Legal Notices

Warranty

The only warranties for HP 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. HP 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. Valid license from HP 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 2009 - 2015 Hewlett-Packard Development Company, L.P.

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://protect724.hp.com/welcome

You will receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Part Number: 1-16b3-2015-04-430-01
Contents

Preface ................................................................................................................................................................. vi

Contacting Fortify Software .......................................................................................................................... vi

For More Information ...................................................................................................................................... vi

About the HP Fortify Software Security Center Documentation Set .......................................................... vi

Change Log ........................................................................................................................................................ vii

HP Fortify Plugin for Eclipse .......................................................................................................................... 8

About the HP Fortify Plugin for Eclipse ........................................................................................................ 8

Installing the HP Fortify Plugin for Eclipse Locally ....................................................................................... 8

Installing the Eclipse Plugin from an Update Site .......................................................................................... 11

Posting the Eclipse Plugin to an Internal Update Site .................................................................................. 11

Installing the Eclipse Plugin from an Update Site .......................................................................................... 11

About Re-Installing After Upgrading the Static Code Analyzer Suite from Audit Workbench ................. 12

About Uninstalling the Eclipse Plugin ........................................................................................................... 13

Uninstalling the Eclipse Plugin from the Eclipse User Interface ................................................................ 13

Uninstalling the Eclipse Plugin from the Command Line ............................................................................. 13

About Source Code Scanning ......................................................................................................................... 14

About Scan and Analysis Settings ................................................................................................................. 14

Configuring Analysis Settings ....................................................................................................................... 14

Configuring Advanced Scan Options ........................................................................................................... 15

Running Scans in Quick Scan Mode ............................................................................................................. 15

Enabling FindBugs During Scans .................................................................................................................. 15

Specifying Additional SCA Arguments ......................................................................................................... 15

About the Scan Results File Name and Directory .......................................................................................... 16

About Specifying Resources to Scan ............................................................................................................ 17

Viewing the Resources and Classpath to be Scanned ................................................................................. 17

Scanning Projects ........................................................................................................................................... 17

Scanning Individual Files and Packages ...................................................................................................... 17

About Re-Scanning Source Code ................................................................................................................... 18

About Viewing Scan Results ......................................................................................................................... 19

Viewing Summary Graph Information ......................................................................................................... 19

About the SCA Analysis Results View ......................................................................................................... 22

About Filter Sets ............................................................................................................................................ 22

Selecting the Filter Set for New Projects ....................................................................................................... 22

About the Folders Tabs ................................................................................................................................... 23

About the Analysis Tabs .................................................................................................................................. 24

Opening the Project Summary View ............................................................................................................. 25
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Security Content</td>
<td>57</td>
</tr>
<tr>
<td>About the Source Code View</td>
<td>26</td>
</tr>
<tr>
<td>About the Issue Auditing Panel</td>
<td>26</td>
</tr>
<tr>
<td>About Auditing Analysis Results</td>
<td>28</td>
</tr>
<tr>
<td>Opening an Existing Audit</td>
<td>29</td>
</tr>
<tr>
<td>Obtaining New Results</td>
<td>29</td>
</tr>
<tr>
<td>Viewing Analysis Evidence</td>
<td>29</td>
</tr>
<tr>
<td>About Searching Issues</td>
<td>29</td>
</tr>
<tr>
<td>Performing Simple Searches</td>
<td>33</td>
</tr>
<tr>
<td>Performing Advanced Searches</td>
<td>34</td>
</tr>
<tr>
<td>About Working with Issues</td>
<td>35</td>
</tr>
<tr>
<td>Grouping Issues</td>
<td>35</td>
</tr>
<tr>
<td>Evaluating Issues</td>
<td>36</td>
</tr>
<tr>
<td>Creating Issues</td>
<td>37</td>
</tr>
<tr>
<td>Suppressing Issues</td>
<td>37</td>
</tr>
<tr>
<td>Customizing the SCA Analysis Results View</td>
<td>38</td>
</tr>
<tr>
<td>Submitting an Issue as a Bug</td>
<td>39</td>
</tr>
<tr>
<td>About HP Fortify Reports</td>
<td>40</td>
</tr>
<tr>
<td>Opening HP Fortify Report Templates</td>
<td>40</td>
</tr>
<tr>
<td>Generating Reports</td>
<td>40</td>
</tr>
<tr>
<td>About HP Fortify Report Templates</td>
<td>41</td>
</tr>
<tr>
<td>Saving Report Templates</td>
<td>43</td>
</tr>
<tr>
<td>Synchronizing with Software Security Center</td>
<td>46</td>
</tr>
<tr>
<td>Scheduling Synchronization</td>
<td>46</td>
</tr>
<tr>
<td>Understanding Project Templates and Project Configuration</td>
<td>47</td>
</tr>
<tr>
<td>About Managing Folders</td>
<td>48</td>
</tr>
<tr>
<td>Configuring Custom Tags for Auditing</td>
<td>50</td>
</tr>
<tr>
<td>Setting the Default Filter Set</td>
<td>51</td>
</tr>
<tr>
<td>Creating a New Filter Set</td>
<td>51</td>
</tr>
<tr>
<td>Configuring Filters</td>
<td>51</td>
</tr>
<tr>
<td>Saving Project Templates</td>
<td>53</td>
</tr>
<tr>
<td>About Project Template Sharing</td>
<td>53</td>
</tr>
<tr>
<td>Working with Projects</td>
<td>54</td>
</tr>
<tr>
<td>Opening Projects</td>
<td>54</td>
</tr>
<tr>
<td>Merging Audit Data</td>
<td>56</td>
</tr>
<tr>
<td>Uploading Results to HP Fortify Software Security Center</td>
<td>56</td>
</tr>
<tr>
<td>About Security Results</td>
<td>57</td>
</tr>
<tr>
<td>Updating Security Content</td>
<td>57</td>
</tr>
<tr>
<td>Configuring Security Content Updates</td>
<td>58</td>
</tr>
<tr>
<td>About Advanced Configuration</td>
<td>59</td>
</tr>
<tr>
<td>Using the Audit Guide in Advanced Mode</td>
<td>59</td>
</tr>
<tr>
<td>About Bug Tracking System Integration</td>
<td>60</td>
</tr>
</tbody>
</table>
About Troubleshooting Problems with the Eclipse Plugin .................................................. 61
Resolving the Java.lang.OutOfMemory Message ................................................................. 61
Resolving Scan Failures Due to Insufficient Memory ......................................................... 61
Using the Debugging Option ......................................................................................... 61
Preface

Contacting Fortify Software
If you have questions or comments about using this product, contact HP 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@hp.com

To Call Support
650.735.2215

For More Information
For more information about HP Enterprise Security Products:
http://www.hpenterprisesecurity.com

About the HP Fortify Software Security Center Documentation Set
The HP Fortify Software Security Center documentation set contains installation, user, and deployment guides for all HP Fortify Software Security Center 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 HP ESP user community Protect724 website:

https://protect724.hp.com/welcome
You will need to register for an account.
## Change Log

The following table lists changes made to this document.

<table>
<thead>
<tr>
<th>Software Release-Version</th>
<th>Change</th>
</tr>
</thead>
</table>
| 4.30-01                  | • Removed the *About the Security Scope Details Tab* section.  
                          | • Modified the following sections based on changes to the user interface:  
                          |   • *About the Issue Auditing Panel* on page 26 |
| 4.21-01                  | Added information about the new Quick View filter set to *About Filter Sets* on page 22. |
| 4.10-01                  | • Added this Change Log section.  
                          | • Added the section *About Re-Installing After Upgrading the Static Code Analyzer Suite from Audit Workbench* on page 12.  
                          | • Added *Best Practices*: on page 14.  
                          | • Added the following sections:  
                          |   • *About the Scan Results File Name and Directory* on page 16  
                          |   • *Changing the Default Location and FPR File Name for all Projects* on page 16  
                          |   • *Changing the Default Location and FPR File Name for Specific Projects* on page 16  
                          | • Added the following sections:  
                          |   • *About Re-Scanning Source Code* on page 18  
                          |   • *Enabling the Merging of Scan Results as the Default for all Projects* on page 18  
                          |   • *Preventing the Plugin from Merging Scan Results for a Given Project* on page 18  
                          | • Added a link for the Protect724 website to the Preface. |
HP Fortify Plugin for Eclipse

The following topics provide information about how to install and use the HP Fortify Plugin for Eclipse (Eclipse Plugin).

About the HP Fortify Plugin for Eclipse

The Eclipse Plugin consists of three separate components: an audit plugin component, an analysis plugin component, and a collaboration component. The audit plugin component enables you to open existing scan results and audit them. The analysis plugin component enables you to initiate a Static Code Analyzer (SCA) scan and analysis, view the results, and fix the code associated with uncovered issues, all within the Eclipse IDE. The collaboration component includes server-related functionality such as connecting to Software Security Center (SSC), uploading results to SSC, and performing collaborative audits. (If you do not want that functionality, then there is no need to install the collaboration plugin.)

The audit plugin component displays the SCA scan results within the Eclipse IDE. These results include detailed descriptions of the security vulnerabilities detected and recommended remediation strategies. The audit plugin component helps security code inspection by enabling you to easily navigate to the source code location associated with each vulnerability, and then prioritize and audit the results.

The analysis plugin component locates potential security issues in your Java code using SCA and HP Fortify Security Content for Java and J2EE so that you can then fix the source code that contains the issues.

You can either install the Eclipse Plugin from an update site (see Installing the Eclipse Plugin from an Update Site on page 11), or you can install it locally (see Installing the HP Fortify Plugin for Eclipse Locally on page 8).

Note: For information about supported versions of Eclipse and Eclipse-based IDE versions, see the HP Fortify Software Security Center System Requirements document.

Installing the HP Fortify Plugin for Eclipse Locally

To install the Eclipse Plugin, you must have Eclipse Java Development Tools (JDT) installed. You can get JDT from the main Eclipse update site. To do this, select the Contact all update sites during install to find required software check box during your Eclipse installation.

Notes:

- To update from an earlier Eclipse Plugin version, you must first remove the existing version. For information about how to uninstall the plugin, see About Uninstalling the Eclipse Plugin on page 13.
- The following procedure is based on the assumption that you selected the Eclipse Plugin during your SCA installation.

To install the Eclipse Plugin locally:

1. Start Eclipse.
2. Select Help → Install New Software.
3. Click **Add**.

The Add Repository dialog box opens.

4. To create a local update site on your file system (as opposed to one on the Internet):
   a. In the **Name** box, type a name for the local update site.
   b. Click **Local**, and then browse to the `<Fortify_Install>/plugins/eclipse` directory. (Make sure that you point to the directory itself, and not the `site.xml` file).

In the Install window, the **Work with** list displays the name and location of your local update site and the **Fortify Eclipse Plugins** node is listed as available software.
5. Expand the **Fortify Eclipse Plugins** node, and then select the **Fortify Eclipse Plugins** check box.

6. Click **Next**.
   
   The **Install Details** step lists the plugins you selected.

7. To display version and copyright information for a plugin in the **Details** box, click the plugin name.

8. On the **Review Licenses** step, review and accept the terms of the HP Fortify license agreement.

9. Click **Finish**.
   
   During installation, Eclipse displays a warning that the software contains unsigned content.

10. Click **OK**.

11. To complete the installation, click **Restart Now** when prompted.

After Eclipse restarts, the menu bar includes the **HP Fortify** menu and the Eclipse toolbar displays the Fortify icon.

![Installation Screenshot]
Installing the Eclipse Plugin from an Update Site

An alternative to requiring every developer to install HP Fortify plugins locally is to post the plugins to an internal update site that can serve as a single distribution point. The only requirement is that you have an internal web server.

Posting the Eclipse Plugin to an Internal Update Site

To post the plugin for access by other users:

1. Copy the contents of `<Fortify_Install>/plugins/eclipse` directory on to your web server.
2. Provide the URL for the update site to the appropriate users.

**Note:** If you are using an Eclipse installation such as Eclipse for C/C++ Developers, which does not include the Eclipse Java Development Toolkit (JDT), you can bundle the JDT with the HP Fortify plugins on your update site so that it is installed automatically. For help with this, contact HP Fortify Support (see Contacting Fortify Software on page vi).

