Legal Information

Book Name: FlexNet Code Insight 2020 R1 User Guide
Part Number: FNCI-2020R1-UG00
Product Release Date: February 2020

Copyright Notice

Copyright © 2020 Flexera

This publication contains proprietary and confidential information and creative works owned by Flexera and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera, must display this notice of copyright and ownership in full.

FlexNet Code Insight incorporates software developed by others and redistributed according to license agreements. Copyright notices and licenses for these external libraries are provided in a supplementary document that accompanies this one.

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see https://www.flexerasoftware.com/legal/intellectual-property.html. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.
## Contents

1. **FlexNet Code Insight 2020 R1 User Guide** ......................................................... 11
   - Intended Audience .................................................................................. 12
   - Contacting Us ......................................................................................... 12

2. **Using FlexNet Code Insight** ........................................................................ 13
   - Opening FlexNet Code Insight ................................................................ 14
     - Viewing Online Help and Online Guides ............................................. 15
     - Changing Your Password .................................................................... 15
   - Roles and Permissions in FlexNet Code Insight .................................... 15
   - What is a Code Insight Project? ............................................................... 16
     - Key Project Elements .......................................................................... 16
     - Common Project Configurations ....................................................... 16
   - Creating a Project .................................................................................... 17
   - What Is a FlexNet Code Insight Scan? ................................................... 18
   - Applying a Scan Profile to the Project .................................................... 19
     - About Scan Profiles ............................................................................ 19
     - Applying a Scan Profile ...................................................................... 19
   - Selecting Materials to Scan .................................................................... 20
     - Uploading a Project Codebase .............................................................. 20
     - Uploading the Codebase ..................................................................... 20
     - Supported Archive Types for Expansion ........................................... 21
     - More About Archive Expansion Behavior During Codebase Uploads  22
   - Scanning the Codebase .......................................................................... 24
   - Overview of Scan Results ...................................................................... 25
     - Inventory .............................................................................................. 25
     - Review Status of Inventory ................................................................. 26
     - Inventory Priority ................................................................................ 26
     - Inventory Confidence ......................................................................... 27
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Vulnerabilities Associated with Inventory</td>
<td>28</td>
</tr>
<tr>
<td>Inventory Usage Information</td>
<td>31</td>
</tr>
<tr>
<td>Scan Evidence</td>
<td>32</td>
</tr>
<tr>
<td>License Information Associated with Inventory</td>
<td>33</td>
</tr>
<tr>
<td>License Details from the Code Insight Data Library</td>
<td>33</td>
</tr>
<tr>
<td>License Priority</td>
<td>34</td>
</tr>
<tr>
<td>Reporting of Detected License Text through the As-Found Text Inventory Field</td>
<td>35</td>
</tr>
<tr>
<td>Notices Text</td>
<td>37</td>
</tr>
<tr>
<td><strong>Analyzing (Auditing) Scan Results</strong></td>
<td>38</td>
</tr>
<tr>
<td>Opening the Analysis Workbench</td>
<td>38</td>
</tr>
<tr>
<td>The Analysis Workbench Layout</td>
<td>39</td>
</tr>
<tr>
<td>Searching for Codebase Files Based on Name</td>
<td>40</td>
</tr>
<tr>
<td>Searching for Codebase Files Based on Search Criteria</td>
<td>41</td>
</tr>
<tr>
<td>Creating and Editing File Searches</td>
<td>41</td>
</tr>
<tr>
<td>Creating a New File Search</td>
<td>41</td>
</tr>
<tr>
<td>Editing a File Search</td>
<td>43</td>
</tr>
<tr>
<td>Copying a File Search</td>
<td>43</td>
</tr>
<tr>
<td>Deleting a File Search</td>
<td>44</td>
</tr>
<tr>
<td>Using the Filter Legend Options to Filter the Codebase</td>
<td>44</td>
</tr>
<tr>
<td>Using the Codebase Files Pane Context Menu</td>
<td>46</td>
</tr>
<tr>
<td>Marking Files as Reviewed</td>
<td>46</td>
</tr>
<tr>
<td>Viewing Details for Licenses Associated with Codebase Files</td>
<td>46</td>
</tr>
<tr>
<td>Using the File Details Tab</td>
<td>48</td>
</tr>
<tr>
<td>Viewing the Evidence Summary for a File</td>
<td>48</td>
</tr>
<tr>
<td>Viewing Binary Strings in a File</td>
<td>49</td>
</tr>
<tr>
<td>Viewing Copyright, Email, URL, and License Evidence in a File</td>
<td>49</td>
</tr>
<tr>
<td>Viewing Exact Matches</td>
<td>50</td>
</tr>
<tr>
<td>Viewing Source Matches</td>
<td>51</td>
</tr>
<tr>
<td>More About the “Remote Files” Panels on the Exact or Partial Matches Tabs</td>
<td>52</td>
</tr>
<tr>
<td>Adding a Partial or Exact Match Codebase File to an Inventory Item Based on an Associated Component</td>
<td>54</td>
</tr>
<tr>
<td>Using the Evidence Details Tab</td>
<td>55</td>
</tr>
<tr>
<td>Using the Inventory Details Tab</td>
<td>55</td>
</tr>
<tr>
<td>Using the Inventory Items Context Menu</td>
<td>55</td>
</tr>
<tr>
<td>Viewing Security Vulnerabilities for Inventory in Analysis Workbench</td>
<td>56</td>
</tr>
<tr>
<td>Viewing Details About Licenses Associated with Inventory in Analysis Workbench</td>
<td>57</td>
</tr>
<tr>
<td>Viewing or Editing Inventory Usage Information from Analysis Workbench</td>
<td>57</td>
</tr>
<tr>
<td>Viewing and Updating Detection and Auditing Notes in Analysis Workbench</td>
<td>58</td>
</tr>
<tr>
<td>Component Lookup</td>
<td>58</td>
</tr>
<tr>
<td>Guidelines for Component Lookup</td>
<td>58</td>
</tr>
<tr>
<td>Component Lookup Results</td>
<td>59</td>
</tr>
<tr>
<td>Performing Component Lookup</td>
<td>59</td>
</tr>
<tr>
<td>Creating an Inventory Item from the Analysis Workbench</td>
<td>60</td>
</tr>
<tr>
<td>Creating Inventory from the Inventory Items List</td>
<td>60</td>
</tr>
<tr>
<td>Creating Inventory from the Codebase Lists</td>
<td>62</td>
</tr>
<tr>
<td>Editing Inventory from the Analysis Workbench</td>
<td>64</td>
</tr>
</tbody>
</table>
Contents

Publishing or Recalling Inventory from Analysis Workbench .............................................. 64

Reviewing Published Inventory ......................................................................................... 66
  Goal of the Reviewer ......................................................................................................... 67
  Displaying Project Inventory .......................................................................................... 67
  Searching Published Inventory ........................................................................................ 67
  Viewing Security Vulnerabilities for Project Inventory ..................................................... 69
  Viewing Details About the Licenses Associated with Project Inventory ......................... 69
  Viewing and Updating Notes and Guidance .................................................................... 70
  Viewing Usage Information for Project Inventory ............................................................ 71
  Creating Inventory from the Project Inventory Tab .......................................................... 72
  Editing Inventory from the Project Inventory Tab ............................................................. 74
  Approving or Rejecting Inventory Items ......................................................................... 75
  Creating and Managing Tasks for Project Inventory ........................................................ 75
  Creating and Editing Custom Components ...................................................................... 86
  Creating a Custom License ............................................................................................... 97
  Supported Forge-URL Domains for Custom-Component Creation .................................. 97

Managing Security Vulnerability Alerts .......................................................................... 81
  Accessing Security Vulnerability Alerts ......................................................................... 82
  Using the Alerts Dialog to Manage Alerts ...................................................................... 84
  Alert Details ................................................................................................................... 84
  Changing the Priority of an Alert .................................................................................... 86
  Changing the Status of an Alert ....................................................................................... 86

Creating and Editing Custom Components ..................................................................... 86
  Creating a Custom Component ....................................................................................... 87
  Step 1: Access the Component Lookup Feature ............................................................ 87
  Step 2: Create the Custom Component ......................................................................... 87
    Create the Custom Component Based on a Keyword in Its Name or Title ................... 88
    Create the Custom Component Based on Its Project or Forge URL ......................... 89
    Create the Custom Component Based on Its Forge ..................................................... 91
    Create the Custom Component in Free Form ............................................................. 92
  Step 3: Associate an Instance of the Custom Component with the Inventory Item ........... 93
  Editing a Custom Component ........................................................................................ 94
  Custom Component Properties ....................................................................................... 95
  Supported Forge-URL Domains for Custom-Component Creation ............................... 97

Creating and Editing Custom Licenses ......................................................................... 97
  Creating a Custom License ............................................................................................. 97
  Step 1: Initiate the Creation of a Custom License ............................................................ 98
    When Using Component Lookup to Register a Component Instance for a “component” Inventory Item ......................................................... 98
    When Selecting a New License for an Existing Inventory Item .................................. 99
    When Creating or Editing a “License Only” Inventory Item ....................................... 100
## Contents

### Accessing and Viewing Projects in the System
- Navigating to the Projects List ......................................................... 111
- Using the Project Dashboard ............................................................. 112
  - Filtering Inventory for a Project from the Project Dashboard ............ 114
- Opening a Project ............................................................................ 114
- Showing Only Your Projects .............................................................. 115
- Searching the System ...................................................................... 115
  - Available Filters for Searching Across Projects ............................. 116
  - Searching for Projects by Name ...................................................... 117
  - Searching All Projects for Inventory Based on a Specific Component and Version ...................................................... 118
  - Searching All Projects for Inventory Associated with a Specific License ...................................................... 119
  - Searching All Projects for a Security Vulnerability Advisory .......... 119
  - Restoring the Full Project List .......................................................... 120
- Managing Items in the Project List .................................................. 121

### Managing a Project from the Summary Tab
- Opening the Project Summary Tab .................................................... 122
- Generating Reports ......................................................................... 122
  - The Project Report ....................................................................... 122
  - The Audit Report ......................................................................... 123
  - The Notices Report ...................................................................... 123
    - Generating the Notices Report ..................................................... 124
- Custom Reports ............................................................................... 124
- Assigning Project Roles to Users ...................................................... 125
- Editing the Project Definition and General Settings .......................... 126
- Updating Scan Settings for a Project ................................................. 126
- Automatically Publishing Inventory .................................................. 126
- Updating Inventory Review and Remediation Settings for a Project .... 127
- Connecting the Project to Remote Data Sources ............................... 128
  - Version Control Settings ............................................................... 128
  - ALM Settings ............................................................................. 128
- Changing Project Owners .................................................................. 131
- Rescanning Your Codebase .............................................................. 131
  - Change Events Resulting in Full or Incremental Rescans ................. 132
  - Effects of Scan-Setting Changes on Rescans ................................. 133

### Managing Custom Detection Rules
- Creating a Custom Detection Rule .................................................... 104
  - Creating a Custom Detection Rule from Inventory of “Component” Type ...................................................... 104
  - Creating a Custom Detection Rule from Scratch ......................... 106
- Viewing All Current Custom Detection Rules .................................... 106
- Editing a Custom Detection Rule ...................................................... 107
- Deleting a Custom Detection Rule .................................................... 107
- Rule-Processing Considerations ....................................................... 107

### Finalizing the Notices Text for the Notices Report
- Step 2: Create the Custom License ................................................... 100
- Editing a Custom License ................................................................ 101
- Custom License Properties ............................................................. 102

### Generating Reports
- Searching All Projects for Inventory Associated with a Specific License ...................................................... 119
- Searching All Projects for a Security Vulnerability Advisory .......... 119
- Restoring the Full Project List .......................................................... 120
- Managing Items in the Project List .................................................. 121

### The Notices Report
- The Audit Report ......................................................................... 123
- The Notices Report ...................................................................... 123
  - Generating the Notices Report ..................................................... 124
- Custom Reports ............................................................................... 124
- Assigning Project Roles to Users ...................................................... 125
- Editing the Project Definition and General Settings .......................... 126
- Updating Scan Settings for a Project ................................................. 126
- Automatically Publishing Inventory .................................................. 126
- Updating Inventory Review and Remediation Settings for a Project .... 127
- Connecting the Project to Remote Data Sources ............................... 128
  - Version Control Settings ............................................................... 128
  - ALM Settings ............................................................................. 128
- Changing Project Owners .................................................................. 131
- Rescanning Your Codebase .............................................................. 131
  - Change Events Resulting in Full or Incremental Rescans ................. 132
  - Effects of Scan-Setting Changes on Rescans ................................. 133

### Custom License Properties
- Creating a Custom Detection Rule from Scratch ............................. 106
- Creating a Custom Detection Rule from Inventory of “Component” Type ...................................................... 104
- Creating a Custom Detection Rule from Scratch ......................... 106

### Operations Related to Projects
- Rescanning Your Codebase .............................................................. 131
5 Automated Analysis ................................................................. 169
   What is Automated Analysis? ................................................. 169
   Supported Development Ecosystems ........................................ 169
      Supported Ecosystems ...................................................... 170
      Notes About Ecosystem Support ......................................... 171
      Notes about Dependencies Support ...................................... 173
   Supported Archive Formats ................................................... 173
   Additional Rule-based Detection Capabilities ............................. 173

6 Performing Inventory-Only Scanning ....................................... 175
   Inventory-Only Scan .......................................................... 175
   Creating a Project Without Uploading a Codebase ....................... 175
   FlexNet Code Insight Plugins .............................................. 176

7 Configuring Source Code Management ..................................... 179
   Managing Source Code Management (SCM) Instances ................... 179
      Prerequisites .................................................................... 179
      Adding an SCM Instance to the Code Insight Project ................. 180
      Testing an SCM Instance .................................................. 180
      Synchronizing an SCM Instance .......................................... 180
      Deleting an SCM Instance .................................................. 181
      Configuring a Git SCM Instance .......................................... 181
         Adding a Git SCM Instance to the Code Insight Project ........... 181
         Fields Used to Configure a Git SCM Instance ....................... 182
      Configuring a Perforce SCM Instance .................................... 182
         Adding a Perforce SCM Instance to the Code Insight Project ....... 182
         Fields Used to Configure a Perforce SCM Instance .................. 183
      Configuring a TFS SCM Instance ......................................... 184
         Adding a TFS SCM Instance to the Code Insight Project .......... 184
         Fields Used to Configure a TFS SCM Instance ....................... 185

8 Pages and Panels ................................................................. 187
   The FlexNet Code Insight Dashboard ....................................... 188
   Users/Permissions Tab ......................................................... 189
   Add User Dialog .................................................................... 190
   Edit User Dialog .................................................................... 191
   Electronic Updates Tab .......................................................... 192
      Overview of Electronic Update Setup ...................................... 192
      Field Descriptions ............................................................ 193
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Server Tab</td>
<td>195</td>
</tr>
<tr>
<td>LDAP Tab</td>
<td>196</td>
</tr>
<tr>
<td>ALM Tab</td>
<td>200</td>
</tr>
<tr>
<td>Scan Servers Tab</td>
<td>202</td>
</tr>
<tr>
<td>Scan Server Dialog</td>
<td>203</td>
</tr>
<tr>
<td>Scan Profiles Tab</td>
<td>207</td>
</tr>
<tr>
<td>Create/Edit Scan Profile Dialog</td>
<td>208</td>
</tr>
<tr>
<td>Project Defaults Tab</td>
<td>210</td>
</tr>
<tr>
<td>System Settings Tab</td>
<td>217</td>
</tr>
<tr>
<td>Projects List Page</td>
<td>217</td>
</tr>
<tr>
<td>Project Summary Tab</td>
<td>219</td>
</tr>
<tr>
<td>Edit Project: General Tab</td>
<td>224</td>
</tr>
<tr>
<td>Edit Project: Scan Settings Tab</td>
<td>226</td>
</tr>
<tr>
<td>Edit Project: Review and Remediation Settings Tab.</td>
<td>228</td>
</tr>
<tr>
<td>Edit (Default) Project Users Page</td>
<td>233</td>
</tr>
<tr>
<td>Scan History Dialog</td>
<td>234</td>
</tr>
<tr>
<td>Select a New Project Owner Page</td>
<td>235</td>
</tr>
<tr>
<td>Analysis Workbench</td>
<td>236</td>
</tr>
<tr>
<td>File Search Results Pane</td>
<td>237</td>
</tr>
<tr>
<td>Advanced File Search Dialog</td>
<td>238</td>
</tr>
<tr>
<td>Advanced File Search Add Dialog</td>
<td>239</td>
</tr>
<tr>
<td>Inventory Details Pane in Analysis Workbench</td>
<td>239</td>
</tr>
<tr>
<td>Evidence Details Pane</td>
<td>245</td>
</tr>
<tr>
<td>Project Inventory Review Page</td>
<td>245</td>
</tr>
<tr>
<td>Project Inventory Details Pane</td>
<td>247</td>
</tr>
<tr>
<td>Policy Page</td>
<td>253</td>
</tr>
<tr>
<td>Policy Details Page</td>
<td>254</td>
</tr>
<tr>
<td>Impact on Policies When CVSS Version Changes on System</td>
<td>258</td>
</tr>
<tr>
<td>Custom Detection Rules Tab</td>
<td>258</td>
</tr>
<tr>
<td>Custom Detection Rule Dialog</td>
<td>260</td>
</tr>
<tr>
<td>Edit Custom Rule Dialog</td>
<td>262</td>
</tr>
<tr>
<td>License Details Window</td>
<td>264</td>
</tr>
<tr>
<td>Lookup Component Window</td>
<td>265</td>
</tr>
<tr>
<td>Add Project Dialog</td>
<td>266</td>
</tr>
<tr>
<td>Preferences Page</td>
<td>267</td>
</tr>
<tr>
<td>Add Token Dialog</td>
<td>268</td>
</tr>
<tr>
<td>Edit Token Dialog</td>
<td>269</td>
</tr>
<tr>
<td>Advanced Inventory Search Dialog</td>
<td>270</td>
</tr>
<tr>
<td>Import Project Data Dialog</td>
<td>276</td>
</tr>
</tbody>
</table>
A  FlexNet Code Insight User Roles and Permissions .................................................. 279
   System Roles and Permissions .................................................................................... 279
   Project Roles and Permissions ................................................................................... 281
   Roles and Permissions to Manage Project Task Flow .................................................. 283
FlexNet Code Insight empowers organizations to take control of and manage their use of open source software (OSS) and third-party components. It helps development, legal, and security teams use automation to create a formal OSS strategy that balances business benefits and risk management.

The *FlexNet Code Insight User Guide* describes how to use FlexNet Code Insight to realize these benefits. The guide includes the following sections.

**Table 1-1 • FlexNet Code Insight User Guide**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using FlexNet Code Insight</td>
<td>“How to” information for using Code Insight functionality.</td>
</tr>
<tr>
<td>Performing Advanced Searches</td>
<td>Overview and procedures for using advanced searches to find specific inventory.</td>
</tr>
<tr>
<td>Exporting and Importing Project Data</td>
<td>Explanation and procedures for exporting and importing project data.</td>
</tr>
<tr>
<td>Automated Analysis</td>
<td>Information about Code Insight automated analysis tools and features.</td>
</tr>
<tr>
<td>Performing Inventory-Only Scanning</td>
<td>Information about the Code Insight agent scan, performed remotely.</td>
</tr>
<tr>
<td>Pages and Panels</td>
<td>Reference to field descriptions on the pages, panes, tabs, and dialogs used in the Code Insight user interface.</td>
</tr>
<tr>
<td>FlexNet Code Insight User Roles and Permissions</td>
<td>A reference to the various user roles and permissions available in Code Insight to control access to Code Insight functionality.</td>
</tr>
</tbody>
</table>
Intended Audience

The *FlexNet Code Insight User Guide* is intended for anyone who uses FlexNet Code Insight for scanning, analyzing, and reviewing project codebases.

Contacting Us

Flexera is headquartered in Itasca, Illinois, and has offices worldwide. To contact us or to learn more about our products, visit our website at:

https://www.flexerasoftware.com/about-us/contact-us.html

For FlexNet Code Insight support, visit the following webpage, which includes all relevant details, including access to the Customer Community, online web form, and phone numbers:

https://flexeracommunity.force.com/customer/
Using FlexNet Code Insight

This chapter provides basic information about FlexNet Code Insight that will enable you to start using the product effectively. The following topics are covered in this section:

- Opening FlexNet Code Insight
- Roles and Permissions in FlexNet Code Insight
- What is a Code Insight Project?
- Creating a Project
- What Is a FlexNet Code Insight Scan?
- Applying a Scan Profile to the Project
- Selecting Materials to Scan
- Scanning the Codebase
- Overview of Scan Results
- What Does an Analyst do?
- Analyzing (Auditing) Scan Results
- Reviewing Published Inventory
- Managing Security Vulnerability Alerts
- Creating and Editing Custom Components
- Creating and Editing Custom Licenses
- Managing Custom Detection Rules
- Finalizing the Notices Text for the Notices Report
- Accessing and Viewing Projects in the System
- Managing a Project from the Summary Tab
- Creating a Private Project
Opening FlexNet Code Insight

FlexNet Code Insight runs in your web browser. This section explains how to start FlexNet Code Insight and access the Dashboard.

Note • If this is the first time you have opened FlexNet Code Insight or if you have recently upgraded FlexNet Code Insight or shut down your Tomcat server, you must start up the Tomcat server with the startup command before opening FlexNet Code Insight. For more information, see “Starting and Stopping Tomcat” in the “Installing FlexNet Code Insight” chapter in the “FlexNet Code Insight Installation and Configuration Guide”.

Task To open FlexNet Code Insight, do the following:

1. Launch a web browser and navigate to: http://<your_server_host_name>:8888/codeinsight.

Note • If you are unsure about your server host name, contact your system administrator for guidance.

2. Enter your Code Insight credentials in the Username and Password fields.

Note • The default login name is admin, the default password is Password123. Your installation might require a different login name and password. If you are unsure about what credentials to enter, contact the Code Insight Administrator for guidance.

3. Click Login. The FlexNet Code Insight Dashboard appears:
Notes • The statistics displayed on the Dashboard are from scans that were run on your codebases.

Viewing Online Help and Online Guides

FlexNet Code Insight provides online help topics and online versions of its guides so you can find answers to your questions about the product while you are using it.

<table>
<thead>
<tr>
<th>Task</th>
<th>To access online help and guides, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>To access the online help, click the Help icon ( ) from any page in the product. Help is displayed for that page.</td>
</tr>
<tr>
<td>2.</td>
<td>To access the online guides, click the Open Menu icon ( ) and select HELP from the menu. A list of available online documentation appears.</td>
</tr>
</tbody>
</table>

Changing Your Password

If you want to change your current FlexNet Code Insight password, use this procedure.

<table>
<thead>
<tr>
<th>Task</th>
<th>To change your current Code Insight password, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click the Open Menu icon in the upper right of any FlexNet Code Insight page:</td>
</tr>
<tr>
<td>2.</td>
<td>Select Preferences to open the Preferences page.</td>
</tr>
<tr>
<td>3.</td>
<td>Enter your new password in New Password, and then reenter it in New Password Confirm.</td>
</tr>
<tr>
<td>4.</td>
<td>Click Update Password.</td>
</tr>
</tbody>
</table>

Roles and Permissions in FlexNet Code Insight

FlexNet Code Insight offers a set of user roles and permissions that enables your site to control access to Code Insight features and functionality. The initial Code Insight Administrator can assign system-level roles to users, including roles to manage Code Insight policies and to create and manage Code Insight projects. An Administrator can also assign the Administrator role to other users. Project Owners can assign project-specific roles to users to analyze and review project scan results and can also transfer project ownership to another user.

The FlexNet Code Insight User Roles and Permissions appendix serves as a reference to the various Code Insight roles available and the permissions granted to each role. As you prepare use the Code Insight, refer to this appendix to determine the roles required to perform certain Code Insight functionality and the permissions the roles enable.
What is a Code Insight Project?

A project represents the scan and analysis of a codebase and related artifacts. Typically, you would create a project for each one of your products or services, but you might also create projects to review vendor code for security or licensing issues, to screen an open-source component you are considering using, or to prepare for an open-source contribution.

For added flexibility, you can group projects in project folders that represent business units, teams, product lines, tools, or any other groupings that help you locate projects more easily. The folders can be nested to the desired level.

All projects have the same basic key elements but use various configurations, as described in these next sections:

- **Key Project Elements**
- **Common Project Configurations**

**Important** • You can create projects only if the Administrator has granted you permission to do so, as described in the “FlexNet Code Insight Installation and Configuration Guide”.

Key Project Elements

The following key elements of a project are important to keep in mind when creating, configuring, and organizing projects:

- **Materials to scan or analyze**—Each project has an uploaded codebase or a configured remote scan location (such as on a build server, artifact repository, or version control system).

- **Scan profile**—Each project has an associated scan profile with a set of scan settings that are applied when the project is scanned. (The profile can be one of the default scan profiles or a custom scan profile).

- **Policy profile**—Each project has an associated policy profile with a set of intellectual property or security policies that are applied when project inventory is published to the project (such as during the first scan or when manually published by a project user).

- **Project visibility**—Each project has an associated visibility configuration that specifies which logged-in users have the ability to view or change the project.

Common Project Configurations

These are some examples of common project configurations:

- **Project to scan source code**—The project is configured for a local scan with code that is uploaded to the Scan Server or synchronized to the server through a Version Control System. The selected scan profile performs a full analysis of the source—including searches for exact matches of entire files and for partial source-code matches (fingerprints)—and processes files inside archives.

