:

- **Throw** `com.fortify.pub.bugtracker.support.BugTrackerException` **for any error that the user can act on.** Example invalid configuration, errors arising from bug tracking system, bug tracking system failing, and so on. The error message with this exception is relayed back to the user and is expected to be user friendly.
- **Throw** `com.fortify.pub.bugtracker.support.BugTrackerAuthenticationException` **if and only if credentials provided to the bug tracking system are incorrect.** This exception results in cached bug tracker credentials being cleared.
- **Throw** `RuntimeException` or its subclasses **for internal exceptions.**

## Almost Stateless

With every top-level request that Fortify Software Security Center sends to the plugin framework bug tracker (and that needs to communicate with the bug tracker provider), the `setConfiguration` call is made. The only states that should be saved within the plugin are the configuration values that this method provides. The configuration values can be used during bug tracker plugin internal processing. From this point on, all plugin calls are expected to be stateless.
Plugin instances must not maintain any state, leave open connections, or try to use connections opened in the previous call. Software Security Center does not cache or reuse plugin instances across plugin operations. New states must be opened on each call and cleaned up before method exit.

**Debugging a Bug Tracker Plugin**

Apache Commons logging is supported in plugins. The resulting logs are appended into the file `plugin-framework.log` located in the `<fortify.home>/<appcontext>/plugin-framework/logs` directory. All exceptions are automatically logged. You can also perform remote debugging of your plugin by connecting to your application server from the plugin project within your IDE.

**Deploying a Customized Bug Tracker Plugin**

To deploy a customized bug tracker plugin, build a JAR that contains the plugin classes and any of its dependent classes.

The following is an example of a script used to build a bug tracker plugin with Gradle:

```
apply plugin: 'java'
sourceCompatibility = '1.7'
targetCompatibility = '1.7'
dependencies {
    compile fileTree(dir: 'lib', include: '*.jar')
}
jar.enabled = false // There is no need to generate a default non-osgi jar during build.
clean {
    delete "${projectDir}/dist"
}
task pluginJar(type: Jar) {
    baseName "com.fortify.BugTrackerPluginAlm"
    from sourceSets.main.output
    destinationDir = file("${projectDir}/dist")
    manifest {
        from "${projectDir}/META-INF/MANIFEST.MF"
    }
```

from(projectDir) {
    include "plugin.properties"
    include "plugin.xml"
}

into("lib") {
    from "${projectDir}/lib"
    include "*.jar"
    exclude "fortify-public*.jar"
}

build.dependsOn(pluginJar)

**Important:** If you customize the sample bug-trackers code that Fortify Software Security Center provides, but you use the same plugin classname, do not change the short display name of the plugin. It is used for the name of the bugfield template group. (For consistency, also avoid changing the long display name.) If you do change the name of the main implementation class, then you must also change the display name(s) for the plugin.

For information about how to build a library that includes all bug tracker plugin dependencies, see the `<ssc_install_dir>/Samples/<bugtracker>/README` file.

**See Also**

"Authoring Bug Tracker Plugins" on page 314
Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

**Feedback on User Guide (HPE Security Fortify Software Security Center 17.20)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to FortifyDocTeam@hpe.com.

We appreciate your feedback!