Installing the Eclipse Plugin from an Update Site

To install the Eclipse Plugin after it has been posted to an update site:

1. Obtain the URL of the plugin update site.
2. Select Help → Install New Software.
3. Click Add.
4. In the Name box, type a name for the update site.
5. In the Location box, type the URL of the update site.
6. Click OK
   In the Install window, the Work with list displays the update site you specified and the Fortify Eclipse Plugins node is listed as available software.
7. Expand the Fortify Eclipse Plugins node, select the Plugins check box, and then select the check box or check boxes for the plugins you want to install.

**Note:** If you select the audit or analysis plugin component, do not select the Fortify Remediation Plugin for Eclipse check box. For information about the HP Fortify Remediation Plugin for Eclipse, see the HP Fortify Remediation Plugin for Eclipse Installation and Usage Guide.
8. Click **Next**.

   The **Install Details** step lists the plugins you selected.

9. To display version and copyright information about the plugin in the **Details** box, click the plugin name.

10. On the **Review Licenses** step, review and accept the terms of the HP Fortify license agreement.

11. Click **Finish**.

   During installation, Eclipse displays a warning that the software contains unsigned content.

12. Click **OK**.

13. To complete the installation, click **Restart Now** when prompted.

After Eclipse restarts, the menu bar includes the **HP Fortify** menu and the Eclipse toolbar displays the Fortify icon.

### About Re-Installing After Upgrading the Static Code Analyzer Suite from Audit Workbench

If you have upgraded your Static Code Analyzer suite from Audit Workbench, you must uninstall, and then reinstall the Eclipse Plugin. For information about how you can upgrade the Static Code Analyzer Suite from Audit Workbench, see the **HP Fortify Audit Workbench User Guide**.
About Uninstalling the Eclipse Plugin

You can uninstall the Eclipse Plugin from either the Eclipse user interface or from the command line.

Uninstalling the Eclipse Plugin from the Eclipse User Interface
To uninstall the Eclipse Plugin from the Eclipse user interface:

1. Start Eclipse.
2. Select Help → About Eclipse.
3. Click Installation Details.
   The Eclipse Installation Details window opens.
4. On the Installed Software tab, select Fortify Plugin for Eclipse.
5. Click Uninstall.
6. In the Uninstall window, click Finish.
7. To implement the change, click Restart Now.

The Eclipse menu bar no longer includes the HP Fortify menu and the Eclipse toolbar no longer contains the Fortify icon.

Uninstalling the Eclipse Plugin from the Command Line
To uninstall the Eclipse Plugin from the command line, run one of the following scripts:

- On a Windows system, run uninstall-fortify_plugins.cmd
- On a Linux or Macintosh system, run uninstall_fortify_plugins.sh

These scripts are located in the <install_root>/plugins/eclipse directory.
About Source Code Scanning

If you installed the analysis plugin component, you can initiate an SCA scan and analysis of your Java source code from Eclipse. The SCA scans are invoked from the Eclipse Plugin with the server Java Virtual Machine. During a scan, SCA cleans up old source code analysis files, rebuilds the solution, compiles JSP files, performs the security analysis, and then displays the results in Eclipse.

Best Practices:

- HP Fortify recommends that you periodically update the HP Fortify Security Content. For instructions, see About Security Content on page 57.
- To get the best results from your scans, before you scan your project source code, make sure that you can compile the project with no errors.

About Scan and Analysis Settings

You can customize your scan and analysis settings to suit your requirements. You also have the option of running scans in quick scan mode. The following sections provide instructions on how to configure your scans and how to use quick scan mode.

Configuring Analysis Settings

The source code analysis settings are available only if the analysis plugin is installed. The source code analysis settings enable you to configure different Rulepacks and amount of memory to use during the scan to control what SCA looks for during a scan.

To configure the analysis settings:

1. Select HP Fortify → Options.
   The HP Fortify Options dialog box opens.
2. Select Default Project Settings.
   The Analysis Configuration tab opens.
3. To specify the amount of memory to use for the scan (such as 500 MB), type an integer in the Memory (MB) box.
4. By default, SCA assumes that SQL files contain PL/SQL. To change this to T-SQL, from the SQL Type list, select TSQL.
5. To use specific security content to scan the project (instead of all security content), in the Security Content section, clear the Use All Installed Security Content check box, and then select the check boxes for the installed Fortify security content and any custom security content to use.
6. Click OK.
Configuring Advanced Scan Options

The following topics describe how to configure advanced scan options. These options are available only if the analysis plugin is installed.

Running Scans in Quick Scan Mode

You can use quick scan mode to quickly scan projects for major issues. A quick scan of the WebGoat sample application uncovers 284 possible issues. By contrast, a full scan of the WebGoat sample application uncovers 1,150 possible issues.

In quick scan mode, Static Code Analyzer uses the fortify-sca-quickscan.properties file (instead of the standard fortify-sca.properties file) to search for high-confidence, high-severity issues. Quick scans are a great way to get many applications through an assessment so that you can quickly find issues and begin remediation.

Keep in mind that, although the scan is significantly faster than a full scan, it does not provide as robust a result set. Critical and other issues that a quick scan cannot detect may exist in your application. HP Fortify recommends that you run full scans whenever possible.

To enable quick scan mode:
1. Select HP Fortify → Options.
2. In the left panel of the Options dialog box, select Default Project Settings.
3. In the right panel, select the Advanced Options tab.
4. In the Advanced Analysis Options section, select the Enable quick scan mode check box.
5. Click OK.

Enabling FindBugs During Scans

FindBugs (http://findbugs.sourceforge.net) is a static analysis tool that detects quality issues in Java code. You can run FindBugs with the Eclipse Plugin. The results are integrated into the analysis results file. Enabling -findbugs also adds the -java-build-dir parameter with a path to your compiled java classes. Unlike SCA, which runs on Java source files, FindBugs runs on Java byte code. Therefore, you must compile your project successfully before you run a scan with -findbugs enabled. Otherwise, the -findbugs option is ignored and SCA issues a warning to that effect.

To add the -findbugs option to the sourceanalyzer command to be run:
1. Select HP Fortify → Options.
2. In the left panel of the Options dialog box, select Default Project Settings.
3. In the right panel, select the Advanced Options tab.
4. In the Advanced Analysis Options section, select the Enable findbugs check box.
5. Click OK.

Specifying Additional SCA Arguments

To specify additional SCA arguments:
1. Select HP Fortify → Options.
   The HP Fortify Options dialog box opens.
2. Select Default Project Settings.
3. Click the Advanced Options tab.
4. Select **Use Additional SCA Arguments** and then enter command line options for either the translation or scan phase.

For example, if you include the `-verbose` command line argument, detailed status messages are sent to the console during the analysis.

For information about the available arguments and syntax format, see the *HP Fortify Static Code Analyzer User's Guide*.

5. Click **OK**.

### About the Scan Results File Name and Directory

By default, after you scan a project, the Eclipse plugin assigns the results file (FPR file) a name in the format `<Project_Name>Scan.fpr` and places it in a new project folder in your Eclipse working directory. You can, if you prefer, store your project scan results file under a different name and directory.

To change the default directory and FPR file name for all projects, use the HP Fortify Options dialog box. To change the default directory and FPR file name for a specific project, use the Eclipse Properties window.

#### Changing the Default Location and FPR File Name for all Projects

To specify a default FPR file name and directory for all projects:

1. Select **HP Fortify → Options**.
2. In the left panel of the Options dialog box, select **Default Project Settings**.
3. In the right panel, select the **Advanced Options** tab.
4. Select the **Use Additional SCA Arguments** check box.
5. Do one of the following:
   - In the **Output results to** box, type the absolute path for FPR files.
   - To specify a name and a static workspace folder for FPR files, click **Workspace**, and then, in the Folder Selection window, navigate to and select a workspace relative directory.
   - To specify a name and a static folder that is *not* part of your workspace, click **File System**, and then select a directory for FPR files.
   - To specify a name and a dynamic path that changes based on the project you are analyzing, click **Variables**, and then, in the Select Variable window, select core Eclipse variables to specify the relative path for FPR files.

#### Changing the Default Location and FPR File Name for Specific Projects

To specify a default FPR file name and directory for a specific project:

1. From the Java perspective in Eclipse, right-click a project name, and then select **Properties** from the shortcut menu.
   
   The **Properties for `<Project_Name>`** window opens.
2. In the left panel, select **Fortify Project Properties**.
3. In the right panel, select the **Enable Project Specific Settings** check box.
4. In the right panel, click the **Advanced Options** tab.
5. Select the **Use Additional SCA Arguments** check box.
6. Do one of the following:
   - In the **Output results to** box, type the absolute path for project FPR files.
   - To specify a name and a static workspace folder for project results, click **Workspace**, and then, in the Folder Selection window, navigate to and select a workspace relative directory.
To specify a name and a static folder that is not part of your workspace, click **File System**, and then select a directory for FPR files.

To specify a name and a dynamic path that changes based on the project you are analyzing, click **Variables**, and then, in the Select Variable window, select core Eclipse variables to specify the relative path for project FPR files.

**Note:** Initially, all variables are resolved to a real value for the selected project. You can still use variables, though, and view the resolved value in the **Scan Commandline Preview** box.

### About Specifying Resources to Scan

The Eclipse Plugin automatically includes all source files from dependent projects in scans of selected projects. For JAR files included in the project you select to scan, if the source exists in the workspace for a given JAR, the Eclipse Plugin includes the source in the scan.

### Viewing the Resources and Classpath to be Scanned

To see the project resources and classpath to be scanned if you select a project, and then select **HP Fortify → Analyze Project**:

1. From the Java view in Eclipse, do one of the following:
   - Right-click a project name, and then select **Advanced Scan** from the shortcut menu.
   - Select a project name, and then select **HP Fortify → Advanced Scan**.

   The Command Builder opens.

2. Expand the directory tree.

   The Command Builder displays the project resources and classpath to be scanned. If you have “Scan resources in dependent projects” enabled, you can see any dependent projects under the **Workspace Dependencies** root.

### Scanning Projects

The Eclipse Plugin automatically includes all source files from dependent projects in scans. Although you can scan individual packages and files (see **Scanning Individual Files and Packages**), SCA scan results are more accurate if you scan an entire project at once.

**Note:** The Eclipse plugin does not support scanning multiple projects at the same time.

To scan a project:

1. Open the project in the Java perspective in Eclipse.
2. In the **Package Explorer** view, select the project.
3. Do one of the following:
   - On the toolbar, click the **HP Fortify** icon.
   - Select **HP Fortify → Analyze Project**.

After the scan begins, a progress bar in the Scanning window enables you to follow the process. After the scan finishes, the results are loaded into and displayed in the Fortify Audit perspective in Eclipse.

### Scanning Individual Files and Packages

You can also scan individual files and packages.

**Note:** HP Fortify does not recommend this method, because analysis results are more accurate when an entire project is scanned at once.
To scan individual files or packages:

1. From Eclipse, open the project in the Java perspective.
2. In the Package Explorer view, right-click the file or package to scan, and then select Analyze Project Component from the shortcut menu.

**About Re-Scanning Source Code**

When you re-scan a project from Eclipse, the plugin does not automatically merge the results from the previous scan with the results from the new scan. However, if you want to see specifically what issues have been fixed and which issues were introduced since the earlier scan, you can configure the plugin to merge scan results.

**Enabling the Merging of Scan Results as the Default for all Projects**

To enable the Eclipse Plugin to merge the results of the next scan you run with results from the previous scan:

1. Select HP Fortify → Options.
2. In the left panel of the Options dialog box, select Default Project Settings.
3. In the right panel, click the Advanced Options tab.
4. In the Advanced Analysis Options section, select the Merge with previous scan check box.
5. Click OK.

*Note:* You can override this merging option for a given project by configuring project properties.

**Enabling the Merging of Scan Results on a Per-Scan Basis**

If you run an advanced scan, you can specify whether the results are merged with the previous scan results for the project.