- **Project to scan build output or binaries**—The project is configured for a remote system scan using one of the scan agent plugins. The selected scan profile performs Automated Analysis and processes dependencies to generate inventory, but does not perform a full analysis of the source. This scan profile can also be selected for a local scan.
Creating a Project

You must create a project in FlexNet Code Insight before you can scan data and generate reports. Use the following procedure to create a project.

**Important** • You can create projects only if the Administrator has granted you permission to do so, as described in the “Configuring FlexNet Code Insight” chapter in the “FlexNet Code Insight Installation and Configuration Guide”. The **Add New** button referenced in the following procedure is available only if you have this permission.

Task  **To create a project, do the following:**

1. Click the **Open Menu** icon in the upper right of any FlexNet Code Insight page:

2. Select **Projects** from the menu. The Projects page appears. In FlexNet Code Insight, a **project** represents an application version or release that contains a codebase to be scanned.

3. Click **Add New** and select **Project** from the pulldown menu. The **Add Project** dialog appears.

4. Complete the following fields on the **Add Project** dialog:
   - **Name**—Type a name for the new project.
   - **Project Type**—From the dropdown menu, select the type of scan that will be run on this project:
     - **Standard**—This is the default scan type. It requires that you upload your codebase to FlexNet Code Insight Scan Server or configure version-control settings to synchronize the codebase to the server. Refer to **Selecting Materials to Scan** in this chapter for information about uploading your codebase or to the **Configuring Source Code Management** chapter for information about synchronizing your codebase with the server.
     - **Inventory Only**—This type of scan allows for remote scanning and does not require a codebase on the FlexNet Code Insight Scan Server. To learn more about inventory-only projects, see the **Performing Inventory-Only Scanning** chapter.
   - **Project Visibility**—Select one of the project visibility options from the dropdown menu:
     - **Public**—All users in the system can view and change the project. This is the default value for this field.
     - **Private**—For more information on private projects, see **Creating a Private Project**.
What Is a FlexNet Code Insight Scan?

The FlexNet Code Insight Scan Server performs a static analysis of files of any type (source or binary) to find open source and third-party components, licenses, and security vulnerabilities and to identify file-level and snippet-level evidence to aid users in determining the origin of every file in the codebase. The end goal of the Insight scan is to build the most accurate Bill of Materials and to eliminate the security and intellectual property (IP) risk associated with the materials.

During a codebase scan, FlexNet Code Insight processes every file in the materials, regardless of programming language or file type. It processes source materials, scripts, object code, binaries, images, icons, and documents to identify both open source and closed source components, licenses, and security vulnerabilities. Code Insight identifies these elements using a combination of Automated Analysis and Advanced Analysis techniques:

- **Automated Analysis**—The Scan Server uses automated detection rules to identify components, versions, licenses, and security vulnerabilities. In applying these rules, the Scan Server automatically generates inventory items that make up the Bill of Materials. The rules are found in the Code Insight data library, which is updated on your Code Insight server through both an internal process and as part of the weekly Electronic Update. For more about Automated Analysis, see the Automated Analysis chapter.

- **Advanced Analysis**—The Scan Server uses advanced analysis techniques to detect copyrights, emails, URLs, search terms, exact files, and source-code fingerprints (snippets) that match those found in third-party or open-source code. Advanced Analysis requires the FlexNet Code Insight Compliance Library (CL), downloaded from the Product and License Center. The CL is a database used by the Scan Server to perform exact-file and source-code fingerprint (snippet) matching. Code Insight compares elements of scanned codebase files with information contained in the CL to generate file-level evidence on which you can take action.
Applying a Scan Profile to the Project

FlexNet Code Insight supports scan profiles for abstracting and reusing scan settings. Often, organizations are concerned about consistent scan or audit practices across their enterprise, and scan profiles support that need. The following describes scan profiles and how to create one:

- About Scan Profiles
- Applying a Scan Profile

About Scan Profiles

FlexNet Code Insight includes the following default scan profiles:

- **Basic Scan profile (without a CL)**—Used to produce automated findings along with string-based third-party indicators at a file level. This profile disables both exact-file and source-code matching, and therefore does not require a Compliance Library (CL).
- **Standard Scan profile**—Expands the file-level third-party indicators with exact-file matches based on the Compliance Library.
- **Comprehensive Scan profile**—Further expands the file-level third-party indicators with exact file-level and source-code matches based on the Compliance Library.

Additional scan profiles can be defined by the application administrator for use across projects, as described in the *FlexNet Code Insight Installation & Configuration Guide*.

Applying a Scan Profile

The scan profile is used to abstract and reuse scan settings across projects. The scan profile currently selected for a project shows in the Scan Settings section on the Summary tab. The scan settings specified in the current scan profile are applied for each project scan. However, if you want to apply a different scan profile to the project, follow these steps.

You must be Project Owner to apply a scan profile to a project.

<table>
<thead>
<tr>
<th>Task</th>
<th>To select a new scan profile, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>From the list of projects, select the project for which you want to apply a scan profile.</td>
</tr>
<tr>
<td></td>
<td>(Optional) Click the <strong>My Projects</strong> toggle at the top of the list to show only those projects with which you are associated as Project Owner or through a project role. (For details, see <strong>Showing Only Your Projects.</strong>) You can also search projects by name, inventory, or security vulnerability as described in <strong>Searching the System.</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Do one of the following to open the project:</td>
</tr>
<tr>
<td></td>
<td>• Click the project name (in the example, <strong>New Project</strong>) in the title bar of the right panel.</td>
</tr>
<tr>
<td></td>
<td>• Click the <strong>Open Project</strong> icon ( ).</td>
</tr>
<tr>
<td>3.</td>
<td>Click the <strong>Summary</strong> button at the top of the window to open the Summary tab for the project.</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>Manage Project</strong>, and select <strong>Edit Project</strong> from the popup menu.</td>
</tr>
</tbody>
</table>
From the **Edit Project** dialog, navigate to the **Scan Settings** tab, and select the desired scan profile for your project. (Click the information icon next to a selected scan profile to open a read-only view of its attributes.)

### Selecting Materials to Scan

In preparing a project for scanning, you must identify which materials to scan and configure the project to point to these materials. The way in which you do this will largely depend on the type of scan you are performing:

- **Traditional scan** where the codebase is uploaded to the Scan Server or synchronized using a source code management system (SCM) such as Git or Perforce. With a traditional scan, you can manually move the code to the Scan Server, upload the code, or configure the project with an SCM. See these locations for instructions:
  - Uploading a Project Codebase
  - Configuring Source Code Management chapter

- **Remote scan** using a FlexNet Code Insight scan agent plugin to perform a scan remotely within the context of an Engineering application (such as an IDE, source-management, artifact-repository, CI, build, testing, or installation application). With a remote scan, the FlexNet Code Insight scan agent plugin is configured to scan remotely and send results to FlexNet Code Insight for review and remediation. See the following for more information:
  - Creating a Project Without Uploading a Codebase in the “Performing Inventory-Only Scanning” chapter
  - *FlexNet Code Insight Plugins Guide* (available for download in the Flexera Customer Community)

In both traditional and remote scan scenarios, the results are processed by FlexNet Code Insight, which creates inventory, detects licenses and security vulnerabilities, applies policies for automated review, and creates review and remediation tasks per configuration.

### Uploading a Project Codebase

Before FlexNet Code Insight can scan your code, you must upload an archive file containing your codebase. If your codebase changes, you can upload a new version of the codebase file by following the same procedure. Supported archive types for uploading a codebase include `.zip`, `.tar`, `.tar.gz`, and `.7z`.

The following topics describe the codebase upload process:

- Uploading the Codebase
- Supported Archive Types for Expansion
- More About Archive Expansion Behavior During Codebase Uploads

Refer to the *FlexNet Code Insight User Roles and Permissions* appendix for role requirements to upload the codebase.

### Uploading the Codebase

The Scan Server to which you are uploading the codebase must be running (that is, the Tomcat server installed on the same instance as the Scan Server must be running).

The following describes how to upload the project codebase.
To upload a project codebase, do the following:

1. Navigate to the Summary tab, as described previously in Applying a Scan Profile to the Project.
2. Click Upload Project Codebase. The File Upload dialog appears.
3. Click Select Archive File to browse for archive containing your codebase.
4. (Optional) Select Delete existing project codebase files to have FlexNet Code Insight delete previously uploaded codebase files and scan results associated with this project.

Note • If you select to delete existing codebase files, a Warning dialog appears, asking you to confirm the deletion. Be aware that all existing codebase files for project will be permanently removed from the Scan Server during the upload. If you rescan the project without replacing these files via a new upload, the scan results for the removed files will be permanently deleted.

5. For Archive File Expansion Options, select the level of archive expansion you want to perform on the codebase:
   - Uploaded file only—Extract the files from the uploaded archive. Any extracted archives are not expanded.
   - Uploaded file and first-level archives only—Extract the files from the uploaded archive and expand all first-level archives in the codebase. Note that the expanded archive itself is retained along with its extracted contents in the parent folder (see Retention of the Original Archive Files).
   - Uploaded file and all contained archives—Extract the files from the uploaded archive and expand archives at all levels (that is, archives with archives within archives and so forth) in the codebase. Note that each expanded archive is retained along with its extracted contents in the parent folder (see Retention of the Original Archive Files).

6. Click Upload. FlexNet Code Insight uploads your codebase file and attaches it to the selected project. You can now scan the uploaded codebase.

Supported Archive Types for Expansion

The archive that you upload must be one of these types:

- .zip
- .tar
- .tar.gz
- .7z
The following archive types within the upload archive can be expanded either at the first-level only or recursively, depending on the **Expand Archive** option you select:

**Table 2-1 • Expandable Archives**

<table>
<thead>
<tr>
<th>.7z</th>
<th>.tar.xz</th>
</tr>
</thead>
<tbody>
<tr>
<td>.cpio</td>
<td>.tgz</td>
</tr>
<tr>
<td>.tar</td>
<td>.txz</td>
</tr>
<tr>
<td>.tar.bz2</td>
<td>.tar.lzma</td>
</tr>
<tr>
<td>.tar.gz</td>
<td>.zip</td>
</tr>
</tbody>
</table>

**More About Archive Expansion Behavior During Codebase Uploads**

The following topics describe important information about how archives are expanded when a codebase is uploaded:

- **Retention of the Original Archive Files**
- **Expansion of Archives Containing an Intermediary .tar File**
- **Multiple Codebase Uploads to the Same Project**

**Retention of the Original Archive Files**

The extraction of an archive’s contents occurs directly in the parent folder. No new folder is created to contain the archive contents, and the archive itself is retained in the parent folder. For example, suppose the archive **AppsSport.zip** is located in the **coreApps** directory in your codebase. This archive contains the files **hockey1.exe** and **tennis.exe**. When **AppsSport.zip** is expanded, the resulting codebase tree looks like this, where **AppsSport.zip** is retained at the parent-folder level:

```
coreApps
  --AppsSport.zip
  --hockey1.exe
  --tennis1.exe
```

**Expansion of Archives Containing an Intermediary .tar File**

The **.tar.gz**, **.tgz**, **.txz**, **.tar.xz** archive types and similar archives contain an intermediary .tar file. The codebase upload extracts the intermediary .tar file from the archive, but applies the **Archive Expansion Options** configuration starting with the expansion of the intermediary .tar file, not the initial archive. The following example demonstrates this expansion behavior.

Suppose the archive **jars.tar.gz** has these contents, where the intermediary file is **jar.tar**:

```
jars.tar.gz
  --jars.tar
    ----file-1.txt
    ----file-2.txt
    ----jar.zip
    ------\jar
    ----------abc.jar (color)
```
The uploaded codebase looks like this if the **None** option for **Archive Expansion Options** is applied. The *jars.tar* is extracted from *jars.tar.gz*. The *jars.tar* archive is then expanded, but the *jars.zip* file (contained in *jars.tar*) is not expanded. Keep in mind that the original archive files are retained.

```
file-1.txt
file-2.txt
jars.zip
```

The uploaded codebase looks like this if the **Uploaded file and first-level archives only** option for **Archive Expansion Options** is used. The *jars.tar* is extracted from the initial *jars.tar.gz*. Once the *jars.tar* archive is expanded, the first-level *jars.zip* file (contained in *jars.tar*) is also expanded. However, the second-level *classes.zip* file (contained in *jars.zip*) is not expanded.

```
file-1.txt
file-2.txt
jars.zip
  \jar
    ---abc.jar
    ---xyz.jar
    ---classes.zip
```

The uploaded codebase looks like this if the **Uploaded file and all contained archives** option for **Archive Expansion Options** is used. The *jars.tar* is extracted from the initial *jars.tar.gz*. Once *jars.tar* archive is expanded, the first-level *jars.zip* file and the second-level *classes.zip* file are also expanded.

```
jars.tar
file-1.txt
file-2.txt
jars.zip
  \jar
    ---abc.jar
    ---xyz.jar
    ---classes.zip
      \classes
        ------Corporation.class
        ------Employee.class
```

**Multiple Codebase Uploads to the Same Project**

If multiple codebases are uploaded to the same codebase path for a given project (and existing codebase files are not deleted), the archives within all the codebases for the project are expanded based on the current **Archive Expansion Options** configuration. The following process demonstrates this behavior:

1. Create project1 and upload the codebase *codefiles1.zip*, using the **None** option. The contents of *codefile1.zip* are extracted. Archives in these contents are not expanded.

2. Upload *codefile2.zip* to the same project (at the same codebase path), this time using the **Uploaded file and all contained archives**. (Keep in mind that codebase1.zip was previously expanded with no further expansion of any archives in its contents.) Now all archives at all levels are expanded within the *codefile1* and *codefile2* codebases.
3. Upload codefile3.zip to the same project, this time using **Uploaded file and first-level archives only**. Now only the first-level archives in all three codebases are expanded.

If you upload multiple codebases to the same project, best practice is to keep track of the **Archive Expansion Options** configuration for each upload so that you can apply an appropriate configuration for the subsequent upload.

---

**Scanning the Codebase**

After a codebase is uploaded and the appropriate scan profile is selected, you can scan the codebase. The Scan Server to which you are uploading the codebase must be running (that is, the Tomcat server installed on the same instance as the Scan Server must be running).

Refer to the **FlexNet Code Insight User Roles and Permissions** appendix for role requirements to scan a codebase.

---

**Task**

**To start the scan, do the following:**

1. Navigate to the **Summary** tab, as described previously in **Applying a Scan Profile to the Project**.

2. Click the **Start Scan** button (or the link in **Scan Status**) to start the scan. If other scans are running, the scan is queued and will automatically run based on queue order. (Click the link in **Past Scans** to view details about the scheduled scan.)

---

**Note** • *If the **Start Scan** button is disabled, see Actions to Take When the Start Scan Button is Disabled.*

Information about the scan's progress appears in the **Scan Status** section on the **Summary** tab.

---

**Scan Status**

- **Scan Status:** Project being scanned
- **Scan Progress:** In Scan Queue  (Show Details)
- **Last Scan:** Scan of project Project2 completed
  - Scan Summary: 358 Files | 6.03 MB | 53 Lines of Code
- **Past Scans:** Click [here](#) to view the scan history for this project

When the scan completes, the **Scan Status** will display one of the following messages:

- **Completed**—The scan succeeded with no warnings during scan or analysis. This message appears on screen in green.
- **Completed with warnings**—The scan succeeded but the analysis has warnings.
- **Failed**—The scan failed. This message appears on screen in red.

---

**Note** • *If the scan completed with a warning or if it failed, check your scan log for more information.*

For an overall understanding of the scan results, see **Overview of Scan Results**.
3. Do any of the following:

- Manage the project. For example, you can assign users to project analyzer or reviewer roles, define the project’s scan settings, configure an automated review and remediation workflow, configure a connection to a remote data source such as Perforce or Jira, and more. See Managing a Project from the Summary Tab for details.

- Analyze the scan results, as described in Analyzing (Auditing) Scan Results.

- Generate the following reports:
  - The Project Report
  - The Audit Report
  - The Notices Report

**Actions to Take When the Start Scan Button is Disabled**

The Start Scan button on the Summary page for a project is disabled if the Scan Server associated with the project is not available for scanning. In the button is disabled, check with the administrator to determine the actual status of the server. If the administrator determines that the server is temporarily shut down, you can use the link in Scan Status on the Summary page to queue the scan. The scan will automatically run based on queue order once the server is active again. However, if the server is disabled, you will need to create a new project for the codebase and associate it with an enabled Scan Server.

**Overview of Scan Results**

You can begin to review scan results while a scan is running, including all system-generated inventory and all evidence available in Analysis Workbench. Alternatively, you can wait for the scan to complete to review the scan results and tasks that are generated as a result of the scan. A Code Insight scan can produce any of the following:

- Inventory
- Scan Evidence
- License Information Associated with Inventory

**Inventory**

System-generated inventory is created by FlexNet Code Insight during a scan and is available for view in Analysis Workbench and, if automatically published, on the Project Inventory tab. An inventory item represents an explicit finding in the scanned codebase and can represent any of the following: top-level component, bundled component, component found inside an archive, or direct or transitive dependency component.

An inventory item typically has an associated component, version, license and list of security vulnerabilities, as well as other details about these elements. See Inventory Details Pane in Analysis Workbench for a full description of the information collected by the scan.

These are some important elements about an inventory item that you can view at a glance:

- Review Status of Inventory
- Inventory Priority
Overview of Scan Results

- Inventory Confidence
- Security Vulnerabilities Associated with Inventory
- Inventory Usage Information

The following example highlights these elements for a given inventory item on the Project Inventory tab. Many of these same elements are available in the inventory view in Analysis Workbench. (For more information about the Analysis Workbench, see Analyzing (Auditing) Scan Results. For information about the Project Inventory tab, see Reviewing Published Inventory.)

Review Status of Inventory

During a scan, all inventory is checked against existing policies as defined in the Policy Profile. As a result, inventory is either automatically approved or rejected by policy or unaffected by policy. If inventory is not affected by policy, it should be manually reviewed, and the Policy Profile should be updated to reflect the review decision for future scans. The manual review process is described in detail in Reviewing Published Inventory.

For information about setting up policies that automate the inventory review process, see Managing Policy Profiles.

Note • Unaffected inventory is labeled as Draft in the Review Status field in Analysis Workbench and is represented as a circled X (for Not Reviewed) in the Status field on the Project Inventory tab.

Inventory Priority

The priority of an inventory item is meant to highlight the importance of that item during the inventory review process. FlexNet Code Insight uses the following algorithms determine the default priority of an inventory item.

You can manually change the inventory priority by simply selecting a different priority from the Priority dropdown either in Analysis Workbench or on the Project Inventory tab.
Chapter 2  Using FlexNet Code Insight

Overview of Scan Results

For a “Component” Inventory Type

Code Insight sets the inventory priority to P1 if any of these circumstances exist:

- The inventory item has at least one associated security vulnerability with a severity of High (for CVSS v2) or Critical (for CVSS v3.0).
- The Selected License priority is P1 (see License Priority).
- No licenses are found (that is, the Selected License value is I don’t know and no evidence of other licenses is found in the files associated with the inventory item).

Otherwise, when the user or system selects a component-version-license triad, the inventory priority is based on the license priority or highest associated security vulnerability severity, unless that would mean lowering an existing inventory priority.

Note • If the Selected License value for an inventory item is I don’t know but evidence of other licenses is found in the files associated with inventory item, the inventory priority is based on the highest priority among the found licenses or the highest associated vulnerability severity.

For a “License-Only” Inventory Type

When a user selects a license for a license-only inventory item, the inventory priority is set to the license priority (see License Priority) unless that would mean lowering an existing inventory priority.

Note • Due to the algorithm used to calculate the priority, the system-generated inventory priority will never be lowered by the system. It can only be lowered explicitly by the user.

Inventory Confidence

The Automated Analysis portion of the FlexNet Code Insight Scan Server uses a variety of techniques to identify inventory items from the scanned code base. The Confidence level (High, Medium, or Low) of an inventory item is a measure of the strength of the discovery technique used to generate the inventory item and the certainty of the finding. It is derived by assigning a score to the following elements:

- The strength of the analysis technique that provided the metadata on the inventory item.
- The existence of this inventory item in the Code Insight data library: items that have matching components in the data library have higher levels of confidence.

The Confidence level is represented as a simple three-segment graph for each inventory item in Analysis Workbench or on the Project Inventory tab. Three shaded segments indicate High confidence, two indicate Medium, and one indicates Low.

The following Confidence graph shows High confidence (with all three segments shaded):

The Confidence level is also available as a search criterion on the Project Inventory tab and can be used to quickly identify items that may require additional triage or review.
The following describes the Confidence levels:

- **High confidence**—An inventory item of High confidence means that either the item was identified with a specific and highly targeted rule or from the processing of a structured manifest file from a package manager (such as pom.xml for the maven package manager and package.json for the npm package manager). A High-confidence inventory item almost always matches with a component in the Code Insight data library and rarely requires further triage or review by the Analyst.

- **Medium confidence**—An inventory item of Medium confidence means that the item was identified using a more generic technique or by the processing of a secondary indicator to produce an inventory item. A Medium-confidence inventory item might or might not have a match to a component in the Code Insight data library and might require triage or review in order to be validate or further refine the finding.

- **Low confidence**—An inventory item of Low confidence means that the inventory item was identified using a very generic rule or an exploratory detection technique, and thus might represent a component of unknown origin. Inventory of Low confidence rarely have a match to a component in the Code Insight data library and should be further triaged and reviewed by an Analyst for accuracy and completeness.

The table below summarizes the various detection techniques and the corresponding confidence value:

**Table 2-2 • Confidences Levels Associated with Various Detection Techniques**

<table>
<thead>
<tr>
<th>Detection Technique</th>
<th>Rule or Configuration File Used</th>
<th>Confidence Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzers</td>
<td>Primary</td>
<td>High</td>
</tr>
<tr>
<td>Analyzers</td>
<td>Secondary</td>
<td>Medium</td>
</tr>
<tr>
<td>Search term analysis</td>
<td>Rules with versions</td>
<td>High</td>
</tr>
<tr>
<td>Search term analysis</td>
<td>Component-only rules</td>
<td>Medium</td>
</tr>
<tr>
<td>File name analysis</td>
<td>Specific rules</td>
<td>High</td>
</tr>
<tr>
<td>File name analysis</td>
<td>Generic rules of certain type of components</td>
<td>Medium</td>
</tr>
<tr>
<td>File name analysis</td>
<td>Generic rules</td>
<td>Low</td>
</tr>
<tr>
<td>Direct dependencies</td>
<td>Based on package manager files (pom.xml, package.json, and so forth)</td>
<td>Low by default, but can increase to Medium if matching component + version is found in CL</td>
</tr>
<tr>
<td>Transitive dependencies</td>
<td>Based on lookups against respective repositories (maven, npm, and so forth)</td>
<td>Low by default, but can increase to Medium if matching component + version is found in CL</td>
</tr>
</tbody>
</table>

**Security Vulnerabilities Associated with Inventory**

FlexNet Code Insight uses data from the National Vulnerability Database (NVD) and other advisories such as RubySec to report security vulnerabilities associated with your inventory items. The vulnerabilities information from these sources is used to create vulnerability rankings and alerts.
The **Vulnerabilities** bar graph shows the current security-vulnerability counts by severity level for a given inventory item listed in **Analysis Workbench** or on the **Project Inventory** tab:

![Vulnerabilities bar graph](image)

### Understanding Severity Levels for Security Vulnerabilities

FlexNet Code Insight obtains the severity level of a security vulnerability from the advisory database used to identify the vulnerability. The severity is based on the vulnerability’s CVSS (Common Vulnerability Scoring System) score, which can have two different values depending on the scoring system used to calculate it—CVSS v2 or v3.0. Code Insight supports both systems for displaying the scores and severities of security vulnerabilities. The Code Insight administrator determines which scoring system your system uses.

#### CVSS v3.0 Scoring System

When Code Insight is configured to use the CVSS v3.0 scoring system, the color-coded segments in **Vulnerabilities** bar graph represent the following severity levels:

- **Dark brown**—Critical severity (CVSS score 9.0 - 10.0)
- **Red**—High severity (CVSS 7.0 - 8.9)
- **Gold**—Medium severity (CVSS 4.0 - 6.9)
- **Yellow**—Low severity (CVSS 0.1 - 3.9)
- **None**—No severity available (N/A)

For example, the following **Vulnerabilities** graph reflects vulnerability counts for an inventory item when CVSS v3.0 scoring is used. The graph indicates 13 vulnerabilities of critical severity, 5 of high severity, 3 of medium severity, 0 of low severity, and 5 of unknown severity:

![Vulnerabilities graph](image)

#### CVSS v2 Scoring System

When Code Insight is configured to use the CVSS v2 scoring system, the color-coded segments in graph represent the following severity levels:

- **Red**—High severity (CVSS 7.0 - 10.0)
- **Gold**—Medium severity (CVSS 4.0 - 6.9)
- **Yellow**—Low severity (CVSS 0.1 - 3.9)
- **Gray**—Unknown severity (N/A)

The following example **Vulnerabilities** graph reflects vulnerability counts for the same inventory item referenced in the previous section, but in this case CVSS v2 scoring is used. Note that the graph shows the same total number of vulnerabilities as the previous graph shows, but the severity distribution is different. In this case, the graph indicates 13 vulnerabilities of high severity, 8 of medium severity, 5 of low severity, and 80 of unknown severity:

![Vulnerabilities graph](image)
Viewing Security Vulnerabilities

The following procedure explains how to use this graph to obtain details about the security vulnerabilities associated with the inventory item.

**Task**

To view security vulnerabilities for an inventory item, do the following:

1. For a specific inventory item, click any of the color segments in the **Vulnerabilities** bar graph.

   The **Security Vulnerabilities** dialog is displayed. (This example shows CVSS 3.0 scores and severities.)