To specify whether scan results are merged during an advanced scan:

1. From the Java perspective in Eclipse, select a project name.
2. Select HP Fortify → Advanced Scan.
   
   The Commandline Builder opens.
3. Select the Merge With Previous Scan check box.
4. Specify the rest of the advanced scan settings, and then click Scan.

**Preventing the Plugin from Merging Scan Results for a Given Project**

If you have enabled the merging of scan results as the default behavior, you can override merging for a given project.

To prevent the plugin from merging scan results for a specific project:

1. From the Java perspective in Eclipse, right-click a project name, and then select Properties from the shortcut menu.
   
   The Properties for <Project_Name> window opens.
2. In the left panel, select Fortify Project Properties.
3. In the right panel, select the Enable Project Specific Settings check box.
4. In the right panel, click the Advanced Options tab.
5. Clear the Merge with previous scan check box.
6. Click OK.
About Viewing Scan Results

After a scan is completed (or, after you open an existing audit project), summary results are displayed in the SCA Analysis Results section (top left) and in the Project Summary section (top center) of the Fortify Audit view.

Viewing Summary Graph Information

The summary graph displayed in the Project Summary section provides multiple perspectives on the sets of issues, grouped by priority (Critical, High, Medium, and Low) uncovered during a scan. You can drill down in the graph to see detailed information about each issue set, and create various bar charts for issues based on a selected issue attribute.

The following exercise uses the Webgoat sample Java application to demonstrate how to access information about sets of issues graphically depicted in the summary graph.

To access details about issue sets in an audit project:

1. Scan your project source code or open an existing audit project in Eclipse.

   After the results are loaded, the Project Summary view at the top center of the workspace displays the Summary tab, which includes the summary graph. The summary graph initially displays issues sorted into the Critical, High, Medium, and Low folders.

   Note: If you change the selection in the Filter Set list (issues panel), the summary graph changes accordingly.
2. To see a different view of the high priority issues, click the **High** bar.

![Project Summary](image)

By default, the graph displays high priority issues based on the analysis attribute (assigned analysis values).

**Note:** The example here shows information for scan results that have been partially audited. If these results were from a fresh, unaudited scan, no analysis information would be available. The graph would just display a single bar representing all (unaudited) high priority issues.

3. To view the high priority issues based on a different attribute, select an item from the **View By** list.

![Project Summary](image)
4. On the **Issues in High** bar graph, select a bar for a category that contains multiple issues.

In the example shown here, the **Null Dereference** bar is selected. You can see that of seven issues, three were marked as Suspicious and four were marked as Bad Practice.

5. To synchronize the issues list with the displayed graphical view, click **Synch Issue List with Graph**.

The issues list in the SCA Analysis Results section now reflects the selections in the summary graph.

6. To return to the previous view in the summary graph, click **Back**.
7. To return to the original summary graph view (issues based on priority), click **Return to Folder Graph**.

**About the SCA Analysis Results View**

The **SCA Analysis Results** view provides a way to group and select the issues to audit. This section provides information about each of the elements in this view.

**About Filter Sets**

The selected filter set controls which issues are listed in the **SCA Analysis Results** view. The filter set customizes the **SCA Analysis Results** view by determining the number and types of containers (folders) and how and where issues are displayed. The filter sets sort the issues by severity into the **Critical**, **High**, **Medium**, **Low**, and **All**, folders.

Because filter sets are saved to project files, each project can have unique filter sets. The plugin provides the following filter sets for new projects:

- **Quick View**: This is the default filter set for new projects. 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 is the default filter set for projects scanned in product versions earlier than 4.21. 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.

If you open the scan results for a project that you have previously worked on in a plugin version earlier than 4.21, you cannot see the Quick View filter set, but you might see the following deprecated filter sets:

- **Developer View**: Issues shown include a balance between results that detail all potential issues and a targeted set of possible vulnerabilities.

- **Critical Exposure**: Shows issues within categories that have been proven to be high priority issues across multiple industries and within a variety of environments; used to discover a limited set of well-known, critical security issues.

- **Hotspot**: Shows issues that are of particular interest to developers, such as high accuracy bugs.

If you open an FPR file that contains no custom **filtertemplate.xml** file or if you open an FVDL file or a **webinspect.xml** file, the project opens with the Quick View filter set selected.

**Selecting the Filter Set for New Projects**

You can change that initial filter set or turn if off completely so that the default (the filter set last enabled in the project template) is used to display scan results for new projects.

To select the filter set for new projects:

1. Select **HP Fortify → Options**.
2. In the left panel of the Options dialog box, select **Audit Features Config**.
3. On the right, leave the **Override default filter set on start with** check box selected.

If you clear the check box, the default filter is loaded. For newly-opened projects, the default filter for FPRs that have no embedded template or the default filter from the embedded template is the Security Auditor View filter set. For projects you have already opened in an Eclipse Plugin version earlier than 4.21, the default filter is the last filter set used for that project.
4. From the list to the right of the **Override default filter set on start with** check box, select the filter set to use to display scan results for new projects.

5. Click **OK**.

**About the Folders Tabs**

The color-coded **Critical**, **High**, **Medium**, **Low**, and **All** tabs on the **SCA Analysis Results** view are called “folders.” You can customize the folders and their settings. The number of folders, names, colors, and the issue list can vary between filter sets and projects.

Each folder contains a list of all of the issues with attributes that match the folder filter conditions. One folder in each filter set is the default folder, indicated by **(default)** in the folder name. If an issue matches none of the folder filters, it is listed in the default folder.

**Note:** To show or hide suppressed, hidden, and removed issues, set the user interface preferences from the Options dialog box (see **Customizing the SCA Analysis Results View** on page 38).

**About the Group By List**

The **Group By** list options sort the issues into sub folders. The option you select is applied to all visible folders. To list all issues in the folder without any grouping, select **<none>**.

To customize the existing groups, you can specify which attributes to sort by, add or remove the attributes to create sub-groupings, and add your own grouping options.

The Group By settings apply to the application instance. You can apply the **Group By** option to any project opened with that instance of the application.

**About the Search Box**

The search box enables you to limit the issues displayed in the folder and to search for specific issues. For detailed information about how to use the search box, see **About Searching Issues** on page 29.
About the Analysis Evidence View

When you select an issue, the Analysis Evidence view displays the evidence that the analyzer used to produce the file. This evidence is presented in sequential order. For dataflow issues, this evidence is a presentation of the path that the tainted data follows from the source function to the sink function.

For example, when you select an issue that is related to potentially tainted dataflow, the Analysis Evidence view shows the direction the dataflow is moving in this section of the source code.

The Analysis Evidence view uses the icons listed in Table 1 to show how the dataflow moves in this section of the source code or execution order:

Table 1: Analysis Evidence View Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>:=</td>
<td>Data are assigned to a field or variable</td>
</tr>
<tr>
<td>&lt;</td>
<td>Information is read from a source external to the code such as an html form or a url</td>
</tr>
<tr>
<td>☑</td>
<td>Data are assigned to a globally scoped field or variable</td>
</tr>
<tr>
<td>☑</td>
<td>A comparison is made</td>
</tr>
<tr>
<td>📍</td>
<td>The function call receives tainted data</td>
</tr>
<tr>
<td>📍</td>
<td>The function call returns tainted data</td>
</tr>
<tr>
<td>📍</td>
<td>Passthrough, tainted data passes from one parameter to another in a function call</td>
</tr>
<tr>
<td>📍</td>
<td>An alias is created for a memory location</td>
</tr>
<tr>
<td>📍</td>
<td>Data are read from a variable</td>
</tr>
<tr>
<td>📍</td>
<td>Data are read from a global variable</td>
</tr>
<tr>
<td>📍</td>
<td>Tainted data is returned from a function</td>
</tr>
<tr>
<td>&amp;</td>
<td>A pointer is created</td>
</tr>
<tr>
<td>*</td>
<td>A pointer is dereferenced</td>
</tr>
<tr>
<td>...</td>
<td>The scope of a variable ends</td>
</tr>
<tr>
<td>🜍</td>
<td>The execution jumps</td>
</tr>
<tr>
<td>🛑</td>
<td>A branch is taken in the codes execution</td>
</tr>
<tr>
<td>🛑</td>
<td>A branch is not taken in the codes execution</td>
</tr>
<tr>
<td>🌍</td>
<td>Generic</td>
</tr>
<tr>
<td>🕵️‍♀️</td>
<td>A runtime source, sink, or validation step</td>
</tr>
</tbody>
</table>

The Analysis Evidence view can display inductions. Inductions provide supporting evidence for their parent nodes. Inductions consist of a text node, displayed in italics as a child of the trace node, and an induction trace, displayed as a child of the text node (a box surrounds the induction trace). The italics and the box distinguish the induction from a standard sub trace.
Opening the Project Summary View

The **Project Summary** view displays detailed scan information on the tabs described in this section.

To open the **Project Summary** view:

1. Open an FPR file.
2. Select **HP Fortify → Show Project Summary**.

About the Summary Tab

The **Summary** tab shows high-level information about the project.

About the Certification Tab

The **Certification** tab displays the result certification status. Results certification is a check that the analysis has not been altered since it was produced by HP Fortify Static Code Analyzer or HP Fortify Runtime Application Protection.

About the Runtime Analysis Tab

If Runtime analysis data are available, the **Runtime Analysis** tab displays the following run information:

- Number of issues found by HP Fortify Runtime Application Protection
- Build ID
- Engine version
- Dates and times the run started and ended
- Machine on which the scan was run

About the Build Information Tab

The **Build Information** tab displays the following information:

- Build details such as the build ID, number of files scanned, source last modified date, and the date of the scan, which may be different than the date the files were translated
- List of files scanned, with file sizes and timestamps
- Libraries referenced for the scan

About the Analysis Information Tab

The **Analysis Information** tab shows the SCA version that performed the scan, details about the computer on which the scan was run, the user who started the scan, platform, scan date, machine name, and the time required to scan the code.

The **Analysis Information** tab includes the following subtabs:

- **Security Content**: Lists information about the Rulepacks used to scan the source code.
- **Properties**: Displays the SCA properties files settings
- **Commandline Arguments**: Displays the command-line options used to analyze the project
- **Warnings**: Lists any and all errors and warnings that occurred during the analysis. To view details about a listed warning, click the warning.
About the Source Code View

The source code view in the top middle section of the user interface shows the section of code related to the issue selected in the SCA Analysis Results view. Each time you select an issue in the SCA Analysis Results view, a tab opens in the source code view and displays the code associated with the selected issue.

If multiple nodes represent an issue in the Analysis Evidence view, the source code view shows the code associated with the selected node.

About the Issue Auditing Panel

The issue auditing panel at the bottom center of the user interface provides detailed information about each issue on the tabs described in the following topics:

Note: Select Options → Show View menu to show and hide tabs on the Issue Auditing panel.

About the Issue Summary Tab

The Issue Summary tab displays information about the selected issue and enables auditors to add comments and custom tag values. Table 2 lists the information displayed on the tab.

Table 2: Issue Summary Options

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue</td>
<td>Displays the issue location, including the filename and line number.</td>
</tr>
<tr>
<td>User</td>
<td>Displays the name of the user assigned to the issue if the results were uploaded to SSC and a user was assigned in SSC.</td>
</tr>
<tr>
<td>Analysis</td>
<td>List of values that the auditor can add to the issue as attributes. The auditor can select one of the following Analysis tag values:</td>
</tr>
<tr>
<td></td>
<td>Not an Issue</td>
</tr>
<tr>
<td></td>
<td>Reliability Issue</td>
</tr>
<tr>
<td></td>
<td>Bad Practice</td>
</tr>
<tr>
<td></td>
<td>Suspicious</td>
</tr>
<tr>
<td></td>
<td>Exploitable</td>
</tr>
<tr>
<td>Suppress</td>
<td>Suppresses the issue</td>
</tr>
<tr>
<td>File Bug</td>
<td>Provides access to a bug tracking system, such as Bugzilla or JIRA.</td>
</tr>
<tr>
<td>Comments</td>
<td>Appends additional information about the issue to the comment field.</td>
</tr>
<tr>
<td>Rule Information</td>
<td>Shows information, such as the category and kingdom, that describes the issue.</td>
</tr>
<tr>
<td>More Information</td>
<td>Opens the Issue Details tab.</td>
</tr>
<tr>
<td>Recommendations</td>
<td>Opens the Recommendations tab.</td>
</tr>
</tbody>
</table>
About the Issue Details Tab

The **Issue Details** tab provides a detailed description of the selected issue and guidelines on how to resolve it. Table 3 lists the elements of the **Issue Details** tab.

**Table 3: Issue Details Tab Elements**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract/Custom Abstract</td>
<td>Summary description of the issue, including custom abstracts defined by your organization.</td>
</tr>
<tr>
<td>Explanation/Custom Explanation</td>
<td>Description of the conditions in which this type of issue occurs. This includes a discussion of the vulnerability, the constructs typically associated with it, how it can be exploited, and the potential ramifications of an attack. This element also provides custom explanations defined by your organization.</td>
</tr>
<tr>
<td>Instance ID</td>
<td>Unique identifier for the issue.</td>
</tr>
<tr>
<td>Rule ID</td>
<td>Primary rule that found the issue.</td>
</tr>
<tr>
<td>SCA Confidence</td>
<td>Metric generated by SCA.</td>
</tr>
</tbody>
</table>

About the Security Scope Details Tab

The **Security Scope Details** tab displays the following information about runtime issues found using HP Fortify Runtime Application Protection:

**Arguments:** Shows the Index, Value and Return Value

**Request:** The HTTP Request information including the Method URL, content-length, accept-encoding, referer, connection, accept-language, host, accept-charset, user-agent, content-type, cookie, accept, keep-alive

**Stack Trace:** Shows the order of methods called during execution and line number information. Blue clickable code links are only displayed for code scanned by SCA.

About the Recommendations Tab

The **Recommendations** tab displays suggestions and examples of how to secure the vulnerability or remedy the bad practice. Table 4 lists the elements on the **Recommendations** tab.

**Table 4: Recommendations Tab Elements**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommendations/Custom Recommendations</td>
<td>Recommendations for this type of issue, including examples, as well as custom recommendations defined by your organization.</td>
</tr>
<tr>
<td>Tips/Custom Tips</td>
<td>Tips for this type of issue, including any custom tips defined by your organization.</td>
</tr>
<tr>
<td>References/Custom References</td>
<td>Reference information, including any custom reference defined by your organization.</td>
</tr>
</tbody>
</table>
About the History Tab

The **History** tab displays a complete list of auditing actions, including details such as the time and date, and the name of the user who modified the issue.

About the Diagram Tab

The **Diagram** tab displays a graphical representation of the node execution order, call depth, and expression type of the issue selected in the **Issues** panel.

The **Diagram** tab displays information that is relevant to the rule type. The execution order is represented along the vertical axis.

For dataflow issues, the trace starts at the top with the first function to call the taint source, then traces the calls to the source (blue node), and ends the trace at the sink (red node). In the diagram, the source (src) and sink nodes are also labeled. A red X on a vertical axis indicates that the function called finished executing.

The horizontal axis shows the call depth. A line shows the direction that control is passed. If control passes with tainted data traveling through a variable the line is red, and if it is without tainted data, the line is black.

The icons used for the expression type of each node in the diagram are the same icons used in the Analysis Evidence. To view the icons and the descriptions, see *About the Analysis Evidence View* on page 24.

About the Filters Tab

The **Filters** tab displays all the filters in the selected filter set. *Table 5* lists the **Filters** tab options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Filters | Displays a list of the visibility and folder filters configured in the selected filter set.  
  - Visibility filters show or hide issues  
  - Folder filters sort the issues into the folder tabs in the **SCA Analysis Results** view  
  Right-click a filter to show issues that match the filter or to enable, disable, copy, or delete it. |
| If | Displays the filters conditions.  
  The first list displays a list of issue attributes, the second list specifies how to match the attribute, and third is the value the filter matches. |
| Then | Indicates the filter type, where hide is a visibility filter and folder is a folder filter. |

About Auditing Analysis Results

The **HP Fortify Audit Perspective** displays four audit-focused views that are arranged for maximum efficiency. You can also open audit-related views in other perspectives, such as the Java perspective or C/C++ perspective, and rearrange the views. You might decide to use the audit views only, and stay within a customized development perspective.

The following topics provide information about how to audit your scan and analysis results.
Opening an Existing Audit

You can open a local, previously saved audit, and continue your work. Alternatively, you can open an audit that someone else performed on a different machine.

To open a local saved audit:
1. From Eclipse, open the Java or C/C++ perspective, and then open the audited project.
2. Right-click the project, and then select **Load Fortify Security Audit** from the shortcut menu.

To open an externally generated audit:
1. From Eclipse, open the Java or C/C++ perspective.
2. Select the audited project, and then select **HP Fortify → Load Saved Audit Project**.
3. In the **SCA Issues** panel, select the audit.

Obtaining New Results

This section covers how to obtain new results for an existing audit.

To obtain results for an existing audit:
1. From Eclipse, open the Java perspective.
2. In the **Package Explorer** view, right-click the project, and then select **Fortify Source Code Analysis** from the shortcut menu.
3. To view the results, go to the HP Fortify Audit perspective, or the individual SCA views.

Viewing Analysis Evidence

When you select an issue, the **Analysis Evidence** view displays the relevant trace output. This is a set of program points that show how the analyzer found the issue. For dataflow and control flow issues, the set is presented in the order executed.

For dataflow issues, additional icons show the direction of dataflow in this section of the source code:
- A left-pointing arrow indicates tainted data flowing out of a function.
- A right-pointing arrow indicates data flowing into the function.
- A double-pointed arrow indicates an intermediate assignment or pass-through function.

About Searching Issues

You can enter search terms in the text field below the issue tree. When you enter a search term, the label next to the folder name changes to indicate the number of issues that match the search as a subset of the total.

Search terms can be wrapped with delimiters to indicate the type of comparison that should be performed. You can use the following syntax in the search string field:
- **Contains**: Searches for a term without any special qualifying delimiters
- **Equals**: Searches for an exact match when the term is wrapped in quotation marks (""")
- **Regex**: Searches for values that match a Java-style regular expression delimited by a forward slash (/)
  - An example is /eas.+?/
- **Number range**: Uses standard mathematical syntax, such as "(" and ")" for exclusive range and "[" and "]" for inclusive range where "[2,4]" means greater than two less than or equal to four
- **Not Equals**: Negate any of the search term by preceding the string with an exclamation mark. For example, file:!Main.java returns all issues that are not in Main.java
Search terms can be further qualified with modifiers. For more information, see \textit{About Search Modifiers} on page 30. The syntax for using a modifier is \texttt{modifier:<search_term>}

The search string can contain multiple modifiers and search terms. When more than one modifier is specified, only issues that match all the modified search terms are returned.

For example, \texttt{file:ApplicationContext.java category:SQL Injection} returns issues found in \texttt{ApplicationContext.java} whose category is SQL Injection but not any other issues. If the same modifier is used more than once in a search string, then the search terms qualified by those modifiers will be treated as an OR comparison. Modifying the example to \texttt{file:ApplicationContext.java category:SQL Injection category:Cross-Site Scripting} finds the issues whose category is Cross-Site Scripting as well as the SQL Injection issues. All previous search terms are saved. You can click the down arrow in the text box to select previous search terms.

Creating complex search strings can be a multiple step process. If you enter an invalid search string, the magnifying glass in the text field changes to a warning sign to notify you of the error. Click the warning sign to view feedback on the error in the search term.

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.)

You can also use the Advanced Search string builder to build complex search strings. When you click the advanced link, the search string is parsed, and it populates the Advanced Search dialog box. In this dialog box, you can select the modifier, the comparison and type, and the search term from lists. The list for the search term includes the known values in the current scan for the specified attribute. In order to specify an unqualified search term, select \texttt{Any Attribute} in the modifier list.

When you build a search string in the Advanced Search dialog box, errors are displayed in the status below the search string builder. The \textbf{Find} button is not enabled until all errors are resolved.

\textbf{About Search Modifiers}

A search modifier can be used 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, delimit the modifier with brackets. For example, to search for issues that are new, enter \texttt{[issue age]:new}.

A search that is not qualified by a modifier tries to match the search string 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 \texttt{control flow}. This searches all of the 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: \texttt{analyzer:control flow}. This returns all results whose analyzer is \texttt{control flow}.

\textit{Table 6} lists the search modifiers.

\begin{table}[h]
\centering
\begin{tabular}{|l|l|}
\hline
\textbf{Modifier} & \textbf{Description} \\
\hline
\texttt{[issue age]} & Searches for the issue age, which is either \texttt{removed, existing, or new} \\
\hline
\texttt{<custom_tagname>} & Searches the specified custom tag. Note that tag names that contain spaces must be delimited by square brackets. \\
& \texttt{Example: [my tag]:value} \\
\hline
\texttt{analysis} & Searches for issues that have the specified audit analysis value (such as \texttt{"exploitable,""not an issue," and so on}) \\
\hline
\end{tabular}
\end{table}
<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 Primary Custom Tag is set and false if Primary Custom Tag is not set</td>
</tr>
<tr>
<td>category (cat)</td>
<td>Searches for the given category or category substring</td>
</tr>
<tr>
<td>comments (comment, com)</td>
<td>Searches the comments submitted on the issue</td>
</tr>
<tr>
<td>commentuser</td>
<td>Searches for issues with comments from a specified user</td>
</tr>
<tr>
<td>confidence (con)</td>
<td>Searches for issues that have the specified confidence value. HP 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>dynamic</td>
<td>Searches for issues that have the specified dynamic hot spot ranking 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 the HP Fortify analyzers. 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 up to and including the number specified as the search term</td>
</tr>
<tr>
<td>metagroup</td>
<td>Searches the specified metagroup. Metagroups include [OWASP Top 10 2010], [Sans Top 25 2010], and [pci 2.1], 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 less 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, [source context].</td>
</tr>
<tr>
<td>primaryrule (rule)</td>
<td>Searches for all issues related to the specified sink rule</td>
</tr>
<tr>
<td>ruleid</td>
<td>Searches for all issues reported by the specified rule IDs used to generate the issue source, sink and all passthroughs</td>
</tr>
</tbody>
</table>

Table 6: Search Modifiers (Continued)
Table 6: Search Modifiers (Continued)

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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&lt;br&gt;Also see source, [primary context].</td>
</tr>
<tr>
<td>sourcefile</td>
<td>Searches for dataflow issues with the source function call that the specified file contains.&lt;br&gt;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>
<tr>
<td>trace</td>
<td>Searches for issues that have the specified string in the dataflow trace</td>
</tr>
<tr>
<td>tracenode</td>
<td>Enables you to search on the nodes within an issue's analysis trace. Each tracenode search value is a concatenation of the tracenode's file path, line number, and additional information.</td>
</tr>
<tr>
<td>[no attribute]</td>
<td>Searches for issues that have any of the most common attributes that match the specified string</td>
</tr>
</tbody>
</table>

Search Query Examples

Consider the following examples:

- To search for all privacy violations in file names that contain jsp with getSSN() as a source, enter:
  category:"privacy violation" source:getssn file:jsp

- To search for all file names that contain com/fortify/awb, enter:
  file:"com/fortify/awb"

- To search for all paths that contain traces with mydbcode.sqlcleanse as part of the name, enter:
  trace:mydbcode.sqlcleanse

- To search for all paths that contain traces with cleanse as part of the name, enter:
  trace:cleanse

- To search for all issues that contain cleanse as part of any modifier, enter:
  cleanse

- To search for all suppressed vulnerabilities with asdf in the comments, enter:
  suppressed:true comments:asdf

- To search for all categories except for SQL Injection, enter:
  category:!SQL Injection injection
Performing Simple Searches

To use the search box to perform a simple search, do one of the following:

- Type a search string in the box and press ENTER.

Alternatively,

- To select a search term you used previously, click the arrow in the search box, and then select a search term from the list.