   ![Security Vulnerabilities Dialog Example]

   Note the following details about the **Security Vulnerabilities** list:

   - Each entry identifies a specific security vulnerability associated with the selected inventory item. A vulnerability can be reported by the National Vulnerability Database (NVD) in the form of a CVE (Common Vulnerabilities and Exposures), by Secunia Research in the form an SA (Secunia Advisory), or by other research organizations using their own vulnerability ID formats. In some cases, CVEs will be referenced by one or more advisories. A given entry includes the ID for the vulnerability or advisory, as well as its source (such as NVD or Secunia), severity, CVSS score, and description.

   - The CVSS score label for a given entry indicates whether the value is a CVSS v3.0 or CVSS v2 score. If you click the ![CVSS Score Label](icon) icon, you can view both CVSS score values.

   ![CVSS Score Label Example]

   - In some cases, the vulnerability or advisory CVSS score is unknown because it has not been scored by the supplier. These vulnerabilities are reported by Code Insight with a CVSS score of **N/A** and a severity of **None** (CVSS v3.0) or **Unknown** (CVSS v2).
Note • Your feedback is welcome in how to handle the severity and scoring of currently unscored vulnerabilities. The FlexNet Code Insight team will do its best to incorporate the results of this feedback into the Code Insight vulnerability database. Contact FlexNet Code Insight Support (see Contacting Us).

- You can click the vulnerability or advisory ID link (if available) for a given entry to further investigate the vulnerability:
  
  **Source:** NVD
  **ID:** CVE-2018-5407

- The Security Vulnerabilities list represents vulnerabilities and advisories in a hierarchical fashion, with Secunia and other advisories at the top level, and CVEs at the secondary level of the hierarchy. This behavior is in place because advisories are often well-researched and provide additional information above what is provided by the NVD. CVEs that are not referenced by any advisories also appear at the top-level of the hierarchy. The hierarchy view is two levels deep.

- A CVE that is referenced by multiple advisories for the given inventory item is shown in the secondary list under each of the advisory entries. However, the vulnerability itself will count only once in the Vulnerabilities count on Inventory Details tab.

- All top-level entries (CVEs and advisories) are sorted by CVSS score. Similarly, CVE vulnerabilities in a secondary list under a top-level advisory entry are sorted by CVSS score within the secondary list.

- The Security Vulnerabilities list shows only explicit CVE vulnerabilities, Secunia advisories, or other advisories (that is, those directly mapped to the component version identified by the inventory item) and lists them in their proper hierarchical position.

2. (Optional) Click the hyper-linked CVE in an entry to view the vulnerability details found on the NVD or other website. Accessing these links is recommended if conducting deeper research as it shows referenced CVEs (those that are not explicitly mapped to the component version but can be indirectly related).

3. When you have finished viewing the reported vulnerabilities, click OK to close the dialog.

### Inventory Usage Information

FlexNet Code Insight provides the ability to see and edit usage information for a given inventory item. Usage information is important because it aids users in determining how closely to monitor inventory items for intellectual property (IP) and security risk and in taking appropriate action to approve or reject inventory, create tasks for remediation, and issue alerts and notifications. Usage fields can determine whether the item should be included in Third-Party Notices and what steps need to be taken to satisfy license obligations and conditions of use. They can also help to identify license conflicts and compatibility issues. The following are usage fields available for inventory.

The inventory usage fields are available on the Usage tab for a given inventory item, as found both on the Project Inventory tab (shown below) and in the inventory view in Analysis Workbench. You can update these fields when you manually create or edit inventory items.
Chapter 2  Using FlexNet Code Insight
Overview of Scan Results

- **Distribution Type**—Indicates how you are distributing the item. The distribution type can affect license priority and obligations.
  - Externally with your product, shipped to customers (outside of your organization, including a private cloud deployment at the customer’s site)
  - As an application hosted in your company’s data center (such as a SAAS application)
  - Internally only (such as an internal test framework included in the codebase but not distributed with the product)
  - Distribution method unknown

- **Part of Product**—Indicates whether the item is part of the core product or an infrastructure piece such as a build or test tool. This can affect whether third-party notices are required for this item.

- **Linking**—Indicates whether the libraries are statically linked (included in the materials), dynamically linked (brought in at runtime), or not linked at all. Linking can affect license priority and obligations.

- **Modified**—Indicates whether a project contributor, such as a developer, has modified the software from its original form. Modification can be an important factor for determining license obligations and distribution requirements that are governed by a specific license.

- **Encryption**—Indicates whether the component provides encryption capabilities used in the product. Encryption can affect export controls.

For explicit directions on viewing or editing inventory usage either in **Analysis Workbench** or on the **Project Inventory** tab, see the following:

- Viewing Security Vulnerabilities for Inventory in Analysis Workbench
- Viewing Usage Information for Project Inventory
- Editing Inventory from the Project Inventory Tab

### Scan Evidence

Scan evidence is generated by FlexNet Code Insight during a scan and is available for view in **Analysis Workbench** to any analyst assigned to the project. Scan evidence is typically an indicator of third-party content in the codebase. It can be useful for verifying system-generated inventory, identifying and creating additional inventory not discovered during scan, finding embedded licenses and copyrights in bundled code or archives, determining file origin, and locating stolen or borrowed code.
You can quickly view filter on and view the following evidence for codebase files in Analysis Workbench. (For more details about viewing evidence in Analysis Workbench, see Viewing Details for Licenses Associated with Codebase Files and Using the Evidence Details Tab.)

- **Exact Matches**—A whole-file match to a file in the Compliance Library
- **Source Matches**—Snippet-level matches to files in the Compliance Library
- **Copyrights**—Third-party copyright statements detected in the code
- **Emails/URLs**—Third-party emails and URLs detected in the code
- **Licenses**—Licenses detected in the code based on custom license patterns supplied by Electronic Update
- **Search Terms**—String matches based on pre-configured search terms provided by Flexera and on custom search terms added by the user as part of the Scan Profile

### License Information Associated with Inventory

The FlexNet Code Insight scan detects license text and references to licenses in your codebase and enables you to examine this information in various ways, such as viewing the license or license-reference text highlighted in the codebase file itself (see Viewing Copyright, Email, URL, and License Evidence in a File). The following topics provide an overview of other license-related information you can examine or manage:

- **License Details from the Code Insight Data Library**
- **License Priority**
- **Reporting of Detected License Text through the As-Found Text Inventory Field**
- **Notices Text**

### License Details from the Code Insight Data Library

When an inventory item is automatically created by FlexNet Code Insight, it uses information in the FlexNet Code Insight data library to automatically select a license for the component associated with the inventory item. You can view details from the data library for each license by simply clicking next to any license reference in Analysis Workbench or the Project Inventory tab.

- **Licenses (1)**
  - GNU General Public License v2.0

- **Search Terms (7)**

The License Details window is displayed containing the following information:

- A **General Information** tab that lists details such as the name of the license, its family, and the license priority assigned by FlexNet Code Insight.
- A **License Text** tab that displays the complete license text (representing the external forge license text).

For descriptions of these fields in this window, see License Details Window.
The following lists locations in Code Insight user interface where you can access the License Details window:

- In **Analysis Workshop**, you can view this information by codebase file or inventory item, as described in Viewing Details for Licenses Associated with Codebase Files and Viewing Details About Licenses Associated with Inventory in Analysis Workbench, respectively.
- From **Project Inventory**, you view this information by inventory item, as described in Viewing Details About the Licenses Associated with Project Inventory.
- Whenever you create or edit an inventory item or perform a Component Lookup in **Analysis Workbench** or from **Project Inventory**.

### License Priority

You want to understand the priority of licenses in your codebase so you can handle them based on your corporate policies. FlexNet Code Insight uses a default license priority to highlight which inventory items are more important than others, helping to define day-one work items.

Each license referenced in **Analysis Workbench** and on the **Project Inventory** tab has one of the following priority values:

**Table 2-3 • License Priorities**

<table>
<thead>
<tr>
<th>Priority</th>
<th>Characteristics</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Viral/Strong Copyleft</td>
<td>1</td>
<td>Usually, P1 licenses require immediate attention due to the possibility of tainting proprietary application code, an issue that can have significant business impact.</td>
</tr>
<tr>
<td>P2</td>
<td>Weak Copyleft/Commercial/Uncommon</td>
<td>2</td>
<td>The typical P2 license requires legal review and guidance based on corporate policies about the proper use of these types of licenses in your organization.</td>
</tr>
</tbody>
</table>
Inventory priority (see Inventory Priority) is a risk metric for the inventory item that takes license priority into account as one of the contributing factors. Inventory priority is set at scan time when the inventory item is created by the system or during inventory review. You can set or override the inventory priority at any time. License priority, on the other hand, is static and never changes. The license priority is supplied by the Electronic Update.

Inventory priority typically defaults to the license priority value unless a critical vulnerability exists or you manually override the inventory priority value (as described in Inventory Priority).

**Note** • FlexNet Code Insight REST APIs that reference the license entity, such as the Component Lookup API, include the license priority in the API response body.

### Viewing the License Priority

You can view the license priority from the **License Details** window associated with the license. See License Details from the Code Insight Data Library for details on accessing this window.

### Reporting of Detected License Text through the As-Found Text Inventory Field

The **As-Found License** field (on the **Notices Text** tab for a selected inventory item in Analysis Workbench and in Project Inventory) shows the license text or license references found in the scanned codebase.

### Table 2-3 • License Priorities (cont.)

<table>
<thead>
<tr>
<th>Priority</th>
<th>Characteristics</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P3</td>
<td>Permissive/Public Domain</td>
<td>🟢</td>
<td>In general, P3 licenses are allowed and have minimal impact to an organization as long as license obligations are satisfied. The most common license obligation is properly attributing the use of an open source component to its author. This is the default priority.</td>
</tr>
</tbody>
</table>
Chapter 2  Using FlexNet Code Insight

Overview of Scan Results

The following shows the **Notices Text** tab in **Analysis Workbench**:

![Analysis Workbench Screenshot]

This shows the **Notices Text** tab in **Project Inventory**:

![Project Inventory Screenshot]

The **As-Found License Text** content cannot be edited, but you can copy it to the **Notices Text** field (also on the **Notices Text** tab) if you need to modify it. The text in the **Notices Text** field is considered final and is included in the Notices report. Otherwise, if the **Notices Text** field is empty, Code Insight uses the contents of the **As-Found License Text** field as the license text for the inventory item in the report. If both fields are empty, the report uses the license content from FlexNet Code Insight data library.

For more information about finalizing license text for the Notices report, see **Finalizing the Notices Text for the Notices Report**.
Notices Text

The Notices Text field (on the Notices Text tab for a selected inventory item in Analysis Workbench and in Project Inventory) can be used to finalize the license text for use in the Notices report. For example, you can copy the contents of the As-Found License Text field to this field and modify the text as needed. Alternatively, you can simply provide your own Notices content in the Notices Text field.

When the Notices report is run, the content of the Notices Text field item is pulled into the report if this field contains information. If the Notices Text field is empty, the content of the As-Found License Text field is used in the report. If both fields are empty, the report uses the license content from FlexNet Code Insight data library.

For more information about finalizing license text for the Notices report, see Finalizing the Notices Text for the Notices Report.

What Does an Analyst do?

The role of the Analyst is to transform the evidence uncovered by the Scan Server into an inventory item. Analysts create inventory items that associate files in your codebase to open source projects. For example, Analysts might evaluate files with a copyright of “Copyright (c) 2015 to 2020 Mark Smith” and a license match to the “zlib” license. Then the Analysts would place these files in a group for the “zlib” open-source project and mark those files as reviewed to register progress.

The Analyst will evaluate all of the evidence within a codebase, create inventory items where appropriate, mark the analyzed files as reviewed, and finally publish them. Once published, the inventory will be available for reporting and review.
Analyzing (Auditing) Scan Results

After you scan your codebase, you can evaluate the results of the scan in the Analysis Workbench. In FlexNet Code Insight terminology, this is called auditing. The goal of an audit is a complete and accurate inventory of third-party code within your products. Sometimes this is referred to as a Bill of Materials (BOM). With this inventory, you will be able to do the following:

- Discover and remediate code that is under licenses that put your proprietary source code at risk.
- Discover and remediate code with known security vulnerabilities.
- Discover and remediate code with no license or under business unfriendly licenses from competitors or malicious sources.
- Comply with licenses that have obligations such as providing source code or attribution/credit to authors.
- Apply policies based on the license.
- Generate reports for your customers or for internal use.

Refer to the FlexNet Code Insight User Roles and Permissions appendix for the project roles (in addition to the Analyst role) required to access the Analysis Workbench and to analyze and act on scan results.

Section Overview

The section provides the following topics to describe how to use the Analysis Workbench:

- Opening the Analysis Workbench
- The Analysis Workbench Layout
- Searching for Codebase Files Based on Name
- Searching for Codebase Files Based on Search Criteria
- Creating and Editing File Searches
- Using the Filter Legend Options to Filter the Codebase
- Using the Codebase Files Pane Context Menu
- Marking Files as Reviewed
- Viewing Details for Licenses Associated with Codebase Files
- Using the File Details Tab
- Using the Evidence Details Tab
- Using the Inventory Details Tab

Opening the Analysis Workbench

Use the following procedure to open the Analysis Workbench.
Task To open the Analysis Workbench, do the following:

1. Click the Open Menu icon in the upper right of any FlexNet Code Insight page:

2. Select Projects from the menu. The Projects list is displayed.

3. Select a project from the Projects list to display its Project Dashboard in the right panel.

4. To open the project, either click the Open Project icon ( ) next to the project entry in the Projects list, or click the project’s name link in the upper left corner of the dashboard:

   ![Project Dashboard](image)

   The project opens on either its Project Inventory or Summary tab (both are displayed). If you have permissions to analyze the scan results, the Workbench Analysis tab is displayed.

5. Navigate to the Analysis Workbench tab to begin the analysis process. See the next section, The Analysis Workbench Layout.

The Analysis Workbench Layout

The following is a view of the FlexNet Code Insight Analysis Workbench, showing the various areas of the page:

![Analysis Workbench](image)

After you click Analysis Workbench, the following information appears in the panes of the page:

- Codebase Files—Allows you to browse a tree of the scanned files you uploaded for this project.
Chapter 2 Using FlexNet Code Insight
Analyzing (Auditing) Scan Results

- **File Search Results**—Shows the results of file searches. There are several types of file searches that can be performed. Click a file to see the file’s content and evidence in the File Details panel.

- **File Details**—Shows the actual content of scanned (non-binary) files, including evidence highlighted in color. Here an analyst can research where the code came from to ultimately create an inventory item explaining the scan findings.

- **Inventory Items**—Displays a quick view of all the inventory identified in the codebase. Click the name of any item listed in the Inventory Items pane to display the inventory details for that item.

- **Inventory Details**—Shows information about the selected inventory items identified and used by this codebase.

- **Evidence Details**—Displays evidence that was uncovered by the scan, which is organized and sortable. Click Evidence Details, and the middle pane of the Dashboard displays details about the evidence. To filter the files in the File Search Results to focus attention on a particular finding, select a row or a set of rows and click Search Files. For more ways to filter findings, see Searching for Codebase Files Based on Name.

- **Legend**—Provides a key to the colors used in the various panes of the Dashboard. The Legend is interactive. You can click it to filter what appears in the File Search Results pane.

---

**Note** • Some source files contain indications that they are data files, generated code, or common code that is widely used in many open source projects. In those cases, FlexNet Code Insight records the fact that source matches exist but does not store all of the source match data. These files are indicated in the Analysis Workbench with an icon (✗).

### Searching for Codebase Files Based on Name

You can perform a file search to find files based on the file name to concentrate the Analysis Workbench display on files of interest for conducting your analysis of the scan results. The following limitations apply:

- There is no support for wildcard specifications. The comparison is a case-insensitive filename containing the complete search string.
- Only the first 1,000 matching files are returned by the file search.

**Task** To perform a file search based on name, do the following:

1. In the search text box in the Codebase Files pane, enter the partial or full name of the file or folder that you want to search and press Enter. You must type at least three characters to initiate the filename search. The text box is highlighted with a red border if you enter fewer than three characters, and an error message is shown in a tooltip.

2. When a match is found, the codebase file tree is expanded as much as necessary to highlight the matching file. The file details are not open until you click on the file in the tree.

3. Select the Next Match (>) and Previous Match (<) buttons next to the search string box to navigate the results of the search.

- **Files**—If the Previous or Next match button reaches a file, that file will be highlighted in the codebase tree, and the search term will be highlighted in yellow.

- **Folders**—If the Previous or Next match button reaches a folder, that folder will be highlighted in the codebase tree and the search term will be highlighted in yellow. The folder will also be automatically expanded one level so that you can see its child items.
The counter between the buttons indicates the total number of matches and the current match number.

4. (Optional) Click the name of a file to display its contents in the File Details tab.

5. (Optional) Click the X to clear the search string.

### Searching for Codebase Files Based on Search Criteria

You can perform a file search to find files based on the file name to concentrate the Analysis Workbench display on files of interest for conducting your analysis of scan results.

#### Task

To perform a file search by criteria, do the following:

1. Navigate to the Analysis Workbench tab.
2. Click Advanced Search in the File Search Results pane. The Advanced File Search dialog appears.
3. Pick a predefined search filter or add a new one:
   - To pick a predefined search filter, click the name of a filter to select it; and then click Search to begin the search with the selected filter.
   - To create a new search filter, see Creating and Editing File Searches.

Results are listed in the File Search Results pane.

### Creating and Editing File Searches

You can supplement the built-in filters with custom filters to focus on scan data that are important to you. For example, you can create a new file search from scratch or from a copy of an existing search. You can also edit searches. Refer to the following topics:

- Creating a New File Search
- Editing a File Search
- Copying a File Search
- Deleting a File Search

Any new searches you create or any copies or edits you make are available to all users in your FlexNet Code Insight system. Likewise, any searches that you delete are no longer available to users in the system.

### Creating a New File Search

Use either procedure to create a new file search:

- Create a File Search from Scratch
- Create a File Search from a Copy
Create a File Search from Scratch

Use this procedure to create a file search from scratch.

**Task**

**To create a new search from scratch, do the following:**

1. Navigate to the Analysis Workbench tab.

2. In the File Search Results pane, click Advanced Search. The Advanced File Search dialog appears.

3. Click Add New. The Create Filter dialog appears.

4. In the Name field, type a name for the search.

5. (Optional) In the Description field, type a description of the search. For example, type text that explains what the filter will search for.

6. Enter values in the Criteria fields:
   a. Select a criterion from the drop-down Select Search Field menu.
   b. If applicable, select a search operation (for example, Contains or =) and provide a search string or value.
   c. To add another criterion, click Add Criteria, select a Boolean value to define how the criteria is applied, and repeat the previous steps to define the criterion. Repeat for each criterion added.
   d. To add a group of criteria that serves as a criterion, click Add Criteria Group, and repeat steps a through c to create the group. The following shows an example of a criteria group:

   ![Advanced File Search Dialog](image)

7. Determine how you want to proceed:
   - **Save**—Save your search but do not execute it.
   - **Save and Search**—Save your search filter and then execute it.
   - **Search without Saving**—Execute the search without saving it.
   - **Cancel**—Do not execute the search or save it.

Create a File Search from a Copy

Use this procedure to create a file search from a copy of an existing search. Using a copy keeps the existing search in tact and provides a template for creating the new one.
Task  

To create a search from a copy of an existing one, do the following:

1. Navigate to the **Analysis Workbench** tab.

2. In the **File Search Results** pane, click **Advanced Search**. The **Advanced File Search** dialog appears.

3. Locate the search you want to copy, and click **in its entry. A new file search is created with “Copy of...” in its title.

4. In the entry for the copy, click ** to open the filter properties.

5. In the **Name** field, type a new name for the search.

6. Modify the filter criteria as needed and save the changes. See Create a File Search from Scratch for any additional instructions.

**Editing a File Search**

Use these instructions to edit an existing file search.

Task  

To edit a file search, do the following:

1. Navigate to the **Analysis Workbench** tab.

2. In the **File Search Results** pane, click **Advanced Search**. The **Advanced File Search** dialog appears.

3. In the entry for the file search you want to edit, click ** to open the filter properties.

4. Modify the filter criteria as needed and save the changes. See Create a File Search from Scratch for any additional instructions.

**Copying a File Search**

Use these instructions to create a copy an existing file search (as a backup or a basis for creating a new search, for example).

Task  

To make a copy of an existing file search, do the following:

1. Navigate to the **Analysis Workbench** tab.

2. In the **File Search Results** pane, click **Advanced Search**. The **Advanced File Search** dialog appears.

3. Locate the search you want to copy, and click ** in its entry. A new file search entry is created with “Copy of...” in its title.
Deleting a File Search

Use these instructions to delete a file search. When you delete the search, it is removed from the system and no longer available to users.

Task

To delete an existing file search, do the following:

1. Navigate to the Analysis Workbench tab.
2. In the File Search Results pane, click Advanced Search. The Advanced File Search dialog appears.
3. Locate the search you want to delete, and click X in its entry. A message is displayed to confirm that you want to delete the search.
4. Click Yes to remove the file search from the system.

Using the Filter Legend Options to Filter the Codebase

The codebase filter legend in the ribbon at the top right of Analysis Workbench provides a means of filtering the codebase by evidence type or by files with a “Reviewed” status. For example, by simply clicking an icon (or its label), you can filter to all files containing copyright or email-address evidence or that are exact matches to third-party files.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Label</th>
<th>Filters to files...</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>New Evidence</td>
<td>containing any evidence that the previous scan did not detect but that the most recent scan did.</td>
</tr>
<tr>
<td>✔</td>
<td>Reviewed</td>
<td>marked as “reviewed”.</td>
</tr>
<tr>
<td>■</td>
<td>Exact</td>
<td>that are exact matches to known third-party files.</td>
</tr>
<tr>
<td>■</td>
<td>Copyrights</td>
<td>containing copyright information.</td>
</tr>
<tr>
<td>■</td>
<td>Email/URLS</td>
<td>containing email addresses or URLs.</td>
</tr>
<tr>
<td>■</td>
<td>Licenses</td>
<td>containing license information.</td>
</tr>
<tr>
<td>■</td>
<td>Search Terms</td>
<td>containing search terms defined in the scan profile.</td>
</tr>
<tr>
<td>■</td>
<td>Source</td>
<td>containing code-snippet matches (fingerprints) of known third-party code.</td>
</tr>
</tbody>
</table>
The color theme used for evidence types in this legend is also used to indicate the types of evidence found in a given file in the Codebase Files and File Search Results lists (see the following procedure) and on the File Details tab (see Using the File Details Tab).

**Task**  
To filter the codebase using the filter legend options, do the following:

1. In the Analysis Workbench, click the option in the filter legend to identify how you want to filter the codebase files. Results are listed in the File Search Results pane.

2. Navigate to the File Search Results pane, which now shows a codebase tree containing the files that meet your criterion.

3. Drill down in the codebase tree to view the files.

   Note that each file entry is flagged not only with a icon that matches the filter-legend criterion you selected but also with icons representing all evidence or attributes associated with this file.

4. Select a file a from the filtered codebase list.

   Refer to the following sections for different ways to analyze and act on third-party evidence discovered in the files:
   - Viewing Details for Licenses Associated with Codebase Files
   - Viewing the Evidence Summary for a File
   - Viewing Binary Strings in a File
   - Viewing Copyright, Email, URL, and License Evidence in a File
   - Viewing Exact Matches
   - Viewing Source Matches
   - More About the “Remote Files” Panels on the Exact or Partial Matches Tabs
   - Adding a Partial or Exact Match Codebase File to an Inventory Item Based on an Associated Component
Using the Codebase Files Pane Context Menu

The Codebase Files pane has a context menu containing shortcuts to common codebase tasks. The following tasks are available on the Codebase Files pane context menu:

- **Add to inventory**—Select an item listed in the Codebase Files list that you want to add to inventory, right-click and choose Add to inventory to quickly add your selected items to display the Add to inventory dialog. For more information, see Creating an Inventory Item from the Analysis Workbench.

- **Show file inventory**—Select an item listed in the Codebase Files list that you want to view in the Inventory Items pane, right-click and choose Show file inventory. The selected item is listed in the Inventory Items pane.

- **Mark as reviewed**—After you have reviewed an item in the Codebase Files list, hover over the item, right-click, and then select Mark as reviewed to mark the file reviewed and add a checkmark in the Reviewed column.

- **Mark as unreviewed**—If you determine that a displayed file has not been reviewed, hover over the item, right-click, and then select Mark as unreviewed to mark the file unreviewed and remove the checkmark from the Reviewed column.

- **Download File**—Hover your cursor over an item to download, right-click and select Download File. The selected item is downloaded to the temp subdirectory for the open project.

Marking Files as Reviewed

It is important to keep track of which files have been audited by marking files as reviewed when you are finished auditing them. You can use buttons at the top of the file tree pane to filter on only un-reviewed files to see what is left to evaluate. You can also see the progress of the audit on the Summary tab. When all files with indicators have been marked as reviewed, an overview-style audit can be considered completed.

<table>
<thead>
<tr>
<th>Task</th>
<th>To mark files or directories as reviewed, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>In the Codebase files pane of the Analysis Workbench, right click on a directory or file you want to mark as reviewed. The Inventory popup menu appears.</td>
</tr>
<tr>
<td>2.</td>
<td>Select Mark as reviewed.</td>
</tr>
</tbody>
</table>

*Note:* If you enabled the auto-publish feature in the project scan settings, you can also enable the associated files to be marked as reviewed.