To get assistance in composing the comparison for your search string, do the following:

1. Click your cursor in the search box, and then press CTRL + SPACE.

2. From the displayed list, double-click an issue attribute to begin your search string.

3. To get assistance specifying the comparison, with your cursor placed after the modifier in the search box, press CTRL + SPACE.

4. From the displayed list, double-click the comparison to add to your search string.

5. Finish typing the search term.

The SCA Analysis Results view lists all of the issues that match your search string.

The plugin saves all of the search terms you enter for the current session. To select a search term you used previously, click the arrow in the search box, and then select a search term. (After you quit the plugin, the saved search terms are discarded.)

Creating complex search strings can involve several steps. If you enter an invalid search string, the magnifying glass icon in the text field changes to a warning icon to notify you of the error. Click the warning sign to view information about the search term error.

The advanced search feature makes it easier to build complex search strings. For a description of this feature and instructions on how to use it, see Performing Advanced Searches.
Performing Advanced Searches

You can use the advanced search feature to build complex search strings.

To use the advanced search feature:

1. In the search box, type a search term.
2. To the right of the search box, click Advanced.

   The plugin parses the search term, and uses it to populate the Advanced Search dialog box. The box on the left displays the modifier, the middle box displays the comparison and type, and the box on the right displays the search term.

   The plugin adds a new AND query row to the dialog box.

3. To change the AND operator to an OR operator, double-click AND / OR.
4. Select the modifier, the comparison and type, and the search term from the lists.

   The list for the search term includes the known values in the current scan for the specified attribute. However, you can type any value into this field. To specify an unqualified search term, select Any Attribute from the bottom of the modifier list.

5. To add an AND query row, in the top right corner of the dialog box, click AND add &. To add an OR query row, in the top right corner of the dialog box, click OR add ||.
6. Add as many query rows as you need for the search.
7. To delete a row, to the right of the row, click Delete - . To remove all rows, click Clear.
8. Click Find.

   Note: As you build your search string, the Advanced Search dialog box displays any errors in the status below the search string builder. The Find button is not enabled unless all errors are resolved.
About Working with Issues

This section provides information about how to use the Eclipse Plugin to work with issues.

Grouping Issues

The items visible in the navigation tree vary according to which grouping option is selected. You can view issues using any of the Group By options, and you can create and edit customized groups. The Group By options enable you to group and view the issues in different ways. In practice, you will probably switch frequently between various groupings. Table 7 lists descriptions of the standard Group By options.

Table 7: Group By Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzer</td>
<td>Groups issues by analyzer group</td>
</tr>
<tr>
<td>Analyzer Type</td>
<td>Groups issues by HP Fortify analyzer product</td>
</tr>
<tr>
<td>Audit Analysis</td>
<td>Groups issues by the audit analysis, such as suspicious and exploitable</td>
</tr>
<tr>
<td>Category</td>
<td>Groups issues by vulnerability category. This is the default setting.</td>
</tr>
<tr>
<td>File name</td>
<td>Groups issues by file name</td>
</tr>
<tr>
<td>Package</td>
<td>Groups issues by package or namespace. Does not appear for projects for which this option is not applicable, such as C projects.</td>
</tr>
<tr>
<td>Sink</td>
<td>Groups issues that share the same dataflow sink function</td>
</tr>
<tr>
<td>Source</td>
<td>Groups issues that share the same dataflow source functions</td>
</tr>
<tr>
<td>Taint flag</td>
<td>Groups issues by the taint flags that they contain</td>
</tr>
<tr>
<td>New Issue</td>
<td>Shows which issues are new since the last scan. For example, if you run a new scan, any issues that are new display in the tree under the New Issues group and the others are displayed in the Existing Issues group. Issues not found in the latest scan are displayed in the Removed list.</td>
</tr>
<tr>
<td>(none)</td>
<td>Displays a flat view without grouping.</td>
</tr>
<tr>
<td>Fortify Priority Order</td>
<td>Groups issues High, Medium, and Low issues based on the combined values of SCA confidence and severity.</td>
</tr>
<tr>
<td>Category Analyzer</td>
<td>A sample custom group that groups issues by category and then analyzer.</td>
</tr>
<tr>
<td>Edit</td>
<td>Select Edit to create a custom Group By option. Control group order in the list on the right.</td>
</tr>
</tbody>
</table>
Creating a Grouping Option

You can create a custom Group By option that groups issues in a hierarchical format in sequential order based on specific attributes.

To create a new grouping option:

1. Select **Edit** in the **Group By** list.
   
   The Edit Custom Groupings dialog box opens.

2. From the list on the left, select a grouping option, and then click the right-pointing arrow to move the option to the **Grouping Order** column.

3. Repeat to select additional options.

For example, selecting **Analyzer** creates a list that has top level nodes that contain the category of the issue, such as Buffer Overflow, with the issues grouped below by analyzer, such as semantic, or dataflow, followed by the issues.

- Buffer Overflow [0/2]
  - DataFlow [0/1]
  ---- Main.cs:234
  ---+ Semantic [0/1]

Evaluating Issues

To evaluate and assign auditing values to an issue or group of issues:

1. Select the issue or group of issues in the **SCA Analysis Results** view.
   
   For information about the **SCA Analysis Evidence** view, see **About the SCA Analysis Results View** on page 22.

2. Read the abstract on the **Issue Summary** tab, which provides a high-level information about the issue, such as the analyzer that found the issue.
   
   For example, “Command Injection (Input Validation and Representation, dataflow)” indicates that this issue, detected by the dataflow analyzer, is a Command Injection issue in the Input Validation and Representation kingdom.

3. Click the **More Information** link or the **Issue Details** tab to get more details about the issue.

4. On the **Issue Summary** tab, select one of the following to represent your evaluation:
   
   - Not an issue
   - Reliability issue
   - Unknown
   - Suspicious
   - Exploitable

5. (Optional) In the **Comments** box, type comments relevant to the issue and your evaluation.
Creating Issues
Add undetected issues that you want to identify as issues to the issues list. You can audit manually configured issues on the Issue Summary tab, just as you do other issues.

To create an issue:
1. Select the object in the line of code in the source code view.
2. Right-click the line that contains the issue, and then select Create New Issue from the shortcut menu.
   The Create New Issue dialog box opens.
3. Select the issue category, and then click OK.

The issue is added to the navigation tree, showing "(custom issue)" on the right. You can edit it to include audit information, just as you can the other issues.

Suppressing Issues
You can suppress issues that are either fixed, or that you are not planning to fix.

To suppress an issue, do one of the following:

- In the SCA Analysis Results view, select the issue, and then, on the Issue Summary tab, click Suppress.
- In the SCA Analysis Results view, right-click the issue, and then click Suppress Issue on the shortcut menu.

To review results that have been suppressed, select Show Suppressed Issues from the show issues menu on the SCA Analysis Results toolbar.
Customizing the SCA Analysis Results View

You can customize the SCA Analysis Results view to determine which issues it lists.

To change the SCA Analysis Results view:

1. Select HP Fortify → Options.
   The Options dialog box opens.
2. In the left panel, select Interface Preferences.
3. To change your preferences, select or clear the following check boxes, and then click OK. (To return to the default view, click Reset Interface.)
   - **Show Suppressed Items**: Shows all of the items that you have suppressed. This option is disabled by default.
   - **Show Removed Items**: If you have performed an Import New SCA Analysis, shows all of the items that were removed since the previous analysis.
   - **Show Hidden Items**: Shows all of the items that are hidden.
   - **Collapse Issues**: If you have performed an Import New SCA Analysis, shows all of the items that were removed since the previous analysis.
   - **Use Short File Names**: References the issues in the SCA Analysis Results view by filename only, instead of by relative path. This option is enabled by default.
• **Show Category of View:** Enables you to show the Analysis Evidence, Issues, and Summary panels. It also provides the Other option, which contains standard Eclipse navigation features.

• **Show Abstract in Issue Summary:** Shows the abstract text in the summary.

• **Show Comments in Issue Summary:** Shows the abstract text in the summary.

• **Show All Folder in Issue Summary Graph:** Shows the abstract text in the summary.

• **Right justify All folder:** Displays the All folder with contents aligned on the right.

• **Display name in folder tabs:** Displays the name text in the folder tabs.

### Submitting an Issue as a Bug

You can submit issues to your bug tracking application if you have integrated the application with Eclipse or if you are using HP Fortify Software Security Center.

To submit an issue as a bug if your bug tracking application is integrated with Eclipse:

1. Select the issue in the SCA Analysis Results view, and then, on the Issue Summary tab, click the File Bug icon.
   
   If you are submitting a bug for first time, the Configure Bugtracker Integration dialog box opens. (For information about configuring the plugin with bug tracking systems, see About Bug Tracking System Integration on page 60.)
   
   The File Bug dialog box opens.

2. Specify the values if changes are needed and review the issue description. Depending on the integration and your bug tracking application, the values include items such as the bug tracking application URL, product name, severity level, summary, and version.

3. Click **Submit**.

You must already be logged on before you can file a bug through the user interface for bug-tracking systems that require a logon. The issue is submitted as a bug in the bug tracking application.

If you use HP Fortify Software Security Center, you can submit an issue as a bug from within Eclipse using a bug tracking system configured through HP Fortify Software Security Center. Currently, HP Fortify Software Security Center supports the following bug tracking systems:

- Bugzilla
- Jira
- ALM

To submit an issue as a bug through the Software Security Center Collaboration Module:

1. Select the issue in the SCA Analysis Results view, and then, on the Issue Summary tab, click the File Bug icon.
   
   If you are submitting a bug for first time, the Configure Bugtracker Integration dialog box opens.

2. Select the bug-tracking application, and then click **OK**.
   
   The File Bug dialog box opens.

3. Specify the values if changes are needed and review the issue description. Depending on the integration and your bug-tracking application, the values include items such as the bug-tracking application URL, product name, severity level, summary, and version.

4. Click **Submit**. (If your bug-tracking system requires you to log on, you must do so before you can file a bug through that user interface.)
About HP Fortify Reports

The Eclipse Plugin provides a flexible reporting infrastructure based on user-configurable report templates. Report templates provide several optional sections and subsections that gather and present specific types of data. The following sections provide information about the default reports and report templates, instructions on how to modify existing reports, and how to create your own reports.

Opening HP Fortify Report Templates

To open a report template:

1. Select **HP Fortify → Generate Report**.
   
   The Generate Reports dialog box opens.
2. Select a report template from the **Report** list.
   
   The Generate Report dialog box displays the report template settings.

Generating Reports

After you select a report template and specify report settings, you generate the report to view the results. You can save report results as PDF, RTF, and XML files.

To run a report:

1. Select **HP Fortify → Generate Report**.
   
   The Generate Reports dialog box opens.
2. Select a report template from the **Report** list.
3. (Optional) Make changes to the report section settings.
4. Click **Save Report**.
   
   The Save Report dialog box opens.

5. Make any necessary changes to the report details, including its location and format.
   
   **Note:** If you save the file in rich text format (RTF), the report can be opened only in Microsoft Word or WordPad.
6. Click **Save**.
   
   The report is generated and saved as a file in the format you selected.
About HP Fortify Report Templates

The HP Fortify report templates are displayed when the product is first installed. If you or another user have edited or created other default report templates, you might not see the default report templates.

The HP Fortify report templates include:

- **HP Fortify Security Report**: A mid-level report providing comprehensive information on the analysis that was performed and the high-level details of the audit that was performed. It also provides a high-level description and examples of categories that are of the highest priority.

- **HP Fortify Developer Workbook**: A comprehensive listing of all categories of issues found and multiple examples of each issue. It also gives a high-level summary of the number of issues in each category.

Selecting Report Sections

You can choose sections to include in the report, and you can edit the content displayed in each section.

To select sections to include in the report:

1. Select each section title check box in the list on the left side to include the section in the report.
2. Click a section title to view the contents of the section.

The section details are displayed to the right of the dialog box. For instructions on how to edit each section, see *About Adding Report Subsections* on page 45.

To remove a section from the report, clear the check box next to the section title.

About Report Subsections

When you select a section title, you can edit the contents to display in the report. You can edit text, add or change text variables, or customize the issues shown in a chart or results list.