Viewing Details for Licenses Associated with Codebase Files

In Analysis Workbench, you can view details about the licenses for codebase files associated with your inventory. The license information is pulled from the FlexNet Code data library and is displayed on these tabs in the License Details window:

- A General Information tab that lists details such as the name of the license, its family, and the license priority assigned by FlexNet Code Insight.
- A License Text tab that displays the complete license text (representing the external forge license text).
Chapter 2  Using FlexNet Code Insight
Analyzing (Auditing) Scan Results

Note • This window is also accessible select or view a license as you create or edit an inventory item or perform a Component Lookup from the Inventory Details tab.

Task  To view details for a license, do the following:

1. (Optional) To make file selection easier, you can filter the codebase files to only those containing license evidence. See Using the Filter Legend Options to Filter the Codebase.

2. In the Codebase Files pane or File Search Results pane, select the codebase file containing the license evidence you want to review. A file with license evidence will show a green icon in its entry:

   ![stack icon]

3. Locate a license reference on File Details, Inventory Details, or Evidence Details tab in Analysis Workbench, as in this example in the Evidence Summary subtab on File Details tab:

   ![Evidence Summary Table]

   Note • License references are also displayed when create or edit an inventory item or perform a Component Lookup from the Inventory Details tab.

4. Click the information icon (ı) next to the license name. The License Details window appears with the General Information tab in focus.

   For descriptions of these fields on this tab, see License Details Window. Also see License Priority for background on how the license priority is used.

5. Select the License Text tab to view the license text.

6. When you have finished examining the license details, click Close.
Using the File Details Tab

The File Details tab provides additional information about the files in your codebase:

- Viewing the Evidence Summary for a File
- Viewing Binary Strings in a File
- Viewing Copyright, Email, URL, and License Evidence in a File
- Viewing Exact Matches
- Viewing Source Matches
- More About the “Remote Files” Panels on the Exact or Partial Matches Tabs
- Adding a Partial or Exact Match Codebase File to an Inventory Item Based on an Associated Component

Viewing the Evidence Summary for a File

FlexNet Code Insight provides you the ability to see which scan results were identified for any file. You can use this information to properly write review comments in new or existing inventory items. The Evidence Summary includes a summary of the following string-based scan results for the selected file:

- Copyrights
- Emails/URLs
- Licenses
- Search Terms

This feature is especially useful for binary files (object files, images, executables, etc.) to see a list of third-party evidence in a concise view.

Task

To view the evidence summary, do the following:

1. In the Analysis Workbench, select a file in the Codebase Files panel.
2. Select the File Details tab.
3. Select Evidence Summary. Summary information about the selected file appears in the center pane:
4. (Optional) To view additional information for the selected file, click the expand arrow (➕). The top portion of the tab expands to show details about the file:
Viewing Binary Strings in a File

Use this procedure to view the list of strings (each string consisting of at least three consecutive printable characters) found in the content of a binary file. This list enables you to perform a deep search for evidence, such as a copyright or comment snippet, of third-party code in the file.

**Task**

To view strings that are present in a binary file, do the following:

1. Ensure that you have selected a binary file in the Codebase Files panel, and click File Details.
2. Click Partial Matches. The File Details panel displays the strings that are output.
3. (Optional) Click the expand arrow (expand arrow), to view additional options. The top portion of the tab expands to show details about the binary file.

Viewing Copyright, Email, URL, and License Evidence in a File

For the currently selected codebase file, use this procedure to view highlighted copyright, email, URL, or license text (or a combination of these) identified as third-party evidence by Code Insight.

To view other types of evidence, refer to these other sections:

- For source-code matches (fingerprints), see Viewing Source Matches.
- For codebase files that are exact matches to third-party files, see Viewing Exact Matches.

**Task**

To view copyright, email, URL, and license content in a file, do the following:

1. In the Codebase Files pane or File Search Results pane, select the codebase file containing the evidence you want to review. (Optionally, to make file selection easier, you can filter the codebase files to only those containing a specific type of evidence. See Using the Filter Legend Options to Filter the Codebase.)
2. Click File Details.
3. Select the Partial Matches tab to show the contents of the file.

Color-coded selection boxes at the top of the Partial Matches tab are used to indicate the type of evidence you want to highlight in the file. (Based on your screen size, labels on these selection boxes might not be visible. In this case, hover over a box to see its label.) Depending on the types of evidence existing in the file, certain selection boxes might already be selected; others might be disabled.
4. If necessary, select (or unselect) one or more selection boxes to highlight the evidence you want to view in the file. For example, the following selections will highlight instances of copyright, email, URL, license, and search-term evidence in the file:

Considerations for Viewing License Evidence

When a given source or text file in the Codebase Files list contains license evidence (as indicated by a green icon in the file entry and by the one or more licenses listed on Evidence Summary tab), the Partial Matches tab usually shows the specific evidence for each license highlighted in green within the file content. However, the following exceptions can occur:

- **Licenses are detected but not highlighted in the file**—Cases can occur during a scan when a license is discovered in the scan results and listed on the Evidence Summary tab, but no associated license text is highlighted on the Partial Matches tab. The lack of highlighting occurs because the scanner is unable to calculate the offsets for license text in the file.

- **All content is highlighted, including large sections of non-license-related text**—If a file containing license evidence uses a non-supported file extension, all content in the file is highlighted in green, including large sections of non-license-related information. (This is different from the scenario in which all or nearly all the content in a file is the license text, and thus the entire file is highlighted as such.)

Viewing Exact Matches

Your scan will identify files in the codebase that are exact matches to files in Compliance Library (CL). Follow these steps to review these scanned codebase files that exactly match files (called remote files) in the CL. For a given codebase file with one or more matching remote files, you can then review details about the component version and licenses associated with each remote file.
Task: To review these exact file matches, do the following:

1. Ensure that you have run a scan with Comprehensive Scan Profile selected in the project (or a custom scan profile with exact matches enabled). For more information, see “Creating a Scan Profile” in the FlexNet Code Insight Installation and Configuration Guide.

2. In the Analysis Workbench, click the Exact link in the legend at the top right of the page to easily find all files with exact matches (see Using the Filter Legend Options to Filter the Codebase). Results are listed in the File Search Results pane.

3. Click the codebase file from the list in File Search Results, and select the Exact Matches tab.

   The Remote Files panels are displayed.

4. Select a remote file in the Remote Files panel to see the associated component and license information (on the Components and Licenses panels, respectively).

   The information presented in the Remote Files panel consists of a set of files from the open source community that are an exact match to the scanned file. This means that the scanned file in the codebase likely originated from outside the organization, and its origin needs to be identified.

   See the More About the “Remote Files” Panels on the Exact or Partial Matches Tabs for more information about the functionality available from the three panels.

Viewing Source Matches

When you scan your codebase with source-code (fingerprint) matching enabled, FlexNet Code Insight will produce results that you can view from the Partial Matches tab for a given codebase file. The results include a list of third-party (remote) files associated with fingerprint instances discovered. When you select one of these remote files, the fingerprint instances that match code in the remote file are highlighted in your source code.

Note • The size limit for a file that you open in the Partial Matches tab is 2 MB. If the file you want to inspect is too large, you can download and open it outside of FlexNet Code Insight to inspect it manually for evidence.

Task: To view source matches, do the following:

1. Ensure that you have run a scan with Comprehensive Scan Profile selected in the project (or a custom scan profile with source-code matches enabled). For more information, see “Creating a Scan Profile” in the FlexNet Code Insight Installation and Configuration Guide.

2. In the Analysis Workbench, click the Source link in the legend at the top right of the page to filter to all files with source-code matches (see Using the Filter Legend Options to Filter the Codebase). Results are listed in the File Search Results pane.

3. Click a codebase file in the list in File Search Results, and select the Partial Matches tab.
4. On the **Partial Matches** tab, click the **Source Matches** selection box at the top of the tab to enable *source code fingerprint match* results.

The **Remote Files** panels are displayed.

5. Select a remote file in the **Remote Files** panel on the left to highlight the source code fingerprint matches in the file and to see the lists of associated component and license information (on the **Components** and **Licenses** panels, respectively).

The information in the **Remote Files** panel consists of a set of files from the open source community that contain identical code to the scanned file. This means that the scanned file in the codebase possibly contains content that originated from outside the organization, and its origin needs to be identified.

See the More About the “Remote Files” Panels on the Exact or Partial Matches Tabs for details about the functionality available from the three panels.

Note that, for source matches, the **Remote Files** panel will additionally contain the following **CodeRank™** values:

- **CodeRank (CR%)**: A composite heuristic comprised of Coverage, Clustering, and Uniqueness. The higher the number, the stronger the match confidence.

- **Coverage (CV%)**: The percentage of the matching third-party file contained in your scanned file.

- **Clustering (CL%)**: The density or proximity of the source code matches within your scanned file.

- **Uniqueness (U%)**: The uniqueness of the set of discovered source code matches are in the Compliance Library (CL).

- **Matches**: The number of unique matches in the scanned file.

6. To view the instances of other types of evidence (for example, copyrights, licenses, URLs, email addresses, and search terms) in the codebase file, click the appropriate color-coded selection boxes at the top of the **Partial Matches** tab:

Each instance of evidence is highlighted in the same color as its corresponding selection box.

**More About the “Remote Files” Panels on the Exact or Partial Matches Tabs**

When you open the **Exact Matches** tab or the **Partial Matches** tab (and select the **Partial Matches** checkbox) for a codebase file selected in the **Analysis Workbench**, a **File Details** view is shown in the center of the screen with the following panels:

- **Remote Files Panel**
- **Components Panel**
- **Licenses Panel**
**Note About Filtering in the Panels**

The items in each panel can be filtered in these ways:

- When you select a specific item in one panel, the items in the other panels are filtered to show only those items associated with the selected item.

  For example, when you select a specific remote file in the Remote Files pane, the Components list is filtered to show only items associated with the remote file, and the Licenses list is filtered to show only items associated with the items now listed in the Components panel. Similarly, if you select a specific component in the Components list, the Remote Files and Licenses lists are filtered to show only those items associated with the selected component.

- You can filter the items in a given panel by entering a search string to show only items in that panel containing the string. When the filter is applied, the other panels are automatically filtered to show only items associated with the items now listed in the panel filtered by the search string.

```
<table>
<thead>
<tr>
<th>Component Name</th>
<th>bamboo</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Remote Files Panel**

This panel initially lists all the remote files from the Compliance Library (CL) that are either a perfect match (exact match) or contains partial-match content (source-code fingerprint match) to the scanned file. The partial-match content also ranks the remote files by CodeRank™ values, described in the previous section, Viewing Source Matches.

The remote files list can be filtered as discussed in Note About Filtering in the Panels.

**Components Panel**

This panel initially lists all the component versions that contain the remote files listed in the Remote Files panel. The list can be filtered as discussed in Note About Filtering in the Panels.

You can perform the following operations for a given component in the Components panel:

- To review the path of a remote file within a component, select the file in the Remote Files panel, and then click the Remote File Paths icon in the component row. A remote file is a file found within an open source component release that is either identical to the scanned file, or contains similar partial content as the scanned file. The remote file path is important because similar file structures between the scanned codebase and the remote file content is a potential strong indicator of code reuse from an open source project.

- To view information about the component, click the Information icon.

- To add the selected codebase file to an inventory item associated with the component, click the Add File to Inventory icon. For more information, see Adding a Partial or Exact Match Codebase File to an Inventory Item Based on an Associated Component.

**Licenses Panel**

This panel lists all the licenses associated with the component versions listed in the Components panel but can be filtered as discussed in Note About Filtering in the Panels.

You can view information about the license by clicking the Information icon in the license entry.
Adding a Partial or Exact Match Codebase File to an Inventory Item Based on an Associated Component

Use the following procedure to easily add a given a codebase file that exactly or partially matches a remote file (in the Compliance Library) to an inventory item.

**Task**

**To add an exact or partial match codebase file to an inventory item based on an associated component version, do the following:**

1. In the **Analysis Workbench**, click the **Exact** or **Source** matches link in the legend at the top right of the workbench to search for codebase files that are exact or partial matches to files in the Compliance Library. Results are listed in the **File Search Results** pane.

2. From the list in **File Search Results**, locate and click the codebase file you want to add to an inventory item based on a specific component version associated with the file.

3. Open the **File Details** tab, and, at the top of the tab, select the **Exact Matches** or **Partial Matches** tab. Additionally, if you are on the **Partial Matches** tab, select the **Source Matches** checkbox.

4. From the **Remote Files** panel, select the remote file associated with the component on which the inventory item you want to add is based (or will be based if you need to create an inventory item).

5. In the **Components** panel, locate the component version that you believe is the origin of the matching code in the scanned codebase file, and click the **Add File to Inventory** icon in that component row.

Code Insight searches for existing inventory items associated with the given component version. If one or more inventory items exist, the **Add to Inventory** dialog is displayed, showing the list of available inventory items. Continue with Step 7.

Otherwise, if no inventory items are currently associated with the given component version, the **Lookup Component** window is displayed, showing the given component version. From this window, you can register an instance for the component version (by selecting a license), register a new component version, search for a new component altogether, or create a custom component. Once you click **Use This Instance** for a component version in the **Lookup Component** window, Code Insight creates the inventory item based on the selected component instance.

6. Perform either of the following:
   - If you want to add the codebase file to one of the existing inventory items, continue with Step 8.
   - If you want to add the codebase a new inventory item, click **Add New** to open the **Lookup Component** window, showing the currently available instances for the component version. From this window, you can either select an instance on which to base the inventory item, register a new instance, search for a new component, or create a custom component. Once you click **Use This Instance** for a component version in the **Lookup Component** window, Code Insight creates the inventory item based on the selected instance.

7. Click the checkbox next to the inventory item to which you want to add the file.

8. (Optional) To mark the selected codebase file as reviewed, click **Mark file as reviewed**.

9. Click **Submit**. Code Insight adds the codebase file to the inventory item.
Using the Evidence Details Tab

You can view the following details for the evidence found in your codebase files:

- **Copyrights**—Lists the copyright text of potential third-party software code found in your codebase.
- **Email/URLs**—Lists email addresses and website URLs of potential owners of third-party software found in your codebase.
- **Licenses**—Lists the third-party licenses in your codebase that should be reviewed for IP compliance.
- **Search Terms**—Lists the search terms in your codebase based on the terms listed in the Scan Profile.

In addition to this detailed information, the **Evidence Details** tab provides the total number of files for each piece of evidence, and the total number of those files that have not been reviewed (Unreviewed).

To search for and display a tree view of files containing selected evidence, click the box in front of each piece of evidence listed, and click **Search Files**. A list of files in the codebase that contain that evidence appears in a tree view in the **File Search Results** pane.

Using the Inventory Details Tab

The **Inventory Details** tab allows you to manage details for a selected inventory item:

- **Using the Inventory Items Context Menu**
- **Viewing Security Vulnerabilities for Inventory in Analysis Workbench**
- **Viewing Details About Licenses Associated with Inventory in Analysis Workbench**
- **Viewing or Editing Inventory Usage Information from Analysis Workbench**
- **Viewing and Updating Detection and Auditing Notes in Analysis Workbench**
- **Component Lookup**
- **Creating an Inventory Item from the Analysis Workbench**
- **Editing Inventory from the Analysis Workbench**
- **Publishing or Recalling Inventory from Analysis Workbench**

Using the Inventory Items Context Menu

The **Inventory Items** pane has a context menu containing shortcuts to common inventory tasks. The following tasks are available on the context menu:

- **Publish Inventory**—Select inventory items that you would like to publish, right-click, and choose **Publish Inventory** to quickly publish your selected items. Publishing an inventory item makes it visible in the **Project Inventory** view.
- **Recall Inventory**—Select published inventory items that you would like to recall back to an unpublished state, right-click, and choose **Recall Inventory**. The selected items are removed from the **Project Inventory** view and are only visible in the **Analysis Workbench**.
Chapter 2 Using FlexNet Code Insight
Analyzing (Auditing) Scan Results

Note • Editing an inventory item does not require a recall of the inventory item. The item’s field values may be edited from the Analysis Workbench or the Project Inventory view at any time, even if the item has already been published.

- Show Inventory Files—To see files associated with the selected inventory items, select the list of inventory items, and right-click and choose Show Inventory Files. The associated files will be shown in the File Search Results pane.

- Delete Inventory—Select inventory items that you want to delete, right-click, and select Delete Inventory. The selected items will be deleted from the project.

Note • When you republish an inventory item by selecting the Recall and Publish tasks, the published date on the item is reset. This action in turn affects the age of the inventory item. Republished items are treated as newly published items.

Viewing Security Vulnerabilities for Inventory in Analysis Workbench

FlexNet Code Insight uses data from the National Vulnerability Database (NVD), Secunia advisories (as published by the Secunia Research team from Flexera), and other advisories such as RubySec to report security vulnerabilities associated with your inventory items. The vulnerabilities information from these sources is used to create vulnerability rankings and alerts.

Use this procedure to access details about the security vulnerabilities associated with an inventory item in Analysis Workbench.

**Task** To view security vulnerabilities for an inventory item, do the following:

1. From the Inventory Details tab for a selected inventory item in Analysis Workbench, locate the Vulnerabilities graph. (No graph is displayed if the inventory item has no known associated security vulnerabilities.)

   ![Vulnerabilities](image)

   The severities depicted on the graph differ depending on the CVSS version Code Insight is using (Security Vulnerabilities Associated with Inventory). This example shows vulnerability severity counts using CVSS v3.0.

2. Click any of the counts in the graph to open the Security Vulnerabilities dialog, which lists the current security vulnerabilities for the inventory item.

   For more information about how to use this dialog to obtain details about the vulnerabilities, see Security Vulnerabilities Associated with Inventory.

3. When you have finished viewing the reported vulnerabilities, click OK to return to the Inventory Items list.
Viewing Details About Licenses Associated with Inventory in Analysis Workbench

You can view more details about the licenses associated with the OSS or third-party component on which an inventory item is based. This information is pulled from the FlexNet Code data library and is displayed on the License Details window, which includes the following:

- A General Information tab that lists details such as the name of the license, its family, and the license priority assigned by FlexNet Code Insight.
- A License Text tab that displays the complete license text (representing the external forge license text).

While the forge license text is what is likely to be used by the component, the scan might have found actual license text associated with this component in your codebase that can be different from the forge version. To view the exact license text, if any, that the scan discovered and to prepare the final license text, when necessary, to include in the Notices report for distribution to customers, navigate to the Notices Text tab. Refer to Finalizing the Notices Text for the Notices Report for more information.

The following procedure describes how to access the License Details window from the Inventory Details tab in Analysis Workbench.

**Note** • This window is also accessible when create or edit an inventory item or perform a Component Lookup from Analysis Workbench.

### Task

<table>
<thead>
<tr>
<th>Task</th>
<th>To view details for the inventory license, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>From the Inventory Details tab for a selected inventory item in Analysis Workbench, locate the License field. This field lists the license currently that is associated with the component identified for the inventory item.</td>
</tr>
<tr>
<td>2.</td>
<td>Click the information icon (.) next to the License value. The License Details window appears with the General Information tab in focus. For descriptions of these fields on this tab, see License Details Window. Also see License Priority for background on how the license priority is used.</td>
</tr>
<tr>
<td>3.</td>
<td>Select the License Text tab to view the license text.</td>
</tr>
<tr>
<td>4.</td>
<td>When you have finished examining the license details, click Close.</td>
</tr>
</tbody>
</table>

Viewing or Editing Inventory Usage Information from Analysis Workbench

Inventory usage information is important because it aids users in determining how closely to monitor inventory items for intellectual property (IP) and security risk and in taking appropriate action to approve or reject inventory, create tasks for remediation, and issue alerts and notifications. Usage fields can determine whether the item should be included in Third-Party Notices and what steps need to be taken to satisfy license obligations and conditions of use. They can also help to identify license conflicts and compatibility issues.
Chapter 2  Using FlexNet Code Insight

Analyzing (Auditing) Scan Results

Task  To view or edit inventory usage information, do the following:

1. From the Inventory Details tab for a selected inventory item in Analysis Workbench, select the Usage tab.
2. View and, if necessary, edit the usage fields.
   
   For details about the inventory usage fields and how they are used, see Inventory Usage Information.

Viewing and Updating Detection and Auditing Notes in Analysis Workbench

The Notes tab can provide information about automated and manual analysis of codebase as it relates to an inventory item. This can help you in your analysis of your product’s use of the OSS or third-party software identified by the inventory item.

Task  To view notes, do the following:

1. From the Inventory Details tab for a selected inventory item in Analysis Workbench, select the Notes tab.
2. Review or update content in the following fields as needed:
   
   • Detection Notes—Information generated during the scan to explain the means by which OSS or third-party software was detected in the codebase. This information is not editable.
   
   • Audit Notes—Information recorded about the manual analysis of the codebase associated with this software. You can add your own notes. For example, you might indicate that you needed to create this inventory item manually.

3. Click Save in the upper right corner of the Inventory Details tab to save any updates to the Audit Notes field.

Component Lookup

Component Lookup is the search feature for inventory components. It allows you to gain more information about the vulnerabilities and potential license issues with items in your inventory, as described in these topics:

• Guidelines for Component Lookup
• Component Lookup Results
• Performing Component Lookup

Guidelines for Component Lookup

When possible, use the Forge or URL search for the most targeted search results, and use the Keyword search in other cases.

• Use the Forge option if you know the forge (project repository) of the component. For example, Github, NuGet Gallery, and PyPI are forges.
• Use the URL option if you know project URL or the forge URL. For example, https://github.com/jquery/jquery or http://jqueryui.com.
• Use the **Keyword** option to search all the component names in the FlexNet Code Insight data library. The component name is a unique identifier that may be based on the project name, package name, gem name, or other convention such as author and repository. The following are common conventions for component names:
  
  - **Github**— `<AUTHOR>-<REPOSITORY_NAME>`, for example “jquery-jquery-ui”
  - **NuGet Gallery**— `<PACKAGE_NAME>`, for example “newtonsoft.json”
  - **Apache**— `<PROJECT_NAME>`, for example “apache-batik”
  - **Pypi**— `<PACKAGE_NAME>`, for example “hash_ring”
  - **RubyGems**— `<GEM_NAME>`, for example “x-editable-rails”
  - **Other**— `<PROJECT_NAME>`, for example “openssl”

• If you cannot locate the component by keyword, select a **Forge** or **URL** search. If you are still unable to locate the component, the component might not exist in the FlexNet Code Insight data library. In this case, you have options to do one of the following:
  
  - Create your inventory item as **Work in Progress** and name it using the convention `<COMPONENT> <VERSION> (<LICENSE>)`. For example, `myComponent 1.2 (MIT)`. (You can later edit this inventory item to convert it to one of the other inventory types—**Component** or **License**.)
  - Create a custom component. See Creating and Editing Custom Components for details.

**Component Lookup Results**

Component Lookup search results are prioritized in the following order:

1. **Registered Components**—Components with a history of use (one or more instances of the component are registered for use in the system).
2. **Important Components**—Components that are marked by Flexera as important due to popularity or presence of security vulnerabilities.
3. **All other Components**—Components that are neither registered nor important.

If no results are returned, the component might not exist in the FlexNet Code Insight data library. See the previous section for options in dealing with components not available in the library.

**Performing Component Lookup**

<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>To perform a Component Lookup, do the following:</td>
</tr>
<tr>
<td>1. Open a project and navigate to <strong>Analysis Workbench</strong> (or the <strong>Project Inventory</strong> tab).</td>
</tr>
<tr>
<td>2. Select an inventory item from the list in the <strong>Inventory Items</strong> pane. The item appears in the <strong>Inventory Details</strong> pane. (For an item selected from the <strong>Project Inventory</strong> tab, you need to also click <strong>Edit Item</strong> to proceed with the next step.)</td>
</tr>
<tr>
<td>3. From the <strong>Type</strong> dropdown, select <strong>Component</strong> and click <strong>Lookup Component</strong>. The <strong>Lookup Component</strong> window appears.</td>
</tr>
</tbody>
</table>
4. Select the search type (Keyword, URL, or Forge), and enter the required search criteria. See Guidelines for Component Lookup.

Click Search to find components matching your search criteria. For information about the results of the Component Lookup, see Component Lookup Results.

Creating an Inventory Item from the Analysis Workbench

When you identify third-party code in your codebase, you should create an inventory item to record it. Inventory items contain information critical for review and approval. The process for creating inventory in the Analysis Workbench proceeds in the following way:

**Phase 1**—Filter files that contain evidence of third-party code, such as copyright text or content from an open source license. See Searching for Codebase Files Based on Search Criteria and Using the Evidence Details Tab.

**Phase 2**—Research the findings and identify the origin of the files.

**Phase 3**—Create an inventory item with details about the origin of the code. This is typically an open source project, such as zlib, OpenSSL, or ReactJS.

If you do not know code’s origin, you have options to create either a License Only inventory item (if the codebase files are governed by a common license) or a Work In Progress inventory item to serve as placeholder until you obtain more information. Inventory types are described in more detail in the procedure below.

**Phase 4**—When all of the evidence is explained in the files you are looking at (bearing in mind that some files might have code from several origins), mark the files as “reviewed”.

**Phase 5**—When you are finished creating inventory items, publish the ones you would like to report on. You can choose not to publish internal or test tools.

For more details about creating inventory items in the Analysis Workbench, see the following sections:

- Creating Inventory from the Inventory Items List
- Creating Inventory from the Codebase Lists

Creating Inventory from the Inventory Items List

This section describes how to create inventory from the Inventory Items list in the Analysis Workbench. (For instructions on creating inventory items for codebase files in Codebase Files list or File Search Results list in the Analysis Workbench, see Creating Inventory from the Codebase Lists.)

**Task**

To create inventory from the Inventory Items list, do the following:

1. If not already on the Analysis Workbench, navigate to it.
2. Navigate to the Inventory Items list.
3. Click Add New at the top of the Inventory Items list. A new item, showing default values, opens in its own tab in the Inventory Details pane.
4. For the Name field, perform the appropriate step, based on the inventory type you intend to select for the Type field (see the next step):
   - For inventory of the type Work in Progress, specify a name for the inventory item. Best practice is to provide a name in the following conventional syntax used by Code Insight, even if the elements represented in the name are not available in the data library:
     
     \(<\text{COMPONENT\_NAME}> \ <\text{VERSION}\> \ (\text{LICENSE\_NAME})\)
   - For inventory of the type Component or License only, leave the Name field blank. The field will be automatically populated based on the registered component or license instance.

5. From the Type dropdown, select the type of inventory item you want to create and perform the related step or steps:
   - Work in Progress—Create this type of inventory item if you want to quickly represent third-party code or an artifact without having to select an associated component, version, or license from the data library. (You can later edit this inventory item to convert it to one of the other inventory types.) This option is typically used if you need a placeholder or cannot find the associated element in the data library. Items of type Work in Progress are not affected by policies and do not receive vulnerability updates or alerts.
   - Component—Create this type of inventory item if you know the component, version, and license for the third-party code or artifact and either you are able to locate it in the Code Insight data library using the Component Lookup feature or you need to create it as a custom component because it is not in the library. This type of inventory is associated with a registered component instance—that is, a unique component-version-license combination—and is affected by policies and receives vulnerability updates and alerts.

The Component Lookup feature, made available when you select the Component type, enables you to associate the inventory item with an existing registered component instance (or a new instance that you create) or to create the custom component and instance to associate with the item.

The following are basic steps for using Component Lookup. For details, see Component Lookup.

a. Click the Lookup Component button to locate the component of interest (as described in the next steps) or to create a custom component and instance to associate with the inventory item (see Creating and Editing Custom Components for continued steps).

b. In the list of results, navigate to the appropriate component, and click Show Versions to display the list of registered instances for that component.

c. Click Use This Instance next to an existing registered instance to associate that instance with the inventory item.

or

Click Register New Instance to create a new instance. Complete the registration by selecting an existing component version (or choosing the Create Custom Version value to specify a new version) and then selecting the license to associate with the instance. Click Use This Instance next to the new instance to associate it with the inventory item. (If you register a new component instance when creating inventory, the registered instance becomes available for selection across the system.)

The Name and Description editable fields for the inventory item are automatically populated with information based on the registered instance you selected. Additionally, the Component and License fields are displayed, showing the component, its version, and the license for the instance.
• **License Only**—Create this type of inventory item if you know the license for the third-party code or artifact but do not know the component. (You can later edit this inventory item to convert it to one of the other inventory types.) This type of inventory is typically used for groups of files of unknown origin that are governed by a specific license. The inventory is affected by policies.

Simply select the appropriate license from **License Only** dropdown, which is enabled when you select this type.

The **Name** field for the inventory item is automatically populated with the name **Files under <LICENSE_NAME> License**, where `<LICENSE_NAME>` is license you selected.

6. Update the remaining fields if appropriate:

• **Description**—Provide any meaningful information about the inventory item. When the inventory type is **Component**, this field is automatically populated with information about the component, license, or both, but can be edited.

• **Url**—Enter the website for the third-party code or artifact represented by the inventory item.

• **Disclosed**—Indicate whether the third-party component or artifact represented by the inventory item was a known third-party dependency in your code before it was discovered by the scan or you.

• For **Distribution Type**, **Part of Product**, **Linking**, **Modified**, or **Encryption**, see **Inventory Usage Information**.

• **Workflow URL**—Enter the URL (or a text reference such as a Jira issue number) that points to the specific request-related data for this inventory item as found in your site’s external workflow system.

If a URL is entered here, it will display as a link (labeled as **View Associated Request**) on the **Inventory Details** tab in **Project Inventory**. This link enables the reviewer to easily access the workflow request data that tracks the status of open tasks for the inventory item.

If a string that provides reference information is entered here, it is not converted to a link on the **Inventory Details** tab. However, depending on the string content, it can still provide direction in locating appropriate data in the workflow system.

The value remains **None** if you enter no URL or reference.

Additionally, when you view the **Inventory Details** tab in **Project Inventory**, an **i** icon will be displayed next to the URL if additional request-related details are available for the inventory item. The reviewer can then click the icon for a quick review of pertinent details about the request without having to access the workflow system.

7. (Recommended) On the **Notes & Guidance** tab, add content to the **Audit Notes** field to indicate that this inventory item was manually created. This is helpful information for other auditors and for reviewers.

8. (Optional) Drag and drop one or more files from the **Codebase Files** list (or **File Search Results** list) to the **Associated Files** tab to associate files with the inventory item.

9. When you completed the details for the new inventory item, click **Save**. The name of the inventory item appears in the **Inventory Items** pane.

10. (Optional) To report on newly created or edited inventory items, click **Publish**.

### Creating Inventory from the Codebase Lists

This section describes how to “inventory” selected codebase files from the **Codebase Files** or **File Search Results** list in the **Analysis Workbench**, either by associating these files with existing inventory or by creating a new inventory item with which to associate them.
Alternatively, for instructions on creating inventory items from the **Inventory Items** list in the **Analysis Workbench**, see Creating Inventory from the Inventory Items List.

### Task
**To create an inventory item from the Codebase Files list, do the following:**

1. In the left pane of the **Analysis Workbench**, open a folder listed in the **Codebase Files** list or the **File Search Results** list.
2. Select and right-click one or more codebase files that you want to inventory. A pop-up menu is displayed.
3. Select **Add to inventory** from the popup menu to open the **Add to inventory** dialog.
4. Continue with either process:
   - Add Selected Codebase Files to Existing Inventory
   - Create a New Inventory Item with Which to Associate Selected Codebase Files

#### Add Selected Codebase Files to Existing Inventory

This procedure describes how to use the **Add to inventory** dialog to add the selected codebase files to one or more existing inventory items. (Steps to access the **Add to inventory** dialog are described in the preceding main procedure, Creating Inventory from the Codebase Lists.)

### Task
**To add the selected codebase files to existing inventory, do the following:**

1. In the **Add to inventory** dialog, select one or more inventory items to which to add the selected codebase file or files. (You can use the search field to search for the inventory.)
2. (Optional) Click **Mark files as reviewed**.
3. Click **Submit** to add codebase files to the **Associated Files** tab for each selected inventory item.

#### Create a New Inventory Item with Which to Associate Selected Codebase Files

This procedure describes how to use the **Add to inventory** dialog to add a new inventory item with which to associate the selected codebase files. (Steps to access the **Add to inventory** dialog are described in the preceding main procedure, Creating Inventory from the Codebase Lists.)

### Task
**To add a new inventory item with which to associated selected codebase, do the following:**

1. In the **Add to inventory** dialog, click **Add New**. A new inventory item “candidate”, showing default values, opens in its own tab on the **Inventory Details** tab.

   Note that the selected codebase files for which you are creating the inventory item are automatically added to the **Associated Files** tab for the new inventory item.

2. Complete the fields to define the new inventory item, as described in the previous section, Creating Inventory from the Inventory Items List.
3. (Optional) Drag and drop one or more additional files from the **Codebase Files** list (or **File Search Results** list) to the **Associated Files** tab.
4. When you completed the details for the new inventory item, click Save. The name of the inventory item appears in the Inventory Items pane.

### Editing Inventory from the Analysis Workbench

Use the following steps to edit an inventory item from the Analysis Workbench as needed.

<table>
<thead>
<tr>
<th>Task</th>
<th>To edit an inventory item in Analysis Workbench, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>If not already on the Analysis Workbench, navigate to it.</td>
</tr>
<tr>
<td>2.</td>
<td>Navigate to the Inventory Items list in the right pane.</td>
</tr>
<tr>
<td>3.</td>
<td>Select the inventory item that you want to edit.</td>
</tr>
<tr>
<td></td>
<td>A new tab, labeled with the inventory name and showing information about the inventory item, is opened within the Inventory Details tab.</td>
</tr>
<tr>
<td>4.</td>
<td>Make changes to the fields as needed. Refer to Creating Inventory from the Inventory Items List for field descriptions and additional steps required when updating the inventory type.</td>
</tr>
</tbody>
</table>

Note the following:

- For a Component inventory item, you can use the Component Lookup feature to select a different registered instance (or create a new one) or to create a custom component and instance to associate with the inventory item. The Name, Component, and License fields are updated accordingly.

- You can convert a Work In Progress or License Only inventory item to a different inventory type, using the Type field and performing the additional steps required for the type. The Name and other appropriate fields are updated accordingly.

- If you need to update the component version or associated license only, simply click the Edit (📝) icon next to the Component or License value, and select a different license or version or both. (This avoids performing a Component Lookup process to edit these elements.)

- Update any of the other fields as necessary.

5. Click Save to change the changes to the inventory item.

### Publishing or Recalling Inventory from Analysis Workbench

If you have performed manual work on your inventory items, you must publish the items to Project Inventory before anyone can review your work. Likewise, you can recall a published inventory item (that is, remove it from Project Inventory) for further auditing.

In Analysis Workbench, you publish or recall inventory from either the Inventory Details tab or the Inventory Items pane:

- Publish or Recall an Inventory Item from the Inventory Details Tab
- Publish or Recall Inventory from the Inventory Items Pane
Note • If you enabled the auto-publish feature in the project scan settings, you do not need to perform the steps below because system-created inventory items are automatically published.

### Publish or Recall an Inventory Item from the Inventory Details Tab

You these steps to publish or recall an inventory item from the Inventory Details tab.

**Task**

**To publish or recall an inventory item from its Inventory Details tab, do the following:**

For the unpublished inventory item currently in focus on the **Inventory Details** tab in **Analysis Workbench**, click the **Publish** button. The newly published item now appears in the **Inventory Items** list with a filled box icon before its name (and is now listed in **Project Inventory**).

or

For a published inventory item currently in focus, click the **Recall** button. The item now appears in the **Inventory Items** list with a clear box icon before its name (and is no longer listed in **Project Inventory**).

### Publish or Recall Inventory from the Inventory Items Pane

Use the following procedure to publish or recall one or more inventory items from the **Inventory Items** pane.

**Task**

**To publish or recall inventory from the Inventory Items pane, do the following:**

1. From the **Inventory Items** pane of the **Analysis Workbench**, select the items to publish so that a checkmark appears in front of each item.

   or

   Select the published items you want to recall so that a checkmark appears in front of each item.

   **Note** • If you do not see an inventory item you want to publish or recall, enter a term to search and click the search magnifier button.
Chapter 2  Using FlexNet Code Insight

Reviewing Published Inventory

2.  Right click to open the context menu, and choose either Publish Inventory or Recall Inventory.

- If you selected Publish Inventory, the newly published items appear in the Inventory Items list with a filled box icon before their names (and are now listed in Project Inventory).

- If you selected Recall Inventory, the recalled items appear in the Inventory Items list with a clear box icon before their name (and are no longer listed in Project Inventory).

Note • During the scan, inventory item priorities for auto-published inventory are automatically assigned based on the associated license.

Reviewing Published Inventory

The Project Inventory tab shows a list of all the inventory items that have been published for the current project, either automatically by the system or manually by a Reviewer or Analyst. From the Project Inventory tab, users can view details for the inventory item, and designated reviewers for the project can manage existing inventory (that is, set the status, change inventory priority, edit details, create and inventory, and manage review and remedial tasks).

Refer to the FlexNet Code Insight User Roles and Permissions appendix for the project roles (in addition to the Reviewer and Analyst roles) required to review and act on published project inventory.

The following topics describe the various actions you can perform review and manage project inventory:

- Goal of the Reviewer
- Displaying Project Inventory
- Searching Published Inventory
- Viewing Security Vulnerabilities for Project Inventory
- Viewing Details About the Licenses Associated with Project Inventory
- Viewing and Updating Notes and Guidance
- Viewing Usage Information for Project Inventory
- Viewing Associated Files
Goal of the Reviewer

The goal of the inventory review is to assess every inventory item and categorize it as approved or rejected for use in the current project based on your company policy. To review inventory, the user first must be assigned the role of Reviewer (or a role with Reviewer permissions). See Assigning Project Roles to Users.

Displaying Project Inventory

When an inventory item has been published, it can be reviewed, updated, and reported on from the Project Inventory tab. Use this procedure to display the Project Inventory tab.

<table>
<thead>
<tr>
<th>Task</th>
<th>To view project inventory, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open a project and click the Project Inventory tab. The Inventory Items list pane is displayed on the left.</td>
</tr>
<tr>
<td>2.</td>
<td>From the list, click the inventory item you want to review. Information about the selected item is displayed in the Inventory Details pane on the right.</td>
</tr>
<tr>
<td>3.</td>
<td>Select any of the tabs to display additional information about the inventory item.</td>
</tr>
<tr>
<td>4.</td>
<td>To view the published inventory items sequentially:</td>
</tr>
<tr>
<td></td>
<td>• Use the up and down arrows on your keyboard to step through inventory items quickly.</td>
</tr>
<tr>
<td></td>
<td>• Use the Next Item and Previous Item buttons to move among inventory items.</td>
</tr>
<tr>
<td>5.</td>
<td>You can view or change various details on the tabs, as well as change priority and status. For more information about the fields on the tabs, see Inventory Details Pane in Analysis Workbench.</td>
</tr>
</tbody>
</table>

Searching Published Inventory

FlexNet Code Insight provides the Advanced Search dialog to enable you to quickly filter the list of published inventory items to those of interest based on many available criteria—inventory attributes, selected license attributes, and associated security vulnerabilities, tasks, and security alerts. In this way, you can easily focus on only those inventory items in which you are interested within the list of published items. The following procedure shows you how to access and use this dialog. Refer also to the Performing Advanced Searches chapter for practical applications of this search feature.
Task  

To filter published inventory, do the following:

1. Open a project, and click the **Project Inventory** tab. The **Inventory Items** pane appears, showing the list of inventory items.

2. Click the **Advanced Search** button at the top of the list to open the **Advanced Inventory Search** dialog.

3. From this dialog, select search criteria as needed from the following categories. For a detailed description of the search criteria, see [Advanced Inventory Search Dialog](#).