Editing Text Subsections

To edit a text subsection:

1. Select the check box next to the subsection title to include this text in the report. A description of the text displays below the subsection title.
2. Click **Edit Text**.
   
The text box displays the text and variables to be included in the report.
3. Edit the text and text variables as needed.

When you edit text subsections, you can insert variables that are defined when you run the report (see *Table 8*).

### Table 8: Text Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$AUDIT_GUIDE_SUMMARY$</td>
<td>List of filters created by answering Audit Guide questions</td>
</tr>
<tr>
<td>$CLASSPATH_LISTING$</td>
<td>JAR files used during scan, one relative path per line</td>
</tr>
<tr>
<td>$COMMANDLINE_ARGS$</td>
<td>Complete listing of command line arguments (same format as project summary)</td>
</tr>
<tr>
<td>$FILE_LISTING$</td>
<td>List of files scanned, each file in format <code>&lt;relative file path&gt; # Lines # kb &lt;timestamp&gt;</code></td>
</tr>
<tr>
<td>$FILTERSET_DETAILS$</td>
<td>List of filters in use by current filter set</td>
</tr>
</tbody>
</table>
Table 8: Text Variables (Continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$FILTERSET_NAME$</td>
<td>Name of current filter set</td>
</tr>
<tr>
<td>$FORTIFY_SCA_VERSION$</td>
<td>SCA version</td>
</tr>
<tr>
<td>$LIBDIR_LISTING$</td>
<td>Libdirs specified during scan, one relative path per line</td>
</tr>
<tr>
<td>$LOC$</td>
<td>Total lines of code</td>
</tr>
<tr>
<td>$NUMBER_OF_FILES$</td>
<td>Total number of files scanned</td>
</tr>
<tr>
<td>$PROJECT_BUILD_LABEL$</td>
<td>Build label of project</td>
</tr>
<tr>
<td>$PROJECT_NAME$</td>
<td>Build ID</td>
</tr>
<tr>
<td>$PROPERTIES$</td>
<td>Complete listing of properties set during analysis phase (same format as project summary)</td>
</tr>
<tr>
<td>$RESULTS_CERTIFICATION$</td>
<td>Complete certification detail with listing of validity on a per file basis (see project summary)</td>
</tr>
<tr>
<td>$RESULTS_CERTIFICATION_SUMMARY$</td>
<td>Short description of certification (same format as project summary)</td>
</tr>
<tr>
<td>$RULEPACKS$</td>
<td>Complete list of Rulepacks used during analysis (same format as project summary)</td>
</tr>
<tr>
<td>$RUN_INFO$</td>
<td>Content from the Project Summary Runtime Information tab</td>
</tr>
<tr>
<td>$SCAN_COMPUTER_ID$</td>
<td>Hostname of machine on which the scan was performed</td>
</tr>
<tr>
<td>$SCAN_DATE$</td>
<td>Date of analysis with the default formatting style for the locale</td>
</tr>
<tr>
<td>$SCAN_SUMMARY$</td>
<td>Summary of code base scanned in format # files, # lines of code</td>
</tr>
<tr>
<td>$SCAN_TIME$</td>
<td>Time of analysis phase</td>
</tr>
<tr>
<td>$SCAN_USER$</td>
<td>Username for the user who performed the scan</td>
</tr>
<tr>
<td>$SOURCE_BASE_PATH$</td>
<td>Source base path of code base</td>
</tr>
<tr>
<td>$TOTAL_FINDINGS$</td>
<td>Total number of findings, not including suppressed or removed issues</td>
</tr>
<tr>
<td>$WARNINGS$</td>
<td>Complete list of warnings that occurred (same format as project summary)</td>
</tr>
<tr>
<td>$WARNING_SUMMARY$</td>
<td>Count of warnings found in scan</td>
</tr>
</tbody>
</table>

Editing Results List Subsections

To edit a result list subsection:

1. Select the check box next to the subsection title to include this text in the report. A description of the results list displays below the subsection title.
2. Click the issues listing heading to expand the options.
3. Select the attributes that the results list will be grouped by. For the list of attributes to group by, see About Working with Issues on page 35. If you group by category, the recommendations, abstract, and explanation for the category are also included in the report.
4. You can refine the issues shown in this subsection by using the Search functions. For more details on the search syntax, see About Searching Issues on page 29.
   The query displays in the Refine Issues in Subsection field.

5. Select or clear the Limit number of Issues in each group check box.

6. If you selected the check box, type the number of issues to display per group.

Editing Charts Subsections
To edit a chart subsection:

1. Select the check box next to the subsection title to include this text in the report. A chart description is displayed below the subsection title.

2. Select the attributes that the chart data will be grouped by. For the list of attributes to group by, see About Working with Issues on page 35.

3. You can refine the issues shown in this subsection by using the Search functions. For more details on the search syntax, see About Searching Issues on page 29.
   The query is displayed in the Refine Issues in Subsection field.

4. Select the chart type (table, bar, or pie).

Saving Report Templates
You can save the current report settings as a new template that you can select at a later time to run more reports.

To save settings as a report template:

   The Generate Reports dialog box opens.

2. Select the report template from the Report list.

3. Make changes to the report section and subsection settings.

4. Click Save as New Template.
   The new report template is saved. When you select the report template name from the Report list, the report settings are displayed in the Generate Report dialog box.

Saving Changes to Report Templates
You can save changes to a report template so that your new settings are displayed as the defaults for that template.

To save changes a report template:

   The Generate Reports dialog box opens.

2. Select the report template to save as the default report template from the Report list.

3. (Optional) Make changes to the report section and subsection settings.

4. Click Save Settings as Default.
Editing Report Template XML Files

Report templates are saved as XML files. You can edit the XML files to make changes or to create new report template files. When you edit the XML files, you can choose the sections and the contents of each section to include in the report template.

The default location for the report template XML files is:

```
eclipse_install_directory>/Core/config/reports
```

You can also customize the logos used in the reports by specifying paths or replacing `header.png` and `footer.png` in this directory.

Adding Report Sections

You can add report sections by editing the XML files. In the structure of the XML, the `ReportSection` tag defines a new section. It includes a `Title` tag for the section name, and it must include at least one `Subsection` tag to define the contents of the section in the report. The following XML is the Results Outline section of the HP Fortify Security Report:

```xml
<ReportSection enabled="false" optionalSubsections="true">
    <Title>Results Outline</Title>
    <SubSection enabled="true">
        <Title>Overall number of results</Title>
        <Description>Results count</Description>
        <Text>The scan found $TOTAL_FINDINGS$ issues.</Text>
    </SubSection>
    <SubSection enabled="true">
        <Title>Vulnerability Examples by Category</Title>
        <Description>Results summary of the highest severity issues. Vulnerability examples are provided by category.</Description>
        <IssueListing limit="1" listing="true">
            <Refinement>severity:(3.0,5.0] confidence:[4.0,5.0]</Refinement>
            <Chart chartType="list">
                <Axis>Category</Axis>
            </Chart>
        </IssueListing>
    </SubSection>
</ReportSection>
```

In this example, the Results Outline section contains two subsections. The first subsection is a text subsection named Overall number of results. The section subsection is a results list named Vulnerability Examples by Category. A section can contain any combination of subsections as its contents.
About Adding Report Subsections

In the report sections, you can add subsections or edit the contents of the subsections. Subsections can generate text, results lists, or charts.

Adding Text Subsections

In a text subsection, you can include the Title tag, the Description tag, and the Text tag. In the Text tag, you can provide the default content although the user can edit the content before generating a report. For a description of the text variables available to use in text subsections, see About Report Subsections on page 41. The following XML is the Overall number of results subsection in the Results Outline section:

```
<SubSection enabled="true">
  <Title>Overall number of results</Title>
  <Description>Results count</Description>
  <Text>The scan found $TOTAL_FINDINGS$ issues.</Text>
</SubSection>
```

In this example, the text subsection is titled Overall number of results. The description text to describe the purpose of the text is Results count. The text in the text field that the user can edit before running a report uses one variable named $TOTAL_FINDINGS$.

Adding Results List Subsections

In a results list subsection, you can include the Title tag, the Description tag, and the IssueListing tag. In the IssueListing tag, you can define the default content for the limit and set listing to true. You can include the Refinement tag either with or without a default statement although the user can edit the content before generating a report. To generate a results list, the Chart tag attribute chartType is set to list. You can also define the Axis tag. The following XML is the Vulnerabilities Examples by Category subsection in the Results Outline section:

```
<SubSection enabled="true">
  <Title>Vulnerability Examples by Category</Title>
  <Description>Results summary of the highest severity issues. Vulnerability examples are provided by category.</Description>
  <IssueListing limit="1" listing="true">
    <Refinement>severity:(3.0,5.0] confidence:[4.0,5.0]</Refinement>
    <Chart chartType="list">
      <Axis>Category</Axis>
    </Chart>
  </IssueListing>
</SubSection>
```

In this example, the results list subsection is titled Vulnerability Examples by Category. The description text to describe the purpose of the subsection is Results summary of the highest severity issues. Vulnerability examples are provided by category. This subsection will list (listing=true) one issue (limit="1") per Category (the Axis tag value) where there are issues matching the statement severity:(3.0,5.0] confidence:[4.0,5.0] (the value of the Refinement tag).

Adding Charts Subsections

In a chart subsection, you can include the Title tag, the Description tag, and the IssueListing tag. In the IssueListing tag, you can define the default content for the limit and set listing to false. You can include the Refinement tag either with or without a default statement although the content can be edited by the user before generating a report. To generate a pie chart, the Chart tag attribute chartType is set to pie. The options are table, pie, and bar. The user can change this setting before generating the report. You can also define the Axis tag.
The following code shows an example of a charts subsection:

```xml
<SubSection enabled="true">
  <Title>New Issues</Title>
  <Description>A list of issues discovered since the previous analysis</Description>
  <Text>The following issues have been discovered since the last scan:</Text>
  <IssueListing limit="-1" listing="false">
    <Refinement />
    <Chart chartType="pie">
      <Axis>New Issue</Axis>
    </Chart>
  </IssueListing>
</SubSection>
```

In this subsection, a chart (limit="-1" listing="false") will have the title New Issues and a text section that contains the text "The following issues have been discovered since the last scan." This chart will include all issues (the Refinement tag is empty) and will group the issues on the value of New Issues (the value of the Axis tag). This chart is displayed as a pie chart (chartType="pie").

### Synchronizing with Software Security Center

The Eclipse Plugin enables you to automatically upload your changes to a project version on Software Security Center each time you load, merge, save and/or scan your local project. This automatic synchronization helps facilitate collaborative auditing, and enables you to synchronize any offline changes each time you connect to the server.

**Note:** Automatic synchronization requires that you specify a project version that already exists in Software Security Center. If the project version does not exist in Software Security Center, you must first create it. For instructions, see the HP Fortify Software Security Center User Guide.

To enable or disable synchronization to the server:

1. Select **Remember my decision for all projects** to enable or disable synchronization to the server for all projects you work with in the future. This is optional.
2. To enable synchronization, click **Yes**. To disable synchronization, click **No**.

### Scheduling Synchronization

You can customize which action synchronizes your local version of the project with the server. For example, you can customize so synchronization occurs only when you merge or scan a project.

To customize when synchronization occurs:

1. Right-click a project.
2. Select **Properties**.
   
   The Properties dialog box opens.
3. Select **Fortify Project Properties**.
4. Select the **Synchronize Options** tab.
   
   A check box list is displayed.
5. Select the options that you want to exclude from automatic synchronization.
6. Click **OK**.
Understanding Project Templates and Project Configuration

When SCA analyzes source code, it produces comprehensive results. On large code bases, these results can be overwhelming. The project template assigned to your projects enables you to sort and filter the results to best suit your needs.

The filtering and sorting mechanisms appropriate during a given phase in the development process might be less appropriate later. Similarly, the filtering and sorting mechanisms might vary depending on the role of the user.

You can sort issues by grouping issues into folders, which are logically defined sets of issues listed on the tabs in the SCA Analysis Results view. To customize the sorting further, you can provide custom definitions for the folders into which issues are sorted. You can define any number of folders, the contents of which are then determined by filters.