   - **Inventory Items**—Search for inventory items that have a certain name (or string), priority, review status, or age or that have open vulnerability alerts and work items. (For details on alerts and work items, see [Managing Security Vulnerability Alerts](#) and [Creating and Viewing External Work Items for a Project Inventory Task](#).)

   - **Inventory Tasks**—Search for inventory items that have been assigned tasks. You can refine the search to locate inventory with open or closed tasks, tasks of a certain age or type (such as manual reviews or source-code remediation), or tasks assigned to a specific user.

   - **Security Vulnerabilities**—Search for inventory items that have vulnerabilities of a certain vulnerability ID, CVSS severity, or age. (Note that list of available severities for **Security Vulnerability Severity** varies depending on the CVSS version being used by Code Insight. The picture above shows the severities for CVSS v3.0. See [Security Vulnerabilities Associated with Inventory](#) for details.)
• **Licenses**—Search for inventory items that have licenses of a certain name or license priority.

4. Select **And** or **Or** from the **Apply Criteria** field.

5. Click **Apply** to filter the inventory to display only those inventory items that meet the selected criteria.

6. To refresh the list to show all inventory items, click **Show All Items**.

### Viewing Security Vulnerabilities for Project Inventory

FlexNet Code Insight uses data from the National Vulnerability Database (NVD), Secunia advisories (as published by the Secunia Research team from Flexera), and other advisories such as RubySec to report security vulnerabilities associated with your inventory items. The vulnerabilities information from these sources is used to create vulnerability rankings and alerts.

Use this procedure to access details for the vulnerabilities associated with an inventory item on the **Project Inventory** tab.

<table>
<thead>
<tr>
<th>Task</th>
<th>To view security vulnerabilities for an inventory item, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>If you are not there already, navigate to the <strong>Project Inventory</strong> tab.</td>
</tr>
<tr>
<td>2.</td>
<td>Click a published inventory item from the <strong>Inventory Items</strong> list.</td>
</tr>
<tr>
<td>3.</td>
<td>Select the <strong>Component Details</strong> tab. If known security vulnerabilities exist for the inventory item, the <strong>Vulnerabilities</strong> graph is displayed:</td>
</tr>
</tbody>
</table>

The severity levels depicted in the graph differ depending on the version of CVSS Code Insight is using (see Security Vulnerabilities Associated with Inventory). This example shows vulnerability severity counts using CVSS v3.0.

4. Click any of the counts in the graph to open the **Security Vulnerabilities** dialog, which list current security vulnerabilities for the inventory item.

   For more information about how to use this dialog to obtain details about the vulnerabilities, see Security Vulnerabilities Associated with Inventory.

5. When you have finished viewing the reported vulnerabilities, click **OK** to return to the **Inventory Items** list.

### Viewing Details About the Licenses Associated with Project Inventory

You can view more details about the licenses associated with the OSS or third-party component on which the current inventory item is based. This information is pulled from the FlexNet Code data library and is displayed on the **License Details** window, which includes the following:

- A **General Information** tab that lists details such as the name of the license, its family, and the license priority assigned by FlexNet Code Insight.

- A **License Text** tab that displays the complete license text (representing the external forge license text).
While the forge license text is what is likely to be used by the component, the scan might have found actual license text associated with this component in your codebase that can be different from the forge version. To view the exact license text, if any, that the scan discovered and to prepare the final license text, when necessary, to include in the Notices report for distribution to customers, navigate to the Notices Text tab. Refer to Finalizing the Notices Text for the Notices Report for more information.

The following procedure describes how to access the License Details window from the Component Details tab on the Project Inventory tab.

**Note** • This window is also accessible when create or edit an inventory item or perform a Component Lookup from the Project Inventory tab.

**Task**  
**To view details for the inventory license, do the following:**

1. If you are not there already, navigate to the Project Inventory tab.
2. Select a published inventory item from the Inventory Items list.
3. Do either:
   - For a component-based inventory item, click the Component Details tab. Then click information icon ( ) next to the Selected License value (the license currently associated with the component) or the Possible Licenses (other valid license candidates with which you could associate the inventory item).
   - For a License Only inventory item, click the License Details tab, and then click the information icon ( ) next to the license name.

   The License Details window appears with the General Information tab in focus. For descriptions of these fields on this tab, see License Details Window. Also see License Priority for background on how the license priority is used.

4. Select the License Text tab to view the license text.
5. When you have finished examining the license details, click Close.

**Viewing and Updating Notes and Guidance**

The Notes & Guidance tab can provide notes about the automated and manual analysis performed on the codebase as it relates to the current inventory item. The tab can also include guidance on how to remediate issues associated with your product’s use of the OSS or third-party software identified by the inventory item.

**Task**  
**To view notes and guidance, do the following:**

1. If you are not there already, navigate to the Project Inventory tab.
2. Select an inventory item from list.
3. Select the Notes & Guidance tab.
4. Review or update content in the following fields as needed. All information is editable except for the information in the Detection Notes field:

- **Detection Notes**—Information generated during the scan to explain the means by which OSS or third-party software was detected in the codebase. This information is not editable.
- **Audit Notes**—Information recorded about the analysis of the codebase associated with this software. For example, these notes might indicate that the inventory item needed to be manually created.
- **Usage Guidance**—Any information about why and how your product is using the software and any requirements for using the software.
- **Remediation Notes**—A description of items to be addressed or actions to be taken before the use of this software in your product is acceptable from a legal or security standpoint.

5. Click **Save** in any field in which you have made changes.

6. When you have finished with this tab, navigate to another tab for the inventory item, or select another inventory item.

### Viewing Usage Information for Project Inventory

Inventory usage information is important because it aids users in determining how closely to monitor inventory items for intellectual property (IP) and security risk and in taking appropriate action to approve or reject inventory, create tasks for remediation, and issue alerts and notifications. Usage fields can determine whether the item should be included in Third-Party Notices and what steps need to be taken to satisfy license obligations and conditions of use. They can also help to identify license conflicts and compatibility issues.

---

**Task**

**To view inventory usage information, do the following:**

1. If you are not there already, navigate to the **Project Inventory** tab.
2. Click an inventory item from the **Inventory Items** list.
3. Select the **Usage** tab in the inventory details. For details about the inventory usage fields and how they are used, see **Inventory Usage Information**.

### Viewing Associated Files

Associated files are files that were found in your codebase and are associated with the inventory item selected in the **Inventory Items** pane.

---

**Task**

**To view associated files, do the following:**

1. If you are not there already, navigate to the **Project Inventory** tab.
2. Click an inventory item from the **Inventory Items** list.
3. Select the **Associated Files** tab in the inventory details. A list of files associated with the selected inventory item appears.
4. When you have finished viewing associated files, select another tab or click another item listed in the Inventory Items pane.

Creating Inventory from the Project Inventory Tab

Reviewers can create an inventory item to represent any third-party code or artifact that is not automatically detected by the system.

Use the following steps to create an inventory item from the Project Inventory tab as needed. Note the following:

- When you save the inventory item, it is automatically published.
- No files can be associated with an inventory item when it is created from the Project Inventory tab.
- If you register a new component instance (a unique component-version-license combination) when creating inventory, the registered instance becomes available for selection across the system.
- Inventory of type **Work in Progress**, **Component**, or **License Only** can be created.

**Task**

To create an inventory item from the Project Inventory tab, do the following:

1. Navigate to the Project Inventory tab.
2. Click Add Item at the top of the Inventory Items list.

The New Inventory dialog opens.

3. For the Name field, perform the appropriate step, based on the inventory type you intend to select for the Type field (see the next step):
   - For inventory of the type **Work in Progress**, specify a name for the inventory item. Best practice is to provide a name in the following conventional syntax used by Code Insight, even if the elements represented in the name are not available in the data library:
     
     `<COMPONENT_NAME> <VERSION> (LICENSE_NAME)`
   - For inventory of the type **Component** or **License only**, leave the Name field blank. The field will be automatically populated based on the registered component or license instance.

4. From the Type dropdown, select the type of inventory item you want to create and perform the related step or steps:
   - **Work in Progress**—Create this type of inventory item if you want to quickly represent third-party code or an artifact without having to select an associated component, version, or license from the data library. (You can later edit this inventory item to convert it to one of the other inventory types.) This option is typically used if you need a placeholder or cannot find the associated element in the data library. Items of type **Work in Progress** are not affected by policies and do not receive vulnerability updates or alerts.
• **Component**—Create this type of inventory item if you know the component, version, and license for the third-party code or artifact and you either are able to locate it in the Code Insight data library using the Component Lookup feature or you need to create it as a custom component because it is not in the library. This type of inventory is associated with a registered component instance—that is, a unique component-version-license combination—and is affected by policies and receives vulnerability updates and alerts.

The Component Lookup feature, made available when you select the **Component** type, enables you to associate the inventory item with an existing registered component instance (or a new instance that you create) or to create the custom component and instance to associate with the item.

The following are basic steps for using Component Lookup. For more details, see Component Lookup.

a. Click the **Lookup Component** button to locate the component of interest (as described in the next steps) or to create a custom component and instance to associate with the inventory item (see Creating and Editing Custom Components for continued steps).

b. In the list of results, navigate to the appropriate component, and click **Show Versions** to display the list of registered instances for that component.

c. Click **Use This Instance** next to an existing registered instance to associate that instance with the inventory item.

or

Click **Register New Instance** to create a new instance. Complete the registration by selecting an existing component version (or choosing the **Create Custom Version** value to specify a new version) and then selecting the license to associate with the instance. Click **Use This Instance** next to the new instance to associate it with the inventory item.

The **Name** and **Description** editable fields for the inventory item are automatically populated with information based on the registered instance you selected. Additionally, the **Component** and **License** fields are displayed, showing the component, its version, and the license for the instance.

• **License Only**—Create this type of inventory item if you know the license for the third-party code or artifact but do not know the component. (You can later edit this inventory item to convert it to one of the other inventory types.) This type of inventory is typically used for groups of files of unknown origin that are governed by a specific license. The inventory is affected by policies.

Simply select the appropriate license from **License Only** dropdown, which is enabled when you select this type.

The **Name** field for the inventory item is automatically populated with the name **Files under <LICENSE_NAME> License**, where `<LICENSE_NAME>` is license you selected.

A **License Details** tab is added, enabling to view details about the license selected for the inventory item.

5. Update the remaining fields if appropriate:

• **Description**—Any meaningful information about the inventory item. When the inventory type is **Component**, this field is automatically populated with information about the component, license, or both, but can be edited.

• **Url**—The website for the third-party code or artifact represented by the inventory item.

• **Disclosed**—Indicates whether the third-party component or artifact represented by the inventory item was a known third-party dependency in your code before it was discovered by the scan or you.

• For **Distribution Type**, **Part of Product**, **Linking**, **Modified**, or **Encryption**, see Inventory Usage Information.
• **Workflow URL**—Enter the URL (or a text reference such as a Jira issue number) that points to the specific request-related data for this inventory item as found in your site’s external workflow system.

Once you save this new item, the *Inventory Details* pane for the new item displays the URL as a link (labeled as *View Associated Request*), enabling the reviewer to easily access the workflow request data that tracks the status of open tasks for the inventory item.

If you enter a text reference, it is not converted to a link on the *Inventory Details* pane, but it still provides direction in locating the appropriate data in the workflow system.

The value remains **None** if you enter no URL or reference.

If additional request-related details are later made available for this inventory item, the ![icon](image) icon will be displayed next to the URL. You can click the icon to open the *Workflow Request Details* window for a quick review of pertinent details about the request without having to access the workflow system.

---

**Note** • These details come from the specific external workflow system associated with your site. The details can vary based on your workflow system.

6. Click **Save**. The name of the inventory item is added to the *Inventory Items* list.

7. (Optional) If you created a License Only inventory item, view details about the license selected for the new inventory item on the *Licenses Details* tab in the right pane.

---

**Editing Inventory from the Project Inventory Tab**

Use the following steps to edit an inventory item from the *Project Inventory* tab as needed.

---

**Task**  
*To edit an inventory item from the Project Inventory tab, do the following:*

1. Navigate to the *Project Inventory* tab.

2. In the *Inventory Items* list, select the inventory item that you want to edit. Information about the inventory item is displayed in the right pane.

3. In the header on the right pane, click the **Edit Item** button next to the component name.

The *Edit Inventory* dialog opens.

4. Make changes to the fields as needed. Refer to *Project Inventory Details Pane* for field descriptions and additional steps required when updating the inventory type. Note the following:

• For a **Component** inventory item, you can use the Component Lookup feature to select a different registered instance (or create a new one) or to create a custom component and instance to associate with the inventory item. The *Name*, *Component*, and *License* fields are updated accordingly.
Chapter 2  Using FlexNet Code Insight
Reviewing Published Inventory

- You can convert a **Work In Progress** or **License Only** inventory item to a different inventory type, using the **Type** field and performing the additional steps required for the type. The **Name** and other appropriate fields are updated accordingly.

- If you need to update the component version or associated license only, simply click the Edit (✏️) icon next to the **Component** or **License** value, and select a different license or version or both. (This avoids performing the longer Component Lookup process to edit these elements.)

- Update any of the other fields as necessary.

- No additional files can be associated with an inventory item from **Project Inventory** tab.

5. Click **Save** to change the changes to the inventory item.

### Approving or Rejecting Inventory Items

The next step in the FlexNet Code Insight workflow is to have security and legal experts review all published inventory and categorize them as approved or rejected for use in the software project. To approve or reject an inventory item, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To approve or reject inventory items, do the following:</strong></td>
<td></td>
</tr>
<tr>
<td>1. Navigate to the <strong>Inventory Items</strong> list.</td>
<td></td>
</tr>
<tr>
<td>2. On the line for the inventory item you want to approve or reject, click the green checkmark to approve the item or the red X to reject the item.</td>
<td></td>
</tr>
</tbody>
</table>

A circle appears around the status icon to indicate it has been selected. A circle around the question mark indicates that no status selection has been made (that is, the inventory item requires further review to determine its status).

Note that, depending on the inventory review and remediation options defined for the project, selecting the **Reject** status can automatically create a Remediate Inventory task. For more information, see *Updating Inventory Review and Remediation Settings for a Project.*

### Creating and Managing Tasks for Project Inventory

Users with access to the project inventory (and edit privileges) can create one or more tasks for a given inventory item. Tasks can be one of three types:

- **Manual Review Inventory**—A task to track the manual review of an inventory item, typically for an inventory item that has not already been auto-reviewed by policy. A manual inventory task alerts the assignee to the need to review the inventory item for use in the current context and to either approve or reject it based on the review. In the case that there is only one manual review task for the inventory item, the inventory status will be updated to Approved or Rejected.

- **Remediate Inventory**—A task to track the remediation efforts of an inventory item, typically for a rejected inventory item. A remediation task signals to the assignee to perform some action to make the inventory item acceptable for use (for example, to upgrade to a new version due to discovered vulnerabilities or to use a specific license and to comply with license obligations). Closing remediation tasks does not affect the inventory status.

- **Miscellaneous**—A task to track any other effort for an inventory item.
The following topics are described in this section:

- Note About External Work Items
- Manually Creating a Task
- Editing a Task

**Note About External Work Items**

If the project is configured to connect to an external ALM (application lifecycle management) system such as Jira, each task can also have one or more associated work items that correspond to issues in the external ALM system. Work items are useful for tracking work that needs to be performed outside of Code Insight. A work item can be created manually using the Create Work Item option or automatically based on the current project settings defined by the Project Owner (as described in Updating Inventory Review and Remediation Settings for a Project). You can create work items only if the project is associated to an ALM instance, which, in turn, defines a set of attributes used to connect to the ALM system and to set up and assign issues. The administrator configures one or more global ALM instances; but, once the project is associated with one of these instances, you can customize the instance to address the needs of the project.

See for ALM Settings details about associating a project with an ALM instance. For more information about managing external work items, see Creating and Viewing External Work Items for a Project Inventory Task.

Currently, Code Insight supports the creation of issues on a Jira server only.

**Manually Creating a Task**

The following procedure describes the manual process for creating a task.

Note that a task can also be created automatically in an automated workflow process (along with external work items) based on review and remediation options that the Project Owner sets up for the project, as described in Updating Inventory Review and Remediation Settings for a Project.

<table>
<thead>
<tr>
<th>Task</th>
<th>To create a task manually, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to the <strong>Project Inventory</strong> page.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the inventory item to which you want to add a task. Alternatively, to help you locate the inventory item, click the <strong>Advanced Search</strong> button to open the <strong>Advanced Inventory Search</strong> dialog. From here you can filter inventory items accordingly. When you select the specific inventory item, the <strong>Inventory Details</strong> tab for the item is displayed.</td>
</tr>
<tr>
<td>3.</td>
<td>In the <strong>Tasks</strong> section, click the <strong>Create Task</strong> button to open the <strong>Create Task</strong> dialog.</td>
</tr>
</tbody>
</table>
4. Select the type of task you want to create—**Manual Inventory Review**, **Remediate Inventory**, or **Miscellaneous**. (Refer to the descriptions of task types earlier in this section.)

5. Complete the following fields as needed:
   - In the **Summary** field, provide a summary or title for the task.
   - In the **Details** field, provide instructions or requirements for completing this task (or provide any information that will be useful to the reviewer).
   - Keep the **Status** as **Open** for a new task.

6. By default, the new task is assigned to the default point of contact (defined for the project), as listed in the **Owner** field. To change the task owner, click the **Assign** button under the **Owner** field, and select a new owner.

7. To create an external work item associated with the task, click the **Create Work Item** button. (See Creating and Viewing External Work Items for a Project Inventory Task for details.)
   
   A “Success” message is displayed if the work item is created successfully on the corresponding ALM system (currently, a Jira server) associated to this project.
   
   You can repeat this step to create another work task.

8. Click **Save** to create the task.

### Editing a Task

The following describes how to edit or change the status of a task associated with an inventory item.

<table>
<thead>
<tr>
<th>Task</th>
<th>To edit a task, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to the <strong>Project Inventory</strong> page.</td>
</tr>
</tbody>
</table>
2. Select the inventory item to which the task you want to edit is associated. Alternatively, click the Advanced Search button to open the Advanced Inventory Search dialog, where you can select filters that help you pinpoint the inventory item. For example, you can select to filter on those inventory items associated with tasks that are assigned to a specific user or created within a certain date range.

When you select the specific inventory item, the Inventory Details tab for the item is displayed.

3. In the Tasks section, click the x Open Tasks or x Closed Tasks link to view the Tasks list for the inventory item. (Use the search filter at the top of the dialog to show All, Open, or Closed tasks.

4. Locate the appropriate task from the Tasks list, and click the link in the Summary column to show the Task Details dialog.

5. Use the information in Manually Creating a Task for updating the task fields or adding an external work item. To change the status of the task, see either Closing or Reopening a Review Task or Closing or Reopening a Remediation or Miscellaneous Task.

6. Click Save to save the updates.

Closing or Reopening a Review Task

You can close a Manual Inventory Review task by setting its status to Approve or Reject, which, in turn, has an effect on the status of the inventory item, as follows:

- If the inventory item has only one review task associated with it, the Approve or Reject status of the task sets the inventory item status to Approve or Reject accordingly.

- If the inventory item has two or more review tasks associated with it, the Reject status of a single review task automatically sets the inventory item status to Reject. All review tasks are closed but can be reopened for further investigation.

- If an inventory item has two or more review tasks associated with it and these tasks are a combination of open tasks and tasks with an Approve status, the inventory item retains its Not Reviewed status.

Note that, depending on the inventory review and remediation options defined for the project, the Reject status that is automatically set when you close a Manual Inventory Review task can automatically create a Remediate Inventory task. For more information about these options, see Updating Inventory Review and Remediation Settings for a Project.
To close or reopen a Manual Inventory Review task, do the following:

1. In the Status section on the Task Details dialog, do either:
   - To close an open task, click the Close Task button and select Approved or Rejected from the Resolution Type pop-up box.
   - To reopen a closed task, click the Reopen button.

2. Click Close.

Closing or Reopening a Remediation or Miscellaneous Task

You can close or reopen a Remediate Inventory or Miscellaneous task.

Note that closing a remediation task does not affect the inventory status; you must manually change the status of the inventory item. Likewise, the status of an external work item associated with the task does not affect the task status. If you want to change the task status based on the status of its external work items, you must do so manually.

To close or reopen a Remediate Inventory or Miscellaneous task, do the following:

1. In the Status section on the Task Details tab, do either:
   - To close an open task, click the Close Task button. If applicable, edit the Details field with information about how the item was remediated and why the task is being closed.
   - Click the Reopen Task button to reopen a closed task. If applicable, edit the Details field with information as to why the task is being re-opened.

2. Click Close.

Creating and Viewing External Work Items for a Project Inventory Task

Users with access to the project inventory (and edit privileges) can create one or more external work items for a task associated with a given inventory item. Each work item in Code Insight contains a corresponding ALM (application lifecycle management) issue on the ALM system (such as Jira) configured for the project.

The following topics are described in this section:

- Prerequisite
- Manually Creating a Work Item
- Viewing a Work Item
Prerequisite

You can create work items only if your project has been associated with an ALM instance. See for ALM Settings details about defining this association. Currently, Code Insight supports the creation of issues on a Jira server only.

Manually Creating a Work Item

The following procedure describes the manual process for creating an external work item for a task.

Note that an external work item can also be created automatically in an automated workflow process based on options that you can set up for the project. See Updating Inventory Review and Remediation Settings for a Project for details on editing the automated workflow options and Edit Project: Review and Remediation Settings Tab for field descriptions.

<table>
<thead>
<tr>
<th>Task</th>
<th>To create a work item manually, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to the Project Inventory page.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the inventory item associated with the task to which you want to add a work item. Alternatively, click the Advanced Search button to open the Advanced Inventory Search dialog, where you can select filters that help you pinpoint the inventory item. For example, you can select to filter on those inventory items associated with tasks that are assigned to a specific user or created within a certain date range. When you select the specific inventory item, the Inventory Details tab is displayed.</td>
</tr>
<tr>
<td>3.</td>
<td>Click the x Open Tasks link to view the list of open tasks for the inventory item.</td>
</tr>
<tr>
<td>4.</td>
<td>Locate the appropriate task from the Tasks list, and click the link in the Summary column to show the Task Details dialog.</td>
</tr>
<tr>
<td>5.</td>
<td>Click the Create Work Item button. The New Work Item page is displayed.</td>
</tr>
</tbody>
</table>

Note • The Create Work Item button is enabled only if the project has been associated with an ALM instance, as described in ALM Settings.

| 6.   | Complete the fields to define the work item. See the inline help for field descriptions. |
|      | This page might already contain default field values based on the project or global application defaults; you can override these values as needed. |

| 7.   | Click Create Work Item. |
|      | A “Success” message is displayed if the work item is created successfully on the corresponding ALM system (currently, a Jira server) associated to this project. |
|      | You are returned to the Task Details dialog. |

| 8.   | Verify that the item was created successfully by clicking the # Open Work Items link in the Work Items section on the Task Details dialog. Then click the External ID link for the issue. The link should connect you with the external Jira server and open the issue that corresponds to the work item. |
Viewing a Work Item

An inventory item containing one or more work items displays an information icon in the upper right-hand corner of its Inventory Details tab. The External Issues field contains links to the open and closed work items.

<table>
<thead>
<tr>
<th>Task</th>
<th>To view a work item, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to the Inventory Details tab for the inventory item associated with the task containing the work item.</td>
</tr>
<tr>
<td>2.</td>
<td>Click the # Open Tasks link. The Tasks list is displayed.</td>
</tr>
<tr>
<td>3.</td>
<td>In the External Issues column for the task containing the work item, click either the # Open Work Items or # Closed Work Items link. The Work Items window is displayed.</td>
</tr>
<tr>
<td>4.</td>
<td>Use the search filter at the top of the window to show All, Open, or Closed work items.</td>
</tr>
<tr>
<td>5.</td>
<td>Click the External ID link for the work item to open the issue in Jira.</td>
</tr>
</tbody>
</table>

Recalling a Published Inventory Item

You can recall (remove) a published inventory item from Inventory Items list if it does not fit the criteria for inclusion. Recalling the item and publishing it again will affect the publish date on the item as well as the age of the inventory item. A Recall is not required to make edits to the inventory item.

<table>
<thead>
<tr>
<th>Task</th>
<th>To recall a published inventory item, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to the Inventory Details page.</td>
</tr>
<tr>
<td>2.</td>
<td>Click Recall Inventory Item. The item is removed from the Inventory Items list.</td>
</tr>
</tbody>
</table>

Managing Security Vulnerability Alerts

FlexNet Code Insight provides the ability to view and clear security vulnerability alerts. When the Electronic Update process is run, it will generate these alerts for any new security vulnerabilities that impact inventory. The alerts allow you to investigate the most recent vulnerabilities and their effect on your project code, if any. Once you have addressed vulnerability impact, either by determining no impact exists or through remediation, you can close the alert.

When the Electronic Update generates security vulnerability alerts, email notifications are sent to the owners of projects with inventory impacted by the alerts. Additionally, users can view the alerts for a given project from the Inventory Details pane in Analysis Workbench or from the Project Inventory tab.

Refer to these topics for more information:

- Accessing Security Vulnerability Alerts
- Using the Alerts Dialog to Manage Alerts
Chapter 2 Using FlexNet Code Insight
Managing Security Vulnerability Alerts

Accessing Security Vulnerability Alerts

The following methods provide access to the Alerts dialog, which allows you to view and manage the security vulnerability alerts impacting inventory in a given project:

- From Email Notifications
- From Analysis Workbench
- From Project Inventory

**From Email Notifications**

Project Owners can be alerted via email to any projects and inventory items that contain new security vulnerabilities so that they can be reviewed and acted upon if necessary. For email alerts to be sent, the email server must be enabled and configured. For more information, see “Configuring an Email Server” in the Installation & Configuration Guide.

Vulnerability alert emails are sent as part of the Electronic Update. A vulnerability alert is generated for each new security vulnerability mapped to a published inventory item. While viewing the alert email, click any of the hyperlinked text in the email to open FlexNet Code Insight or an advisory web site to view additional information about the alert.

**From Analysis Workbench**

This procedure describes how to access security vulnerability alerts from Analysis Workbench.

**Task**

*To view security vulnerability alerts from Project Inventory, do the following:*

1. Open the Analysis Workbench tab for a project.
2. From the Inventory Item pane on the right, click the inventory item for which you want to check for alerts. The Inventory Details tab for the selected item is opened.

   If open alerts exist, the Alerts field provides a link to view them. If no alerts exist, the field shows None.

3. Click the link to open the Alerts dialog, where you can view the open (and closed) alerts for the inventory item.

**From Project Inventory**

This procedure describes how to access the security vulnerability alerts for a specific inventory item from the Project Inventory tab for a project.
To view security vulnerability alerts from Project Inventory, do the following:

1. Open the **Project Inventory** tab for a project. The **Inventory Items** list is displayed in the left pane.

2. (Optional) To filter the **Inventory Items** list to show only inventory that have alerts, click **Advanced Search**, select the **Inventory with Open Alerts** option, and click **Apply**.

3. From the **Inventory Items** list, click the inventory item whose alerts you want to check. Information about the selected inventory item is displayed in the right pane.

   - For a quick check on any open alerts, locate for the icon in the header of this page.

   - To view open or closed alerts, open the **Inventory Details** tab in the right pane. If alerts exist, the **Alerts** field shows separate links to view open or closed alerts, as appropriate.

4. Click the associated link to open the **Alerts** dialog, where you can view details about the alerts.
Using the Alerts Dialog to Manage Alerts

The **Alerts** dialog shows the list of current alerts for a given inventory item in a project. The following describes how to use this dialog to manage security vulnerability alerts for an inventory item:

- **Alert Details**
- **Changing the Priority of an Alert**
- **Changing the Status of an Alert**

### Alert Details

The following columns describe each alert entry listed in the **Alert** dialog. To filter the list of alerts, see [Filtering Alerts](#).

**Table 2-5 • Information on the Alerts dialog**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>The alert type. Currently, only <strong>New Vulnerability</strong> alerts are available.</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>The date that the alert was generated.</td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>The priority of the alert, which, by default, is based on the official severity level of the security vulnerability associated with the alert, as described here:</td>
</tr>
<tr>
<td>- <strong>High</strong></td>
<td>The default when the vulnerability severity level is Critical, High, or None in the CVSS v3.0 scoring system or, in the CVSS v2 scoring system, High or Unknown.</td>
</tr>
<tr>
<td>- <strong>Medium</strong></td>
<td>The default when the severity level is Medium in either scoring system.</td>
</tr>
<tr>
<td>- <strong>Low</strong></td>
<td>The default when the severity level is Low in either scoring system. You can change this value as needed. See <a href="#">Changing the Priority of an Alert</a>.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>The status of the alert in FlexNet Code Insight:</td>
</tr>
<tr>
<td>- <strong>Open</strong></td>
<td>The alert needs to be addressed.</td>
</tr>
<tr>
<td>- <strong>Closed</strong></td>
<td>The alert has been addressed (usually because remediation was performed or it was determined to be a false positive for your code). The icon is shown to identify who closed the alert and when. Change this value as needed. See <a href="#">Changing the Status of an Alert</a>.</td>
</tr>
</tbody>
</table>

For more information about the severity levels for security vulnerabilities, see [Viewing Security Vulnerabilities for Project Inventory](#).
Filtering Alerts

Use the following procedure to change the view of the list of alerts on the Alerts dialog.

1. Locate the dropdown at the top of the Alerts dialog:

   ![Alerts dialog screenshot](image)

2. Select one of the following options from the dropdown:
   - **Show Open Alerts**—Display only open alerts.
   - **Show Closed Alerts**—Display only closed alerts.
   - **Show All Alerts**—Display both closed and open alerts. This option will only be available if more than one alert is available.

---