Filters can either can change the visibility of an issue or place an issue into a folder. If used to sort issues into folders, you can define the nature of the issues placed in the customized folders.

In addition to providing sorting and filtering mechanisms, you can customize the auditing process by defining custom tags in the project template. Custom tags are name-value pairs that are associated with issues by users during auditing. For example, custom tags can be used to track impact, severity, or priority of an issue, using the same names and values used to track these attributes in other systems, such as a defect tracking system.

The filters used to sort and filter issues are split into distinct filter sets. A project template can contain definitions for multiple filter sets. Using multiple filter sets in a project enables you to quickly change the sorting and visibility of the issues you are auditing. For example, the default project template used in the interface provides four filter sets.

Filter sets provide an increasingly restrictive view of security-related issues from Broad, Medium, and Targeted. The fourth filter set, named Developer, provides a view that restricts the visible issues to high-confidence issues that are related to code-quality and reliability issues. Defining multiple filter sets for a project enables different users of the results a different view, and customization of one view does not affect other views.

The project template applied to a project is determined using the following order of preference:

1. The template that exists in the FPR
2. The template `<fortify_install_root>/Core/config/filters/defaulttemplate.xml`
3. The template `<fortify_install_root>/Core/config/rules/defaulttemplate.xml`
4. The embedded HP Fortify default template

The Eclipse Plugin provides many ways for you to configure your projects and project templates. The following sections include instructions on how to manage the project configuration settings.
About Managing Folders

Folders are logical sets of issues that are defined by the filters in the active filter set. Even though a folder may appear in more than one filter set, the contents may differ depending on the filters in that filter set that target the folder. To accommodate filter sets that attempt to provide sorting mechanisms that have little overlap, it is possible to have filter sets with different folders. Folders are defined without any relation to the filter sets they may appear in. A folder definition entitled Hot that is red may be unrelated to the fact that there may be a filter set that only places low priority issues into this folder.

Creating Folders

You can add a folder to a filter set. Folders must have unique names.

To create a new folder:

1. Select **HP Fortify → Project Configuration**.
   
The Project Configuration dialog box opens.

2. Click the **Folders** tab.
   
   A list of the currently defined folders is displayed on the left. Fields that indicate the current Name, Color, and Description of the currently selected folder display on the right.

3. Select a filter set to enable a folder that is displayed in the selected filter set only from the **Folders for Filter Set** list.
   
The **Folders for Filter Set** list filters the folders displayed in the folder list.
   
   If you select **All Folders**, all folders defined in the project template are listed.

4. To add a folder:
   
   a. Click the plus character (+) next to **Folders**.
      
The Create a New Folder dialog box opens.

   b. Type a name for the new folder, select a folder color, and then click **OK**.
      
The folder is added to the bottom of the folder list.

5. (Optional) Drag the folder up or down to change the tab position on the **Issue** panel, where the top position is on the left and the bottom position is on the right.

6. (Optional), select **Default Folder** to put all issues that do not match a folder filter into this folder.

7. Click **OK**

   The folder is displayed as a tab with the other folders. If you selected default, all issues that do not match a folder filter are displayed.

   **Note:** To display issues in this folder, create a folder filter that targets the new folder.

Adding Folders to Filter Sets

This section describes how to enable an existing folder in a filter set. Create a new folder that only appears in the selected filter set using the instructions *Creating Folders* on page 48. To display issues in this folder, create a folder filter that targets the new folder.

To add a folder:

1. Select **HP Fortify → Project Configuration**.
   
The Project Configuration dialog box opens.

2. Click the **Folders** tab.

3. Select a filter set to enable a folder that displays in the selected filter set only from the **Folder for Filter Set** list.
The **Folders for Filter Set** list filters the folders displayed in the folder list. If you select **All Folders**, the list displays all folders defined in the project template.

4. Click the plus character (+) next to **Folders**.
   
   The Add a new Folder to the Filter Set dialog box opens. If this filter set already displays all folders, the Create New Folder dialog box opens.

5. Select the folder to add, and then click **Select**.

6. Click **OK**.

   The folder is displayed as a tab along with the other folders.

### Renaming Folders

You can rename a folder. Note that the folder name change is global and is reflected in all filter sets.

To rename a folder:

1. Select **HP Fortify → Project Configuration**.
   
   The Project Configuration dialog box opens.

2. Click the **Folders** tab.

3. Select a filter set that displays the folder you want to rename from the **Folders for Filter Set** list.

4. Select the folder in the list.
   
   The folder properties dialog box opens.

5. Enter the new name for the folder.
   
   The folder name changes in the list as you are typing.

6. Click **OK**.

   The new folder name displays on the tabs.

### Removing Folders

You can remove a folder from a filter set without removing it from the other filter sets.

To remove a folder:

1. Select **HP Fortify → Project Configuration**.
   
   The Project Configuration dialog box opens.

2. Click the **Folders** tab.

3. Select a filter set from the **Folders for Filter Set** list. The folder is removed only from the selected filter set.
   
   The folder list displays the folders in the selected filter set.

4. Select the folder and click the minus character (-) next to **Folders**.
   
   If the folder is a target of a folder filter, the Conflicts Occurred Removing a Folder dialog box opens.

5. Retarget or delete folder filters, as required.

6. Click **OK**.

   The folder is no longer displayed as a tab.
Configuring Custom Tags for Auditing

You can customize a project by defining custom tabs to use during an audit. After you define a custom tag the Issue Summary tab displays it as a list. If you designate the tag as an extensible tag, users can specify new values for the tag on the fly, as needed for specific issues.

Custom tags are also visible in other areas of the interface, such as in the Group By list (as a way to group issues in a folder), in the search field as a modifier for a search, and in the project summary graph as an attribute by which to graphically sort issues.

If you use a custom tag name as a search modifier, you can search on the value assigned to the tag, or you can specify a range of values. The values for a custom tag are an enumerated list, wherein the first value is 0, the second is 1, and so on. You can use the search syntax for a range of numbers to search for ranges of custom tag values. For example, analysis:[0,2] returns the issues that have the first three analysis values, 0, 1, and 2.

Security auditors can use custom tags to set additional attributes that describe an issue. You can use custom tag values to filter and find issues. The custom tag Analysis is configured by default. After you assign an Analysis tag value to an issue, icons in the issues list in the SCA Analysis Results view indicate the analysis status of that issue.

Set the visibility filters and folder filters conditions to match custom tag values. For example, a visibility filter “Analysis: matches not an issue hide issue” and all the issues that the auditor has marked are removed from the issues list in the SCA Analysis Results view.

Creating Custom Tags

Custom tags are project-wide and are saved as part of a project template.

To create a custom tag:

1. Select HP Fortify → Project Configuration.
   The Project Configuration dialog box opens.
2. Select the Custom Tags tab.
3. Next to Tags, click the plus icon .
   Note: If you previously deleted tags, a list of those tags displays, and you can re-enable those tags. In this case, click Create New to create a new tag.
   The Enter Value dialog box opens.
4. Enter a name for the tag, and then click OK.
   The new tag displays in the list.
5. To add values to a tag:
   a. From the Tags list, select the tag name.
   b. Next to Values, click the plus icon .
   c. In the Enter Value dialog box, type a value, and then click OK.
   d. (Optional) To set the value of the attribute when the auditor does not select a value, from the Default Value menu, select a default value to assign. If you do not specify a default value, the default is null.
6. Repeat Step 5 for each additional value required for the tag, and then click OK.

The Issue Summary tab displays the tags and values.
Deleting a Custom Tag

If you delete a custom tag, it is no longer available on the Issue Summary tab or as a search or filter option. If the custom tag was set for an issue, deleting the tag does not remove the tag or value from the issue.

To delete a custom tag:
1. Select HP Fortify → Project Configuration.
   The Project Configuration dialog box opens.
2. Click the Custom Tags tab.
3. Select the tag from the list.
4. Next to Tags, click the minus icon \( - \).
5. Click OK.

If you delete a tag that has an associated filter, you are prompted to delete the filter.

Setting the Default Filter Set

To specify the default filter set used to view scan findings:
1. From the Filter Set list, select Edit.
   The Project Configuration dialog box opens to the Filter Sets tab.
2. In the Filter Sets list, select the filter set you want to use as the default for the project template.
3. Select the Default Filter set check box, and then click OK.

Creating a New Filter Set

To create a new filter set, you copy an existing set. Once you create the copy, you can modify the settings.

To create a new filter set:
1. Select HP Fortify → Project Configuration.
2. Click the Filter Sets tab.
3. Click + (plus symbol) next to Filter Sets.
   The Create New Filter Set dialog box opens.
4. Enter a name for the new template set.
5. Select an existing template set to copy.
6. Click OK.

A new filter set that has the same folders, visibility filters, and folder filters is created.

Configuring Filters

This section provides instructions on how to create filters from the Issues panel, create filters on the Filters tab, and how to copy a filter to a different filter set.

Creating a Filter from the Issue Panel

When you find an issue in a folder list that you want to hide or direct to another folder, you can create a new filter using the filter wizard. The wizard displays all the attributes with matching conditions for the filter.

**Note:** To find the filter that directed the issue to the folder, right-click the issue, and select Why is this issue here? To find the filter that hid an issue, right-click the issue, and select Why is this issue hidden?
To create a new filter from an issue:

1. From the **Filter Set** list, select a filter set.
2. In the **SCA Analysis Results** view, right-click an issue, and then select **Generate Filter**.
   
   The Create Filter dialog box displays a list of suggested conditions.
3. To see all of the conditions, select the **Show all conditions** check box.
   
   Additional conditions are displayed.
4. Select the conditions you want to use in the filter. Fine tune the filter later by modifying it on the **Filter** tab.
5. Select the type of filter you want to create, as follows:
   - Select **Hide Issue** to create a visibility filter.
   - Select **Set Folder to** to create a folder filter, and then select the folder name or select **Other Folder** to add an existing folder or create a new one.
   
   A new folder is displayed in this filter set only.
6. Click **Create Filter**.
   
   The wizard places the new filter at the end of the filter list. For folder filters, this gives the new filter the highest priority. Issues matching the new folder filter appear in the targeted folder.
7. (Optional) For folder filters, drag the filter higher in the folder filter list to change the priority.
   
   The issues are sorted using the new filter.

**Note:** The filter is created only in the selected filter set.

Creating a New Filter on the Filters Tab

Use the **Filters** tab option to create general filters for the attributes and values you want to filter. The filter is created in the selected filter set only.

Folder filters are applied in order and the issue is directed to the last folder filter it matches in the list. The wizard places your new filter at the end of the list.

To create a new filter on the **Filters** tab:

1. From the **Filter Set** list, select a filter set.
2. Right-click **Visibility Filter** or **Folder Filter**, and then select **Create New Filter** from the shortcut menu.
   
   The **If** panel displays the message, “Please specify a modifier for the search.”
3. From the first list, select an issue attribute.
   
   The second list automatically populates.
4. From the second list, select how to match the value.
   
   The third list automatically displays the values for the attribute.
5. Select a value or specify a range as instructed in the “If” line.
6. Set Then to one of the following options:
   - Select **Hide Issue** to create a visibility filter.
   - Select **Set to Folder** to create a folder filter, and then select the folder name or select **Other Folder** to add a folder from another filter set or create a new folder.
   
   The new filter displays at the end of the list. For folder filters, this gives the new filter the highest priority. Issues matching the new folder filter appear in the targeted folder.
7. (Optional) For folder filters, drag the filter higher in the folder filter list to change the priority.
   
   The issues are sorted using the new filter.

**Note:** The filter is created in the selected filter set only.
Copying a Filter to Another Filter Set

Filter settings are local to the filter set. However, you can copy the filter to another filter set in the project. If you are copying a folder filter to another set and that folder is not already active in the set, the folder is automatically added.

To copy a filter:
1. From the Filter Set list, select a filter set.
2. On the Filters tab, right-click a filter, and then select Copy Filter to from the shortcut menu.
   The Select a Filter Set dialog box lists all of the filter sets.
3. Select a filter set, and then click OK.
   The filter is added to the filter set in the last position.
4. (Optional) For folder filters, you can adjust the order of the filter list by dragging and dropping the filter to a different location in the list.

Saving Project Templates

Once a project template is associated with a project, all changes made to that template, such as the addition of folders, custom tags, filter sets, or filters, apply to the project, and the project template is stored in the FPR when the project is saved. For information about how to the project template associated with a project, see Importing a Project Template on page 54.

About Project Template Sharing

Project templates allow you to use the same project settings for another project. The project template contains the following settings:

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

The following sections provide instructions on how to export and import project templates.

Exporting a Project Template

Exporting a project template creates a file that contains the current project’s filter sets and custom tags. Use the template to import the project template into another project file.

To export a project template:
1. Select HP Fortify → Project Configuration.
   The Project Configuration dialog box opens.
2. Click the Filter Sets tab.
3. Click Export Project Template.
   The Save Project Template dialog box opens.
4. Browse to the location where you want to save the file.
5. Enter a file name without an extension.
6. Click Save.

The current template settings are saved to the new XML file.
Importing a Project Template

Importing a project template overwrites the project configuration settings. The filter sets and custom tags are replaced with the ones in the project template.

To import a project template:

1. Select **HP Fortify → Project Configuration**.
   
The Project Configuration dialog box opens.
2. Click the **Filter Sets** tab.
3. Click **Import Project Template**.
   
The Import Project Template dialog box opens.
4. Select the project template file to import.
5. Click **Import**.

The filter sets and custom tags are updated. You can also click **Reset to Default Project Template** to return the settings to the default project template.

Working with Projects

This section contains the following topics:

- Opening Projects on page 54
- Migrating Audit Data for FPRs from HP Fortify Static Code Analyzer Version 4.5.1 or Earlier on page 54
- Merging Audit Data on page 56
- Uploading Results to HP Fortify Software Security Center on page 56

Opening Projects

To open an FPR file:

1. Open the Eclipse Plugin.
2. Select **File → Open Project**.
   
The Choose Project dialog box opens.
3. Browse to and select the FPR file, and then click **Open**.

If the FPR format is SCA version 4.5.1 or earlier, the Migration Wizard automatically starts. Otherwise, the FPR is displayed in the Audit perspective.

**Important**: Make sure that you migrate the issue IDs before you migrate the audit data.

Migrating Audit Data for FPRs from HP Fortify Static Code Analyzer Version 4.5.1 or Earlier

The current version of the Eclipse Plugin improves the way audit data are managed. Audit data are now customized and configured from the user interface on a per-project basis. Audit data are automatically displayed when you open the project. If custom Audit Labels are present, you no longer need to modify the Eclipse Plugin and Software Security Center configuration files with the custom audit label information. Each project can have a unique set of labels.

In earlier versions, an auditor could only add preconfigured information to an issue. The auditing labels and values were static and local to the instance of the Eclipse Plugin. Customizing the audit labels required the user to manually edit the Eclipse Plugin configuration files. Each instance of the Eclipse Plugin and Software Security Center also had to be manually reconfigured with the same custom audit labels and values.
When you open a version 4.5.1 or earlier FPR file, the Migration Wizard automatically starts. You must map your old audit data into the new custom tags feature. HP recommends that you create version 5.0 custom tag and filter sets before you map the old auditing data into the new format. Make sure that you migrate the issue IDs before you migrate the audit data.

To migrate audit information:

1. Open the FPR format version 4.5.1 or earlier as described in *Opening Projects*.
   - A backup of the old FPR is automatically saved. The Migration Wizard starts.
2. (Optional) Select a migration template file.
3. Click **Next**.
   - The wizard displays the Migrate Analysis Values step.
4. Map the old analysis values to the new values.
5. (Optional) Select **Use Project Template**, and then select an FPR file with the project template to apply.
6. Click **Next**.
   - The Migration Summary dialog box opens.
7. (Optional) To save the migration settings in a file, leave the **Save migration settings** check box selected. The default file is `<eclipse_install_directory>/core/config/migration-settings.properties`.
8. Click **Finish**.
   - If the scan was performed on another machine, you are prompted to indicate whether you want to update the source files location.
9. Update the location, and then click **OK**.

![Migration Wizard](image-url)
Merging Audit Data

Audit data are the custom tags and comments that were added to an issue. You can merge the audit data for your project with audit data from another results file. Comments are merged into a chronological list and custom tag values are updated. If custom tag values conflict (if the same tag is set to different values for a given issue), the Eclipse Plugin prompts you to resolve it.

Note: Issues are not merged. Merged results include only the issues found in the latest scan. Issues uncovered in the older scan that were not uncovered in the latest scan are marked as Removed and are hidden by default.

Make sure that the projects you merge contain the same analysis information. That is, make sure that the scans were performed on the same source code (no missing libraries or files) using the same security content and the same SCA options.

To merge projects:
1. Open a project in Eclipse Plugin.
   The Audit window opens.
2. Select Tools → Merge Audit Projects.
   The Choose an SCA Analysis File dialog box opens.
3. Select an FPR file, and then click Open.
   The Progress Information dialog box opens. When complete, the Merge dialog box opens.
4. Click OK to confirm the number of issues added or removed from the file.
   Note: If the scan is identical, no issues are added or removed.

The project now contains all audit data from both result files.

Uploading Results to HP Fortify Software Security Center

You can upload results to Software Security Center.

To upload results to Software Security Center:
1. Select Options → Options.
   The Options dialog box opens.
2. Click Server Configuration.
3. Specify Server URL for Software Security Center, such as http://111.0.0.1:8181.
4. Click Get New Key.
5. Enter Software Security Center logon information.
6. Click OK.
7. Select Tools → Upload Audit Project.
   A dialog box lists the current projects.
8. Select an existing project, and then click OK.

The plugin displays a message to notify you after the upload is completed.
About Security Content

HP Fortify security content consists of Secure Coding Rulepacks and external metadata. The external metadata include mappings from the HP Fortify categories to alternative categories (such as OWASP 2010, PCI 1.2, and CWE). You can modify the existing mapping in the external metadata document (externalmetadata.xml) or create your own files to map HP Fortify issues to different taxonomies, such as internal application security standards or additional compliance obligations (recommended).

Use any XML editor to make your changes or create a new document. (The existing mapping file is located in the `<SCA_and_Apps_Install>\Core\config\ExternalMetadata` directory.) HP Fortify recommends that you save your new or modified document to the `<SCA_and_Apps_Install>\Core\config\CustomExternalMetadata` directory so that your changes are not lost during security content updates.

To validate a modified or new mapping, use the `externalmetadata.xsd` file, which is located in the `<SCA_and_Apps_Install>\Core\config\schemas` directory. HP recommends that, after you change your mapping document, you open the FPR file in the plugin to see how the mapping works with the scan results.

If you change the external metadata document or create a new mapping document, be sure to make the same changes on Software Security Center.

If you updated security content from AWB, there is No need to update it separately from the Eclipse Plugin.

About Updating Security Content

You can obtain the latest security content by doing one of the following:

- Configure the Security Content update server
- Poll the security content update server for scheduled updates.
- Manually copy any custom rules to the `<SCA_and_Apps_Install>\Core\config\customrules` directory.
- Manually copy any custom external metadata files to the `<SCA_and_Apps_Install>\Core\config\CustomExternalMetadata` directory.

Updating Security Content

**Note:** When you update security content, any changes you have made to the your previous security content are overwritten.

To update your security content:

1. Select **HP Fortify → Options**.
   
   The Options dialog box opens.
2. In the left panel, select **Security Content Management**.
3. Click **Update Security Content**, and then click **OK**.
Configuring Security Content Updates

If the analysis plugin component is installed, you can specify the server information to use to update security content.

To configure the security content update server:

1. Select **HP Fortify → Options**.
   The Options dialog box opens.

2. In the left panel, select **Server Configuration**.

3. In the **Security Content Update Configuration** section, provide the server URL, and, if required, the proxy server and port.

4. To update security content automatically and with a specific frequency:
   a. Select the **Perform Security Content Update Automatically** check box.
   b. In the **Security Content Update Frequency (Days)** box, specify how often (type the number of days) you want the security content automatically updated.
About Advanced Configuration

This section provides information about using the Audit Guide in advanced mode and how to integrate the Eclipse Plugin with a bug tracking system.

Using the Audit Guide in Advanced Mode

You can use the Audit Guide during an audit to manage the way the issues are filtered in the results.

To use the Audit Guide:

1. Open an FPR file or other scan results file in Eclipse (select **HP Fortify → Open Audit Project**).
2. Select **HP Fortify → Audit Guide**.
   
   The Audit Guide wizard starts.
3. Click **Advanced Mode**.

![Audit Guide Questions](image)

4. In the **Audit Guide Questions** list, select the check boxes for the types of issues to filter out and ignore.
   
   To see a description of an issue type, click its name. The Audit Guide displays a description to the right of the list. The Audit Guide also displays the filter details for the issue type in the **Filters** table, including the number of issues that match each filter.

5. To apply your settings, click **OK**.
About Bug Tracking System Integration

Eclipse Plugin provides a plugin interface for integrating with defect tracking systems. This enables you to file bugs directly from the Eclipse Plugin. The Eclipse Plugin supports Bugzilla and HP Quality Center (HPQC) bug tracking systems.

Integrating with Bugzilla

An example plugin is provided for Bugzilla ([www.bugzilla.org](http://www.bugzilla.org)). To select the plugin to use, select Options → Configure Bugtracker Integration.

Source code for the Bugzilla plugin is available in the following directory:

<fortify_install>/Samples/advanced/Bugzilla

To write your own plugin, see the instructions in the README.txt file, which is located in the bugtracker directory.

Integrating with HP Quality Center

Eclipse Plugin supports integration with HP Quality Center (HPQC) bug system.

To configure the secure code plugin to integrate with HPQC:

1. Click Options.
2. Select Configure Bugtracker Integration.
3. In the Configure Bugtracker Integration dialog box, select HPQC from the list.
4. Click OK.
About Troubleshooting Problems with the Eclipse Plugin

This section provides information about how to resolve the "Java.lang.OutOfMemory" error and scan failures resulting from insufficient memory. It also includes instructions on how to use the debugging option.

Resolving the Java.lang.OutOfMemory Message

If you see the java.lang.OutOfMemory message while managing security content or while loading a large HP Fortify source code analysis results file, adjust the JVM size of the virtual machine for your IDE.

To adjust the JVM size, restart the IDE as follows:

eclipse.exe -vmargs -Xmx<nnn>M

where <nnn> is the amount of memory you are allocating to the IDE. For example, to allocate 300 MB to the IDE, enter -Xmx300M.

If you specify this option, make sure that you do not allocate more memory than is physically available. As a guideline, assuming no other memory-intensive processes are running, allocate no more than two thirds of the available memory.

Note: The JVM fails to launch if you allocate more than 2 GB.

Resolving Scan Failures Due to Insufficient Memory

If you run out of memory during a scan, configure project properties settings to increase the memory for that scan. (See About Scan and Analysis Settings on page 14.)

Using the Debugging Option

If you encounter errors, you can enable the debugging option to help troubleshoot.

To enable debugging:

1. Navigate to the <Eclipse_Install>\Core\config directory and open the fortify.properties file.
2. Remove the comment tags from the lines in the following section and change all values to true:

# when set to true will place all the thick tools and SCA into debug mode
#com.fortify.Debug=false
# to selectively place a thick tool into debug mode (unnecessary if com.fortify.Debug is set to true)
#com.fortify.awb.Debug=false
#com.fortify.eclipse.Debug=false
#com.fortify.VS.Debug=false

For help diagnosing the problem, send the log files to HP Fortify Software.

On Windows systems, log files are located in one of the following directories:

C:\Documents and Settings\<username>\Local Settings\Application Data\Fortify\sca<version>\log\sca.log
C:\Documents and Settings\<username>\Local Settings\Application Data\Fortify\Eclipse.Plugin-<version>\log\SCAPlugin.log

On Linux and UNIX systems, log files are located in one of the following directories:

<userhome>/.fortify/sca<version>/log/sca.log
<user.home>/.Fortify/Eclipse.Plugin-<version>/log\SCAPlugin.log