**Table 2-5 • Information on the Alerts dialog (cont.)**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td>Details about the security vulnerability:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Source</strong>—The advisory database in which the Code Insight located the vulnerability, such as NVD (National Vulnerability Database), Secunia (Secunia Advisories), Debian Advisories, or others.</td>
</tr>
<tr>
<td></td>
<td>- <strong>ID</strong>—The identification number of the vulnerability associated with the Common Vulnerabilities and Exposures (CVE). If this is a hyperlinked value, click it to go to the actual entry for the vulnerability on the advisory website.</td>
</tr>
<tr>
<td></td>
<td>- <strong>CVSS Score</strong>—The score of the vulnerability based on the Common Vulnerability Scoring System (CVSS). The values of the CVSS score range from 0.1 to 10, with 10 being the most serious. If the vulnerability has no score, the value is N/A.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Description</strong>—The description of the vulnerability as found in the advisory database.</td>
</tr>
</tbody>
</table>

Also see Security Vulnerabilities Associated with Inventory.
Chapter 2  Using FlexNet Code Insight
Creating and Editing Custom Components

Changing the Priority of an Alert

Use the following procedure to change the High, Medium, or Low priority of an alert. The priority indicates the urgency with which the security vulnerability associated with the alert needs to be addressed. The initial priority value defaults to the severity of the security vulnerability itself, but you can change this priority based on your site’s needs. For more information about vulnerability priority, see Alert Details.

**Note** • If the FlexNet Code administrator has switched Code Insight from CVSS v2 to CVSS v3.0 scoring or vice versa, you might notice a change in the Severity and CVSS Score for the vulnerability associated with the alert. However, the alert Priority should not change from its value current at the time of the switch.

**Task**  To change the priority of a security vulnerability alert, do the following:

1. Open the Alerts dialog for a given inventory item in a project, as described in Accessing Security Vulnerability Alerts.
2. In the Priority column, select the new priority.

Changing the Status of an Alert

Use the following procedure to change the Open or Closed status of a security vulnerability alert. Usually, you close an alert because the associated security vulnerability has been addressed in your product through remediation or the alert is a false positive. You might need to reopen an alert because further remediation is required.

For more information about the Open and Closed statuses, see Alert Details.

**Task**  To change the status of a security vulnerability alert, do the following:

1. Open the Alerts dialog for a given inventory item in a project, as described in Accessing Security Vulnerability Alerts.
2. In the Status column for a given alert, select either option from the dropdown:
   • Open to reactivate the alert.
   • Closed to indicate that the alert has been addressed.

Creating and Editing Custom Components

FlexNet Code Insight enables you to create custom components that represent OSS or third-party software not found in the Code Insight data library or that represent commercial software that you want to track as part of your Bill of Materials. A custom component is currently created or edited within the context of the inventory item with which it is associated, but is saved to the data library and made available for global use.

Once the custom component is created, an inventory item can be associated with a registered instance of the component—that is, a unique component-version-license combination that you define. The custom component is also available for use by policies and is included in the Notices report.
The following topics describe how to create and edit custom components:

- Creating a Custom Component
- Editing a Custom Component
- Custom Component Properties
- Supported Forge-URL Domains for Custom-Component Creation

Creating a Custom Component

Use the following steps to create a custom component:

- Step 1: Access the Component Lookup Feature
- Step 2: Create the Custom Component
- Step 3: Associate an Instance of the Custom Component with the Inventory Item

Step 1: Access the Component Lookup Feature

You create a custom component within the context of Component Lookup feature. Follow these steps to access that feature.

Task

To access the Component Lookup feature, do the following:

1. From the page on which you are creating or editing inventory in Analysis Workbench or from the Project Inventory tab, select Component in the Type field for the inventory item.

2. Click Lookup Component to open the Lookup Component window.

Step 2: Create the Custom Component

Based on the information you have about the custom component you want to create, use one of the following methods to create the component.

- Create the Custom Component Based on a Keyword in Its Name or Title
- Create the Custom Component Based on Its Project or Forge URL
- Create the Custom Component Based on Its Forge
- Create the Custom Component in Free Form
Create the Custom Component Based on a Keyword in Its Name or Title

Use the following method to create the custom component based on a keyword in the name or title you intend to give the component.

Task

To create a custom component based on a keyword in its name or title:

1. On the Lookup Component window, select the Keyword option.
2. In the Keywords field, enter a keyword used in the name of the component you are creating.
3. (Optional) Click Search to see the list of existing components whose names contain the keyword. If the component you intend to create already exists, you can select an instance of the already existing component to associate with the inventory item, or you can continue to create a custom component with different name and title (continue with the next step).
   Keep in mind that the name and title of a component you create must be unique in the FlexNet Code Insight data library.
4. Click Create New Component to open the New Custom Component window, showing the Name and Title fields automatically populated with the keyword you entered.

   Note that window opens in the Free Form format, enabling you to add missing values and edit pre-populated values for the component as needed.
5. Update the component fields as necessary, noting that the Name, Title, and URL fields are required. (Click in the upper part of the window for examples of the standard name, title, and URL conventions used by the Forge value you select.) If you do not know the URL, enter NA. For more information about these fields, see Custom Component Properties.
6. Click **Save**.

- If the component information has been properly entered, the component is saved to the Code Insight data library and listed in the **Lookup Component** window. Continue with **Step 3: Associate an Instance of the Custom Component with the Inventory Item**.

- If the component name and title combination already exists in the data library, an error message is displayed. You can either select the already-existing component from the **Lookup Component** window to associate it with the inventory item or edit the custom component details to provide a different name or title.

### Create the Custom Component Based on Its Project or Forge URL

Use the following method to create the custom component based on its known project or forge URL.

**Task**

**To create a custom component based on its URL:**

1. On the **Lookup Component** window, select the **URL** option.

2. In the **URL** field, enter URL for the component. As you enter the URL, it is checked for an acceptable format (such as `http://example.com`), but not for validity.

3. (Optional) Click **Search** to see the list of existing components that use the entered URL. If the component you intend to create already exists in the FlexNet Code Insight data library, you can select an instance of the already-existing component to associate with the inventory item; or you can continue to create a custom component with a different name and title (continue with the next step)

4. Click **Create New Component**.

- If Code Insight recognizes the URL you entered as belonging to one of the forge-URL domains currently supported for custom component creation, the **New Custom Component** window opens, showing component fields—including **Name**, **Title**, **URL**, and **Forge**—automatically populated with values based on domain conventions. (For the list of supported domains, see Supported Forge-URL Domains for Custom-Component Creation.)
5. Update the component fields as necessary, noting that the Name, Title, and URL fields are required. For more information about these fields, see Custom Component Properties.

- If the URL you initially entered (at the top of the window) belongs to a supported domain and you edit that URL, click Get Details to update the remaining field values according to forge-URL domain conventions.

- If you must manually provide field values because the URL you initially entered does not belong to a supported domain, click in the upper part of the window for examples of the standard name, title, and URL conventions used by the Forge value you select.

6. Click Save.

- If the required information has been properly entered, the component is saved to the Code Insight data library and listed in Lookup Component window. Continue with Step 3: Associate an Instance of the Custom Component with the Inventory Item.

- If the component name and title combination already exists in the data library, an error message is displayed. You can either select the already-existing component from the Lookup Component window to associate it with the inventory item or edit the custom component details to provide a different name or title.
Create the Custom Component Based on Its Forge

Use the following method to create the custom component if you know the forge (project repository) of the custom component you are creating.

**Task**

To create a custom component based on its forge:

1. On the **Lookup Component** window, select the **Forge** option.
2. From the **Forge** field, select the forge of the custom component, and enter the information required to identify the forge. (This information varies by forge.)

![Lookup Component](image)

3. (Optional) Click **Search** to see the list of existing components that use the entered forge specifications. If the component you intend to create already exists in the FlexNet Code Insight data library, you can select an instance of the already-existing component to associate with the inventory item; or you can continue to create a custom component with a different name and title (continue with the next step).

4. Click **Create New Component**.

   - If the forge you entered is one of the forge-URL domains currently supported for custom component creation, the **New Custom Component** window opens, showing component fields—including **Name**, **Title**, and **Forge**—automatically populated with values based on domain conventions. (For the list of supported domains, see Supported Forge-URL Domains for Custom-Component Creation.)

   ![New Custom Component](image)

   - If the forge you entered is not one of the supported domains, the **New Custom Component** window opens, showing the **Forge** field automatically populated with the forge type you selected.
Chapter 2  Using FlexNet Code Insight
Creating and Editing Custom Components

5. Update the component fields as necessary, noting that the **Name**, **Title**, and **URL** fields are required. (Click 🔄 in the upper part of the window for examples of the standard name, title, and URL conventions used by the Forge value you selected.) If you do not know the URL, enter NA. For more information about these fields, see Custom Component Properties.

6. Click **Save**.

   - If the component information has been properly entered, the component is saved to the Code Insight data library and listed in **Lookup Component** window. Continue with Step 3: Associate an Instance of the Custom Component with the Inventory Item.
   
   - If the component name and title combination already exists in the data library, an error message is displayed. You can either select the already-existing component from the **Lookup Component** window to associate it with the inventory item or edit the custom component details to provide a different name or title.

Create the Custom Component in Free Form

Use following method to create the custom component when you do not know the component name (keyword), URL, or forge or when you simply want to provide your own values (for example, when creating a custom component for commercial software you want to track in FlexNet Code Insight for inclusion in the Bill of Materials).

**Task** To create a custom component in Free Form mode:

1. On the **Lookup Component** window, click **Create New Component** to open the **New Custom Component** window.

   The window opens in the Free Form form, enabling you to provide your own values for the component fields. (No field values are automatically populated.)
Optionally, you can switch to the **URL** form on the **New Custom Component** window, enabling you to enter a project or forge URL by which to create the component. Once you enter the URL, you must click **Get Details** to continue:

- If the URL belongs to a supported forge-URL domain, component fields are automatically populated with values based on domain conventions, as described in Create the Custom Component Based on Its Project or Forge URL.
- If the URL does not belong to a supported domain (that is, Code Insight is unable to parse the URL), you must click **OK** on the resulting “Unable to parse URL...” message box to proceed to manually complete component fields in **Free Form** mode (continue with the next step 2).

2. Update the component fields, noting that the **Name**, **Title**, and **URL** fields are required. (Click 🔄 in the upper part of the window for examples of the standard name, title, and URL conventions used by the **Forge** value you select.) If you do not know the URL, enter **NA**. For more information about these fields, see Custom Component Properties.

3. Click **Save**.

   - If the component information has been properly entered, the component is saved to the Code Insight data library and listed in **Lookup Component** window. Continue with Step 3: Associate an Instance of the Custom Component with the Inventory Item.
   - If the component name and title combination already exists in the data library, an error message is displayed. You can either select the already-existing component from the **Lookup Component** window to associate it with the inventory item or edit the custom component details to provide a different name or title.

### Step 3: Associate an Instance of the Custom Component with the Inventory Item

A component instance is a unique component-version-license entity that you can associate with an inventory item. The following procedure creates an instance for the new custom component and associates it with the inventory item you are creating or editing.

You can create multiple instances of the custom component to associate with inventory items. Each instance is saved to the FlexNet Code Insight data library and made available for global use.

<table>
<thead>
<tr>
<th>Task</th>
<th>To associate an instance of the new custom component with the inventory item you are creating or editing, follow these steps:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>On the <strong>Lookup Component</strong> window showing the custom component you just created, click <strong>Show Instances</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Register New Instance</strong> to create a component instance.</td>
</tr>
<tr>
<td>3.</td>
<td>Complete the instance registration by selecting <strong>Create Custom Version</strong> to specify a version and then selecting the license to associate with the instance.</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>Use This Instance</strong> next to the new instance to associate it with the inventory item.</td>
</tr>
</tbody>
</table>

You are returned to the inventory item you are creating or updating. The **Name** and **Description** editable fields for the inventory item are automatically populated with information based on the registered instance you selected. Additionally, the **Component** and **License** fields are displayed, showing the component, its version, and the license for the instance.

You can now proceed with completing the inventory creation or update.
Editing a Custom Component

Use the following procedure to edit a custom component. Currently you must edit the component within the context of an inventory item to which it is associated. However, the changes you make are saved in the FlexNet Code Insight data library and the updated component is available for global use.

<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To edit a custom component, do the following:</strong></td>
</tr>
<tr>
<td>1. From the page on which you are creating or editing inventory, select <strong>Component</strong> in the <strong>Type</strong> field for the inventory item.</td>
</tr>
<tr>
<td>2. Click <strong>Lookup Component</strong> to open the <strong>Lookup Component</strong> window.</td>
</tr>
<tr>
<td>3. Search for the custom component by keyword, URL, or forge.</td>
</tr>
<tr>
<td>4. Locate the component in the search results, and update the component in any of these ways:</td>
</tr>
<tr>
<td>• Click <strong>Edit Custom Component</strong> to update the component properties. See <strong>Custom Component Properties</strong> for field descriptions.</td>
</tr>
<tr>
<td>• Click <strong>Show Versions</strong> to create one or more component-version-license instances for the component.</td>
</tr>
<tr>
<td>5. Click <strong>Use This Instance</strong> next to an instance to associate it with the inventory item or click <strong>Cancel</strong> to close the <strong>Lookup Component</strong> window.</td>
</tr>
</tbody>
</table>

You can now proceed with completing the inventory creation or update.
Custom Component Properties

The following describes the fields on the **New Custom Component** window used to define a custom component. Certain fields might be automatically populated based on information entered on the Lookup Component window. However, any field can be edited.

**Table 2-6 • Fields to Define a Custom Component**

<table>
<thead>
<tr>
<th>Component Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Using</td>
<td>(Available during component creation) The “form” mode used to create the custom component. The information you entered on the <strong>Lookup Component</strong> window initially determines the mode used, but you can switch modes here.</td>
</tr>
<tr>
<td></td>
<td>• <strong>URL</strong>—Mode used when creating the component based on the URL for its project or forge (see Create the Custom Component Based on Its Project or Forge URL). This form includes the actual <strong>URL</strong> value, located beneath the <strong>Create Using</strong> section, which is either pre-populated from the <strong>Component Lookup</strong> window or manually entered here. If necessary, click <strong>Get Details</strong> to view component fields to complete or update them. If the URL is recognized as belonging to a supported forge-URL domain supported for custom component creation, required component fields are automatically populated on the <strong>Component Lookup</strong> window. See the <strong>URL</strong> field description next in this table for more information.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Free Form</strong>—Mode used to define or update component fields manually when creating the custom component using any other method (see Create the Custom Component Based on a Keyword in Its Name or Title, Create the Custom Component Based on Its Forge, Create the Custom Component in Free Form). Certain fields might be automatically populated based on the information entered previously on the <strong>Lookup Component</strong> window.</td>
</tr>
<tr>
<td>URL</td>
<td>(Available under <strong>Create Using</strong> during component creation when the <strong>URL</strong> form is selected) The project or forge URL for which you are creating the custom component. If the URL is recognized as belonging to a supported forge-URL domain supported for custom component creation, required component fields are automatically populated according to domain conventions. Any change made to this <strong>URL</strong> is automatically updated to the other field values when you click <strong>Get Details</strong>. If the URL does not belong to a supported domain, you must manually provide all remaining necessary component details. (Click <strong>Get details</strong> to display the fields.) For information about supported forge-URL domains, see Supported Forge-URL Domains for Custom-Component Creation.</td>
</tr>
</tbody>
</table>
**Table 2-6 • Fields to Define a Custom Component (cont.)**

<table>
<thead>
<tr>
<th>Component Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>(Required) The name of the custom component. During component creation, this field might be automatically populated based on information entered on the Lookup Component window. To help you provide this value in an appropriate format, click <img src="image" alt="example" /> in the upper part of the window for examples of the standard name, title, and URL conventions used by different forge-URL domains.</td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td>(Required) The component title. During component creation, this field might be automatically populated based on information entered on the Lookup Component window. To help you provide this value in an appropriate format, click <img src="image" alt="example" /> in the upper part of the window for examples of the standard name, title, and URL conventions used by different forge-URL domains.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>A description of the custom component to provide any additional meaningful information about the component.</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td>(Required) The URL for the project or forge of the custom component. During component creation, this field is pre-populated with the same URL value provided in the URL form (see the Create Using field) when that URL is recognized as belonging to a supported forge-URL domain. Otherwise, to help you provide this value in an appropriate format, click <img src="image" alt="example" /> in the upper part of the window for examples of the standard name, title, and URL conventions used by different forge-URL domains. If you do not know the URL for the component, enter <strong>NA</strong>.</td>
</tr>
</tbody>
</table>
| **Forge**       | The type of project repository used by the custom component. During component creation, this field is automatically populated with an appropriate value when you are creating the component based on either of the following:  
  - Its forge (see Create the Custom Component Based on Its Forge).  
  - The URL for its project or forge and the URL belongs to a forge-URL domain supported by the custom-component creation process. For more information, see Create the Custom Component Based on Its Project or Forge URL and Supported Forge-URL Domains for Custom-Component Creation. Otherwise, the default **Other** is displayed. However, you can select any other forge from the dropdown. |
| **Encryption**  | **Yes** or **No** value depicting whether this component supports encryption. The default is **No**. |
Supported Forge-URL Domains for Custom-Component Creation

When creating a custom component, you can select any forge supported by FlexNet Code Insight and provide free-form component details. However, the forge might require that the URL and other component details be in a certain format. To help the user properly format component properties, the component-creation process supports certain forge-URL domains. When the user initiates the creation process by providing a URL or forge that the creation process recognizes as belonging to a supported domain, it automatically populates component fields with values formatted according to domain conventions.

The following are the forge-URL domains currently supported by the custom-component creation process:

- GitHub
- NuGet Gallery
- npm
- SourceForge
- RubyGems

For other forges that you might use to create custom components, you can click 📘 on the Lookup Component and New Custom Component windows for guidance on how to format the URL and the component name and title according to forge conventions.

Creating and Editing Custom Licenses

FlexNet Code Insight enables you to create custom licenses that represent licenses not found in the Code Insight data library or commercial EULAs that are typically not included in the data library. The opportunity to create or edit a custom license is made available during those processes prompting you to select a license to associate with an inventory item.

The custom licenses are saved to the data library so that they are available for use by other inventory items across the system. They are also available for use by policies.

The following topics describe how to create and edit custom licenses:

- Creating a Custom License
- Editing a Custom License
- Custom License Properties

Creating a Custom License

Use the following steps to create a custom license:

- Step 1: Initiate the Creation of a Custom License
- Step 2: Create the Custom License
Step 1: Initiate the Creation of a Custom License

You have the option to create a custom license during any of the following procedures that involve associating a license with an inventory item:

- When Using Component Lookup to Register a Component Instance for a “component” Inventory Item
- When Selecting a New License for an Existing Inventory Item
- When Creating or Editing a “License Only” Inventory Item

When Using Component Lookup to Register a Component Instance for a “component” Inventory Item

You can create a custom license when you access the Component Lookup feature to register a new component-version-license instance for a “component” inventory item.

Task | To create a custom license when registering a component instance for a “component” inventory item, do the following:
---|---
1. | For an inventory item that you are creating or editing in Analysis Workbench or from the Project Inventory tab, access the Lookup Component window (see Performing Component Lookup).
2. | Locate the component for which you want to register a new component-version-license instance to associate with the inventory item, and click Show Instances (or Versions) to list its registered instances.
3. | Click Register New Instance to set up a new instance with which to associate the custom license you are creating.
4. | After selecting a component version in the new instance entry, click the Select a License dropdown and choose Select Another License. The Select License dialog is displayed.
5. | Next to the License dropdown, click New to display the Create Custom License window.
6. Continue with **Step 2: Create the Custom License**.

Once you save the custom license, it is automatically associated with the newly registered instance, which you can then associate with the inventory item.

### When Selecting a New License for an Existing Inventory Item

You can create a custom license when updating an existing inventory item of the type **Component** in Analysis Workbench or from the Project Inventory tab.

---

**Task**

**To create a custom license with which to associate an existing “Component” inventory item, do the following:**

1. When editing an existing inventory item of the type **Component** in Analysis Workbench or from the Project Inventory tab, click next to the **License** or **Component** field.

![Edit Version/License dialog](image)

The **Edit Version/License** dialog is displayed.

2. Next to the **License** dropdown, click **New** to display the **Create Custom License** window.

![Create Custom License window](image)

3. Continue with **Step 2: Create the Custom License**.

Once the custom license is saved, a new component-version-license instance using the custom license is automatically created and applied “behind the scenes” to the inventory item. You can view this new instance through the Component Lookup feature.
When Creating or Editing a “License Only” Inventory Item

You can create a custom license to associate with an inventory item of the type **License Only** that you are creating or editing from the **Project Inventory** tab or in **Analysis Workbench**.

**Note** • Generally you create a **License Only** inventory item if you know the license for the third-party code or artifact but do not know the component. (You can later edit this inventory item to convert it to one of the other inventory types.) This type of inventory is typically used for groups of files of unknown origin that are governed by a specific license. When you select the license, the inventory name is automatically generated as **Files under <LICENSE NAME> License**.

**Task**

To create a custom license when creating or editing a “License Only” inventory item, do the following:

1. When creating or editing inventory in **Analysis Workbench** or from the **Project Inventory** tab, select **License Only** in the **Type** field for the inventory item.

2. Next to the **License** dropdown, click **New** to display the **Create Custom License** window.

3. Continue with **Step 2: Create the Custom License**.

Once you save the custom license, it is automatically associated with the inventory item.

**Step 2: Create the Custom License**

Once you performed one of the procedures in **Step 1: Initiate the Creation of a Custom License** to open the **Create Custom License** window, use these steps to create the custom license.
Task To create the custom license, follow these steps:

1. From the Create Custom License window, provide the license properties. Name, Short Name, and License Text are required fields. For a description of the properties, see Custom License Properties.

2. Click Save. The custom license is associated with the inventory item as described in the previous sections.

Editing a Custom License

You can edit only custom licenses. When a custom license is selected in any License dropdown, the Edit button is displayed next to the New button, enabling you to update properties for the license. The updates you make to the license at the inventory-item level are saved to the license in the FlexNet Code Insight data library.

Task To edit a custom license, follow these steps:

1. Using any of the procedures described in Step 1: Initiate the Creation of a Custom License, access the License dropdown used to associate a license with the given inventory item.

2. If the custom license you want to update is not already selected for the inventory item, select it from the License dropdown.
3. Click **Edit** next to the **License** dropdown to open the **Edit Custom License** window.

4. Update the license properties as needed, and click **Save**. For a description of the properties, see **Custom License Properties**.

The license is updated for the inventory item and saved to the FlexNet Code Insight data library for global use.

### Custom License Properties

The following describes the fields on the **Create** (or **Edit**) **Custom License** window used to define a custom license.

**Table 2-7 • Fields to Define a Custom License**

<table>
<thead>
<tr>
<th>Component Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>The full name of the license (for example, <strong>The Rose License 1.5</strong>).</td>
</tr>
<tr>
<td><strong>Short Name</strong></td>
<td>A unique shorthand representation of the license. This is usually the license SPDX short identifier (for example, <strong>Rose-1.5</strong>).</td>
</tr>
</tbody>
</table>
Managing Custom Detection Rules

During a FlexNet Code Insight project scan, the Automated Analysis component of the Scan Server uses a set of internal detection rules, stored in the Code Insight data library, to automatically generate inventory items. However, in some cases, your manual analysis might find codebase files that are associated with a third-party component but not associated with inventory. Code Insight enables you to create custom detection rules that convert such findings into future automated inventory items. These rules are saved to the Code Insight data library for global use by Automated Analysis during scans on future projects (or rescans on current projects).

The following sections provide more information about managing custom detection rules:

- Creating a Custom Detection Rule
- Viewing All Current Custom Detection Rules
- Editing a Custom Detection Rule
- Deleting a Custom Detection Rule
- Rule-Processing Considerations
Creating a Custom Detection Rule

The following sections describe the methods used to create a custom detection rule:

- Creating a Custom Detection Rule from Inventory of “Component” Type
- Creating a Custom Detection Rule from Scratch

Creating a Custom Detection Rule from Inventory of “Component” Type

During codebase analysis in the Analysis Workbench for a project, you might find one or more codebase files that are associated with a specific third-party component but are not associated with current inventory. You can manually update the existing inventory item associated with the component to include the files or, if inventory does not exist, create an inventory item based on the component and associate the files. (The inventory item type must be defined as Component.) You then have the option to create a global custom detection rule based on the details of the updated or created inventory item, as described in the following procedure. This method pre-populates much of the information needed to create the rule, including the MD5 value for each file associated with the inventory item.

Task To create a custom detection rule using the context of a manually created inventory item, do the following:

1. In the Analysis Workbench for the given project, navigate to the Inventory Items pane and select the inventory item with which you have manually associated the codebase files. The Inventory Details tab for inventory item is opened.

2. Click the Create Custom Rule button to open the Custom Detection Rule dialog. For a description of the fields on this dialog, refer to Custom Detection Rule Dialog.

Note that the Component, License, Description, and URL values are pre-populated from the inventory item on which you are basing the rule and are not editable.
3. Add or edit **As-Found License Text**, **Notices Text**, and **Audit Notes** content as needed for the rule. (These fields are pre-populated with any content currently defined in the inventory item on which you are basing the rule.) This information is displayed for inventory items automatically created or updated by the rule in the future.

4. Scroll down to the **File MD5** pane, which is pre-populated with the list of codebase files associated with the inventory item you created. The MD5 value for each file is provided.

5. Select one or more files to add to the rule.

6. Click **Save** to create the rule and add it to the Code Insight data library. You will be asked for confirmation to proceed the creation.
Creating a Custom Detection Rule from Scratch

You can create a custom detection rule from scratch—that is, without being in the context of an inventory item that you have manually updated or created to add codebase files, as described in Creating a Custom Detection Rule from Inventory of “Component” Type. The method enables you to create custom detection rules if you do not have access to the Analysis Workbench for a specific project. However, you will need to provide information manually, including the name and MD5 value for each codebase file that you want to associate with the rule.

To create a custom detection rule from scratch, do the following:

1. Open the Custom Detection Rules tab, using the procedure in Viewing All Current Custom Detection Rules.

2. Click Create Custom Rule to open the Custom Detection Rule dialog. For a description of the fields on this dialog, refer to Custom Detection Rule Dialog. Note the following:
   - Once you use Lookup Component to select or create a component for the rule, the component information is populated on the dialog. However, you can edit this information as needed.
   - You can add As-Found License Text, Notices Text, and Audit Notes content as needed for the rule. This information is displayed in the future inventory items created automatically by the rule.

3. Scroll down to the File MD5 pane.

4. For each codebase file you want to add to the rule, click the Add File button and provide the file’s name and MD5 value.

5. Click Save to create the rule and add it to the Code Insight data library. You will be asked for confirmation to proceed with the creation.

Viewing All Current Custom Detection Rules

Use the following the procedure to access the Custom Detection Rules tab, from which you can view all currently defined custom detection rules and act on them as needed.

Task To view all current custom detection rules created for your FlexNet Code Insight system, do the following:

1. Click the Open Menu icon in the upper right of any FlexNet Code Insight page:

2. Select Custom Data from the menu to open the Custom Detection Rules tab, showing the list of current custom detection rules. From this tab, you can do the following:
   - View the component information (name, version, license, and forge URL) on which each rule is based.
• Create a custom detection from scratch (see Creating a Custom Detection Rule).
• Edit a custom detection rule or remove it from the Code Insight system.

Editing a Custom Detection Rule

Use the following procedure to edit a specific custom detection rule. The changed rule is applied to all future scans or rescans on projects in the FlexNet Code Insight.

Task

To edit an existing custom detection rule, do the following:

1. Open the Custom Detection Rules tab, following the procedure in Viewing All Current Custom Detection Rules.
2. In the Actions column for the entry you want to update, click the Edit (Edit) icon. The Edit Custom Rule dialog opens.
3. Edit fields as needed. See Edit Custom Rule Dialog for a description of each field.
4. Manage the codebase files for the rules:
   • To add a file, click the Add File button and provide the file’s name and MD5 value.
   • To remove a file from the rule, click the Delete File (Delete File) icon.
5. Click Save to update the detection rule changes to the Code Insight data library. You will be asked for confirmation to proceed with the updates.

Deleting a Custom Detection Rule

Use the following procedure to remove a specific custom detection rule from the FlexNet Code Insight data library. The rule will no longer be applied to any future scan in your Code Insight system.

Task

To remove a custom detection rule from the Code Insight data library, do the following:

1. Open the Custom Detection Rules tab, following the procedure in Viewing All Current Custom Detection Rules.
2. In the Actions column for the entry you want to remove, click the Delete (Delete) icon. You are asked to confirm the deletion.

Rule-Processing Considerations

As you manage custom detection rules, consider how the rules are processed under certain circumstances:

• If the custom detection rule is associated with more than one file, the scan uses OR logic when processing the files against the target codebase. Consequently, only one file match between codebase and the rule is required to automatically create an inventory item.
• If two rules are created with identical details and codebase files, a single inventory item is generated during a scan when both rules are applied.
• If two rules are created using the same component, version, and license details and the same codebase files, but have different Description, URL, Audit Notes, As-Found License Text, or Notices Text content, a single inventory item is generated during a scan when both rules are applied. In the inventory item, values that differ between the rules for a given field are separated (shown on separate lines or with a separator) within the field.

• If two rules with are created with the same codebase files but use a different component, two inventory items are generated during the scan.

Finalizing the Notices Text for the Notices Report

If you want to create or modify license text for a given inventory item, you can use the Notices Text field to provide the exact content to include in the Notices report. For example, you can edit any license text previously saved to this field or add your own license text, such as license information for rules that you developed during your manual research on the inventory item. You can also copy the As-Found License Text content to the Notices Text field and modify it as needed. (Content in the As-Found License Text pane is not editable but can be copied to the Notices Text field and modified.)

If the Notices Text field item field contains information when the Notices report is run, the content of this field alone is pulled into the report. If the Notices Text field is empty, the content of the As-Found License Text field is used in the report. If both fields are empty, the report uses the license content from FlexNet Code Insight data library (see License Details from the Code Insight Data Library).

For more information about these fields, see Reporting of Detected License Text through the As-Found Text Inventory Field and Notices Text.

Note • If the As-Found License Text field contains content populated by the Scan Server, best practice is to leave the Notices Text field empty (as long as custom information or edits are not required) so that the report is forced to use the license information found in the As-Found License Text field.

Task

To provide custom content for the Notices report, do the following:

1. Navigate to one of these locations:

   In Analysis Workbench, on the Inventory Details tab for a specific inventory item, open the Notices Text tab.
From **Project Inventory**, select an inventory item and open the **Notices Text** tab.
2. Do one or both of the following:

- In the **Notices Text** field, enter new or modify existing license content for the inventory item. The text and its format should look exactly as you want it to appear in the Notices report.

- Using the following steps, copy the **As-Found License Text** content to the **Notices Text** field and modify the content as needed:
  
  a. Click the Copy to Notices Text button in the top right corner of the **As-Found License Text** field.

     If the **Notices Text** field is empty, the **As-Found License Text** content is copied to the **Notices Text** field, with the formatting preserved.

     ![As-Found License Text copy](image)

     If the **Notices Text** field is not empty, you are given the option to append the **As-Found License Text** content to the existing **Notices Text** content or to replace all the existing **Notices Text** content with the **As-Found License Text** content.

     ![Notices Text copy options](image)

     If you select **Append**, the appended content is added to the **Notices Text** field, starting on a new line after the existing content. If you select **Replace**, the existing **Notices Text** content is replaced.

  b. Modify and format the **Notices Text** content as needed.

3. Save the **Notices Text** changes to the current inventory item:

- If you are in **Analysis Workbench**, click the **Save** button at the top of the **Inventory Details** tab. (Alternatively, click **Close** to shut down the tab for the current inventory item. You are prompted to save the inventory changes before the tab closes.)
• If you are in **Project Inventory**, click the **Save** button at the top of the **Notices Text** field.

When the Notices report is run, the content from the **Notices Text** pane is used as the “notices” information for the inventory item in the report.

### Accessing and Viewing Projects in the System

This section describes the various ways you can access projects in your FlexNet Code Insight system in order to view their details and manage them:

- Navigating to the Projects List
- Using the Project Dashboard
- Opening a Project
- Showing Only Your Projects
- Searching the System
- Managing Items in the Project List

### Navigating to the Projects List

You access projects in the FlexNet Code Insight system from the **Projects** list, a manageable display of the projects available in the system. (The projects can be grouped in folders for easier accessibility.)

Use the following procedure to open the **Projects** list. The procedure assumes that you have logged into FlexNet Code Insight.

<table>
<thead>
<tr>
<th>Task</th>
<th>To open the Projects list, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>From the <strong>FlexNet Code Insight Dashboard</strong>, select <strong>go to project</strong>.</td>
</tr>
</tbody>
</table>
Alternatively, click the **Open Menu** icon in the upper right of any FlexNet Code Insight page:

![Open Menu Icon]

The **Projects** list is displayed.

![Projects List]

2. (Optional) Click the **My Projects** toggle at the top of the list to show only those projects with which you are associated as Project Owner or through a project role. (For details, see **Showing Only Your Projects**.) You can also search projects by name, inventory, or security vulnerability as described in **Searching the System**.

## Using the Project Dashboard

When you select a project from the Projects list, the **Project Dashboard** is displayed, providing you with an interactive view of your project, including security-vulnerability and license exposure, codebase and inventory review statistics, and other information.

The procedure that follows this image describes how to use **Project Dashboard** features.
### Task

To use the Project Dashboard, do the following:

1. Navigate to the **Projects** list. See [Navigating to the Projects List](#) for instructions.

2. Select a project from the **Projects** list. The **Project Dashboard** for the selected project is displayed in the right panel.

   (Alternatively, hover over the project entry, and click its **Load Project Dashboard** icon in the project entry to display the dashboard.)

The **Project Dashboard** contains the following charts to provide an overview of the project’s most recent scan and the resulting inventory:

- **Scan Summary** — A summary of your most recent scan, including number of files scanned, the size of the codebase/files, and the number lines of code.

- **Audit Progress** — A snapshot of the audit progress of the selected project.

- **Security Vulnerability Exposure** — An interactive color-coded chart and legend that provide an overview of the security vulnerabilities by severity across all the project inventory. The number in the center of the chart is the total number of security vulnerabilities found across all inventory items. (The colors in this chart can vary depending on the CVSS version Code Insight is using. See [Security Vulnerabilities Associated with Inventory](#) for details.)

- **License Exposure** — An interactive color-coded chart and legend that provide an overview of the licenses identified by priority across all of the project inventory. The number in the center of the chart is the total number of inventory items identified for the current project.

- **Inventory Priority** — An interactive color-coded chart and legend that provide an overview of the priority of inventory in the selected project. For more information about inventory priority, see [Inventory Priority](#).
• **Inventory Review Status**—An interactive color-coded chart and legend that show you the review status (Approved, Rejected, Not Reviewed) of the inventory for the selected project.

3. (Optional) Hover your mouse cursor over the color-coded segments in the charts to view details related to a given segment. If you want, click a color-coded segment to open the project to view the inventory items associated with the segment. See Filtering Inventory for a Project from the Project Dashboard for details.

Alternatively, you can open the project to view all its inventory (see Opening a Project), or select another project from the Projects list to view its dashboard.

### Filtering Inventory for a Project from the Project Dashboard

After you create a project, and upload and scan a codebase, you can quickly filter the project’s inventory to view potential problems and take steps to eliminate issues, such as high exposure items (shown in red), from your project inventory.

<table>
<thead>
<tr>
<th>Task</th>
<th>To quickly filter inventory on the Project Dashboard, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open the Project Dashboard for a project. See Using the Project Dashboard.</td>
</tr>
<tr>
<td>2.</td>
<td>Navigate to a chart and click a color-coded area. The project is opened to its Project Inventory tab, displaying the project inventory items associated with the information represented by color-code area. You can also click the corresponding colors in the legends below the charts to filter your inventory.</td>
</tr>
<tr>
<td>3.</td>
<td>Click on a project inventory item listed to see more detail in the right pane of the Project Inventory tab. See Reviewing Published Inventory for details about this tab.</td>
</tr>
</tbody>
</table>

### Opening a Project

Use this basic procedure to open a project.

<table>
<thead>
<tr>
<th>Task</th>
<th>To open a project, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to the Projects list. See Navigating to the Projects List for instructions.</td>
</tr>
<tr>
<td>2.</td>
<td>Select a project in the Projects list. Its Project Dashboard is displayed on the right.</td>
</tr>
<tr>
<td>3.</td>
<td>To open the project, either click the Open Project icon (É) next to the project entry in the Projects list, or click the project’s name link in the upper left corner of the dashboard (shown below):</td>
</tr>
</tbody>
</table>

The project is opened on either of the following tabs for the project:

- If the project contains published inventory items, the Project Inventory tab. For more information about the Project Inventory tab, see Reviewing Published Inventory.
• If the project does not contain published inventory items, the project’s Summary tab. For more information about the Summary tab, see Managing a Project from the Summary Tab. For information about publishing inventory, see Publishing or Recalling Inventory from Analysis Workbench.

Note that the Analysis Workbench tab is also available for users with the proper permissions (although you have to navigate to open it). The Analysis Workbench enables a user to perform a deep analysis of the scan results. For more information, see The Analysis Workbench Layout.

Showing Only Your Projects

FlexNet Code Insight provides the option to filter the Projects list to show only those projects with which the current user is associated as either Project Owner, Analyst, Reviewer, or Observer. (For a description of these roles, see Assigning Project Roles to Users.)

Additionally, this filter can work in conjunction with the system filters described in Searching the System to display only your projects that have specific project or inventory attributes.

Task  
To show your projects only, do the following:

1. Navigate to the Projects list. See Navigating to the Projects List for instructions.

2. At the top of the list, click the My Projects toggle.

3. Select a project from the filtered list to open its dashboard. See Using the Project Dashboard for details.

Alternatively, open the project to view its inventory on the Project Inventory tab. See Opening a Project for details.

4. (Optional) To turn off this filter, click the My Projects toggle again.

Searching the System

FlexNet Code Insight enables you to search both globally across all projects, as well as locally for a given project. At the global level, you can use the filters available in the Projects list quickly search for projects and inventory of interest in the system, as described in this section.

At the project-level on the Project Inventory tab, you can further narrow your search results to specific inventory items.
To search globally, use the filters available in the Projects list. Specify criteria to quickly search for and find projects and inventory of interest in the system. Using the search filters available for the Projects list, you can search projects by name, inventory, components and versions, licenses, and security vulnerabilities. You can perform multiple search types, each one further filtering the current search results. Then, at the project level on the Project Inventory tab, you can continue to narrow your search results to specific inventory items.

The following topics describe these search methods:

- Available Filters for Searching Across Projects
- Searching for Projects by Name
- Searching All Projects for Inventory Based on a Specific Component and Version
- Searching All Projects for Inventory Associated with a Specific License
- Searching All Projects for a Security Vulnerability Advisory
- Restoring the Full Project List

### Available Filters for Searching Across Projects

The following filters are available from the Projects list to perform searches across all projects in your FlexNet Code Insight system.

<table>
<thead>
<tr>
<th>To search across all projects for...</th>
<th>...use this filter</th>
<th>Filter criterion</th>
<th>Criterion example</th>
<th>Refer to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Projects with a name containing a specific string</td>
<td>Project Name</td>
<td>Project name</td>
<td>MyProject</td>
<td>Searching for Projects by Name</td>
</tr>
<tr>
<td>Inventory based on a specific component and version</td>
<td>Project Inventory</td>
<td>Component and version as it appears in the Inventory Name value</td>
<td>Apache Struts 2.3.14.3</td>
<td>Searching All Projects for Inventory Based on a Specific Component and Version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Component name as it appears on the Component Details tab for the inventory item</td>
<td>struts2-core</td>
<td></td>
</tr>
<tr>
<td>Inventory associated with a specific license</td>
<td>Project Inventory</td>
<td>The Selected License value as it appears on the Component Details tab for the inventory item</td>
<td>GNU General Public License v2.0</td>
<td>Searching All Projects for Inventory Associated with a Specific License</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The license name as it appears in the Inventory Name value</td>
<td>GNU General Public License or GPL-2.0+</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The SPDX short identifier for the license</td>
<td>GPL-2.0+</td>
<td></td>
</tr>
</tbody>
</table>
Searching for Projects by Name

You can use the **Project Name** search filter available for the **Projects** list to search for a project by its full or partial name.

### Search Rules

When you search for projects by project name, the following rules apply:

- The name string value you enter is case-insensitive.
- All characters in the search string must be consecutive.
- A full or partial string value is supported as search criterion.
- The string can contain any characters (letters, numbers, and special characters).

### Searching for Projects by Name

This procedure shows how to search for projects by a full or partial name string.

#### Task

To search projects by name, do the following:

1. Navigate to the **Projects** list. See *Navigating to the Projects List* for instructions.
2. At the top of the list, select **Project Name** from search dropdown on the left.
3. Enter the project name (or a partial string in the name) in the **Enter Project Name** field. The list of projects changes to reflect the search results, and a filtered count (for example, “(19 of 123”) is provided in the **Projects** list header to show the number of projects returned by the search.

   If no inventory items meet the specified criterion, the **Projects** list shows “No Projects”.

4. Select a project from the filtered list to open its dashboard. See *Using the Project Dashboard* for details.

   Alternatively, open the project to view its inventory on the **Project Inventory** tab. See *Opening a Project* for details.
Searching All Projects for Inventory Based on a Specific Component and Version

You can use the Project Inventory filter to search for those projects whose inventory contains items based on a specific component and version. The search returns a filtered list of projects; and, when a project in the list is opened, its inventory is also filtered by the search criterion.

This search method saves you time in locating specific inventory items that require attention across all projects. For example, you might also use this search method to pinpoint those projects containing inventory items affected by a recent component upgrade.

You can also use this search method to easily locate projects that contain inventory items impacted by a security vulnerability whose exact ID you do not know; you can search instead for projects with inventory based on a component and version known to be affected by the vulnerability. (This search method is an alternative to using the Security Vulnerability filter, which requires the exact vulnerability ID as the search criterion. See Searching All Projects for a Security Vulnerability Advisory.)

Search Rules

When you search projects for inventory based on a specific component and version, the following rules apply.

- A full or partial string value is supported as search criterion.
- All characters in the search string must be consecutive.
- The string value is case-insensitive and can contain letters, numbers, hyphens, and special characters. Spaces are also allowed.
- Only inventory items on the Project Inventory tab are supported in the search.

Searching All Projects by Component and Version

Use this procedure to locate projects with inventory based on a specific component and version.

Task

To search all projects for inventory based on a specific component and version, do the following:

1. Navigate to the Projects list. See Navigating to the Projects List for instructions.
2. At the top of the list, select Project Inventory from search dropdown on the left.
3. In the Enter Search Criteria field, specify the complete name or a partial string for one of the following:
   - The name of the component as it appears on the Component Details tab (for example, struts2-core) for an inventory item
   - The name of the component and version as it appears in the Inventory Name value (for example, Apache Struts 2.3.14.3)

The list of projects changes to reflect the search results, and a filtered count (for example, “(19 of 123)”) is also provided in the Projects list header to show the number of projects returned by the search.
4. Open one of the projects to see a filtered list of inventory items that contain the component or component and version. (See Opening a Project for details.)
Searching All Projects for Inventory Associated with a Specific License

You can use the Project Inventory filter to search for those projects containing inventory items associated with a specific license. The search returns a filtered list of projects; and, when a project in the list is opened, its inventory is also filtered by the search criterion.

This search method saves you time in locating inventory items with license-related issues, such as those items that are associated with a high-risk license, across all projects.

Search Rules

When you search projects for inventory associated with a specific license, the following rules apply:

- A full or partial string value is supported as search criterion.
- All characters in the search string must be consecutive.
- The string value is case-insensitive and can contain letters, numbers, hyphens, and special characters. Spaces are also allowed.
- Only inventory items on the Project Inventory tab are supported in the search.

Searching All Projects by License

Use this procedure to locate projects with inventory associated with a specific license.

<table>
<thead>
<tr>
<th>Task</th>
<th>To search all projects for inventory associated with specific license, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to the Projects list. See Navigating to the Projects List for instructions.</td>
</tr>
<tr>
<td>2.</td>
<td>At the top of the list, select Project Inventory from search dropdown on the left.</td>
</tr>
<tr>
<td>3.</td>
<td>In the Enter Search Criteria field, specify the complete name or a partial string for one of the following:</td>
</tr>
<tr>
<td></td>
<td>• The name of the Selected License as it appears on the Component Details tab (for example, GNU General Public License v2.0) for an inventory item</td>
</tr>
<tr>
<td></td>
<td>• The license SPDX short identifier (for example, GPL-2.0+)</td>
</tr>
<tr>
<td></td>
<td>• The license name as it appears in the Inventory Name value (for example, GNU General Public License or GPL-2.0+)</td>
</tr>
<tr>
<td></td>
<td>The list of projects changes to reflect the search results, and a filtered count (for example, “(19 of 123)”) is also provided in the Projects list header to show the number of projects returned by the search.</td>
</tr>
<tr>
<td>4.</td>
<td>Open one of the projects to see a filtered list of inventory items that contain the license. (See Opening a Project for details.)</td>
</tr>
</tbody>
</table>

Searching All Projects for a Security Vulnerability Advisory

You might find it sometimes necessary to quickly see how a specific security vulnerability impacts your organization. You can search the system for a security vulnerability or advisory in one of the following ways:

- If you know the exact ID of the security vulnerability or advisory—Use the Security Vulnerability search filter with the exact security vulnerability ID as the search criterion, as described in this section.
• **If you do not know the ID of the security vulnerability or advisory**—Use the **Project Inventory** search filter to provide the name of the vulnerable component as the search criterion. See **Searching All Projects for Inventory Based on a Specific Component and Version** for details.

**Note** • A vulnerability or advisory might not have an ID, for example, in the case of a zero-day vulnerability for which an ID has not been published.

**Search Rules**

When you use the **Security Vulnerability** search filter to search projects associated with a specific security vulnerability, the following rules apply:

• Only one vulnerability ID can be specified as a search criterion.
• Only exact matches of the full vulnerability ID string are supported. Partial strings are not supported.
• The string you enter does not support spaces.
• Only published inventory items are searched.
• The search does not validate the vulnerability ID you enter. If you enter an invalid ID, no results are returned in the **Projects** list.

**Searching for a Security Vulnerability**

Use this procedure to locate projects by the exact security vulnerability ID you specify.

**Task**

To search for projects affected by a specific security vulnerability, do the following:

1. Navigate to the **Projects** list. See **Navigating to the Projects List** for instructions.
2. At the top of the list, select **Security Vulnerability** from search dropdown on the left.
3. In the **Enter Vulnerability ID** field, specify the complete ID of the vulnerability (for example, **CVE-2018-11776** for an NVD vulnerability).
4. Press Enter. The list of projects changes to reflect the search results, and a filtered count (for example, “(19 of 123)”) is also provided in the **Projects** list header to show the number of projects returned by the search.
   
   If no inventory items meet the specified criterion, the **Projects** list shows “No Projects”.
5. Open one of the projects to see a filtered list of inventory items that are impacted by the security vulnerability. (See **Opening a Project** for details.)

**Restoring the Full Project List**

Use this step to remove the filter from the **Projects** list and restore the full list.

**Task**

To restore the full list of projects, do the following:

1. Navigate to the **Projects** list. See **Navigating to the Projects List** for instructions.
Chapter 2 Using FlexNet Code Insight

Managing a Project from the Summary Tab

2. At the top of the list, Click the \( \times \) icon in the criterion field to remove the current Projects list filter:

![Projects (19 of 123)](image)

The full list of projects is restored.

Managing Items in the Project List

As Project Owner, you can rename any of your projects in the Projects list or move your projects to different project folders in the list. Additionally, if you have Create Project permissions, you can create new folders in the Projects list.

Task

To rename or move your projects in the Projects list, do the following:

1. Navigate to the Projects list. See Navigating to the Projects List for instructions.
2. Do one or both of the following:
   - To rename one of your projects, double-click the project name, and overwrite the current name with the name.
   - To move one of your projects to a different folder, drag and drop the project to the desired folder.
   - To create a new folder, click the Add New button and select Folder.

Managing a Project from the Summary Tab

The following topics describe how to use features on the Summary tab to manage the currently opened project.

Refer to the FlexNet Code Insight User Roles and Permissions appendix for the various user roles required manage projects.

- Opening the Project Summary Tab
- Generating Reports
- Assigning Project Roles to Users
- Editing the Project Definition and General Settings
- Automatically Publishing Inventory
- Updating Scan Settings for a Project
- Updating Inventory Review and Remediation Settings for a Project
- Connecting the Project to Remote Data Sources
- Changing Project Owners
- Rescanning Your Codebase
- Exporting Project Data
- Importing Project Data
Opening the Project Summary Tab

When you open a project from the Project List page, the Summary tab shows you information about the project. On this page, you can view project details, scan settings, scan status, and report information. You can also change Project Owners, manage project settings, start and stop scans, generate reports, and upload project codebases.

Task

To open the Summary tab, do the following:

1. From the list of projects, click the project you want to open. The name of the project appears at the top of the right panel.

2. Do one of the following to open the project:
   - Click the project name (in the example, New Project) in the title bar of the right panel.
   - Click the Open Project icon ( ).

   The project is opened to its Project Inventory page.

3. Click the Summary button at the top of the window to open the Summary tab for the project.

Generating Reports

On the Summary tab, you can generate the following standard reports that are included with the FlexNet Code Insight product.

- The Project Report
- The Audit Report
- The Notices Report

You can also create custom reports that focus on information relevant to your site. See Custom Reports.

The Project Report

The Project report summarizes the inventory, vulnerabilities, remaining scan evidence, and review and remediation tasks for a selected project. It produces output in JSON and Excel format. This report is useful in understanding the existing project’s legal and security risks based on identified inventory items, as well as the additional potential risk based on the file-based scan results known as third-party indicators.

Task

To generate the Project report, do the following:

1. Navigate to the Summary tab for the project (see Opening the Project Summary Tab).

3. Click **Generate Report**. A prompt appears explaining that the report will be generated in the background while you continue to work in FlexNet Code Insight.

4. Click **OK**. When the report has been generated, the **View | Download** links appear next to the **Select Report** field.

5. Select either option:
   - To view the report in your browser, click **View**.
   - To download the report, click **Download**. A .zip file is downloaded, containing the report in these formats:
     - **JSON**—The report data can be processed programmatically to integrate with other applications.
     - **XLSX**—The report can be viewed in Microsoft Excel.

6. Navigate to the folder where you saved the report .zip file, unzip the file, and open the report in the desired format.

### The Audit Report

Audit reports provide another way to distribute your research and findings to others in your organization. Only published inventory items appear in Audit reports.

<table>
<thead>
<tr>
<th>Task</th>
<th>To generate an Audit report, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Navigate to the <strong>Summary</strong> tab for the project (see <strong>Opening the Project Summary Tab</strong>).</td>
</tr>
<tr>
<td></td>
<td>2. Select <strong>Audit Report</strong> from the <strong>Select Report</strong> dropdown in the <strong>Reports</strong> section.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Generate Report</strong>. A prompt appears explaining that the report will be generated in the background while you continue to work in FlexNet Code Insight.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong>. When the report has been generated, the **View</td>
</tr>
<tr>
<td></td>
<td>5. Select either option:</td>
</tr>
<tr>
<td></td>
<td>• To view the report in your browser, click <strong>View</strong>.</td>
</tr>
<tr>
<td></td>
<td>• To download the report, click <strong>Download</strong>. A .zip file is downloaded, containing the report in these formats:</td>
</tr>
<tr>
<td></td>
<td>• <strong>HTML</strong>—The report can be viewed in any browser.</td>
</tr>
<tr>
<td></td>
<td>• <strong>JSON</strong>—The report data can be processed programmatically to integrate with other applications.</td>
</tr>
<tr>
<td></td>
<td>• <strong>XLSX</strong>—The report can be viewed in Microsoft Excel.</td>
</tr>
<tr>
<td></td>
<td>6. Navigate to the folder where you saved the report .zip file, unzip the file, and open the report in the desired format.</td>
</tr>
</tbody>
</table>

### The Notices Report

FlexNet Code Insight provides the ability to produce a Notices report to satisfy the attribution requirements of most open source licenses. The report is created in text format.

After Engineering has completed the remediation plan, resolving all rejected inventory items, the codebase is rescanned until it is approved for release. When the codebase is approved for release, you need to generate a Notices report to accompany the software application. This report is a compilation of all the open source/third-party components contained in the product and their license content (notices).
Chapter 2  Using FlexNet Code Insight
Managing a Project from the Summary Tab

The Notices report shows only published inventory. The inventory can be system-generated or custom and of any type—Work in Progress, Component, or License.

The following items can appear in the Notices report for each inventory item:

- **Inventory name**—The entry in this field is based on naming conventions, which is usually the component name, version, and governing license name.

- **Inventory URL**—If the inventory URL is not available, FlexNet Code Insight uses the associated component URL. If both are unavailable, no URL will appear in the report.

- **Inventory Notices Text**—The final “notices” text associated with the inventory item. It is pulled from the Notices Text field on the Notices Text tab for a selected inventory item in Analysis Workbench or in Project Inventory. If this field is empty, FlexNet Code Insight uses the content in the As-Found License Text field (also on the Notices Text tab), which shows the verbatim text license text found in the codebase by the system. If no As-Found License Text or Notices Text information is available, the text pulled from the FlexNet Code Insight data library for the selected license is used in the Notices report. For more information, see Finalizing the Notices Text for the Notices Report.

**Generating the Notices Report**

<table>
<thead>
<tr>
<th>Task</th>
<th>To generate a Notices Report, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to the Summary tab for the project (see Opening the Project Summary Tab).</td>
</tr>
<tr>
<td>3.</td>
<td>Click Generate Report. A prompt appears explaining that the report will be generated in the background while you continue to work in FlexNet Code Insight.</td>
</tr>
<tr>
<td>4.</td>
<td>Click OK. When the report has been generated. When the report has been generated, the View</td>
</tr>
<tr>
<td>5.</td>
<td>Select either option:</td>
</tr>
<tr>
<td></td>
<td>- To view the report in your browser, click View.</td>
</tr>
<tr>
<td></td>
<td>- To download the report, click Download. A .zip file is downloaded, containing the report data as a .txt file. (The text format enables you to reformat the report data as you want.)</td>
</tr>
<tr>
<td>6.</td>
<td>Navigate to the folder where you saved the report .zip file, unzip the file, and open the report.</td>
</tr>
</tbody>
</table>

**Custom Reports**

FlexNet Code Insight provides a Custom Reports Framework that enables you to set up and generate reports that show only the information relevant to your site’s needs. You can generate these reports in any format. Once a custom report is defined and registered, you can select it from the same Select Report dropdown on which the other reports are listed. For complete details, navigate to the following link:

Assigning Project Roles to Users

The Project Owner assigns roles to users, enabling them to analyze the codebase and manage and publish inventory, review published inventory, or view private projects. The following are the available roles that users can have in a project:

- **Analysts** have the ability to manage the codebase and inventory using the Analysis Workbench. They can create new inventory, edit existing inventory, and publish inventory. They can also review files and add files to inventory.

- **Reviewers** have the ability to approve and reject inventory and manage inventory using the **Project Inventory** tab. They can create new inventory and edit existing inventory.

- **Observers** have the ability to view inventory in a private project. They have read-only access to project inventory and can run reports. Development managers and executives are usually assigned this role.

  **Note** • The Observer role is available for private projects only.

For public-view projects, users who are not directly assigned the Reviewer or Analyst role have read-only access to the project inventory. However, private projects are hidden from all users except the Project Owner and those users assigned as Analysts, Reviewers, and Observers of the project. For additional information about private projects, see **Creating a Private Project**.

For a reference to the various user roles and their permissions, refer to the **FlexNet Code Insight User Roles and Permissions** appendix.

The following procedure can be used to assign users and roles to public-view and private projects.

**Task**

To assign an analyst, a reviewer, or an observer to a project, do the following:

1. As the Project Owner, navigate to the **Summary** tab (see Opening the Project Summary Tab).

2. Click the **Manage Project** menu at the bottom of the page and select **Edit Project Users**. The **Edit project users** page appears.

3. To assign users to a given role, drag and drop one or more user names from the **Select Users** list to the desired “role” pane (**Analysts**, **Reviewers**, or **Observers**).

   **Note** • The **Observers** pane is visible for only private projects.

4. Repeat this step as necessary to assign users to roles. (A user can be assigned to multiple roles.)

5. To remove a user from a role, simply click **X** next to the user’s name in the appropriate “role” pane.

6. Click **Close** when you have finished managing the reviewer, analyst, and observer role assignments.
Editing the Project Definition and General Settings

The Project Owner can edit the project’s definition and general settings.

Task

To update project settings, do the following:

1. As the Project Owner, navigate to the Summary tab (see Opening the Project Summary Tab).
2. Click Manage Project and select Edit Project from the popup menu. The Edit Project page opens.
3. Select the General tab.
4. Update the fields as needed. Refer Edit Project: General Tab to for field descriptions.
5. Click Save to save the changes.

Updating Scan Settings for a Project

You can update the scan configuration by switching the project to a different scan profile, update which sub-folders to scan, and change settings for automatically publishing inventory during the scan (see Automatically Publishing Inventory).

See also the Edit Project: General Tab to configure the project setting that determines whether the scan retains inventory that has no files associations.

Task

To update scan settings for the project, do the following:

1. As the Project Owner, navigate to the Summary tab (see Opening the Project Summary Tab).
2. Click Manage Project and select Edit Project from the popup menu. The Edit Project page opens.
3. Select the Scan Settings tab.
4. Update the fields as needed. Refer Edit Project: Scan Settings Tab for field descriptions.
5. Click Save to save the changes.

Automatically Publishing Inventory

FlexNet Code Insight provides the ability to automatically publish inventory without the need for an analyst to be involved. This feature supports a fully automated end-to-end process where there is no human analyst involvement. (For example, the auto-publish feature works in conjunction with workflow policies that automatically review inventory items as they are published, as described in Managing Policy Profiles.) If there is a human analyst involved, the auto-publish feature can be turned off, allowing the analyst to publish the inventory manually after analysis.

When the auto-publish feature is enabled, additional options are made available to do the following:

- Set the minimum inventory confidence level for publishing inventory.
- Determine whether to automatically mark files associated with an auto-published inventory as “reviewed”.
- Determine whether to publish inventories with undetermined licenses (that is, their selected License value is I don’t know).
Task  To set the auto-publish feature, do the following:

1. As the Project Owner, navigate to the Summary tab (see Opening the Project Summary Tab).
2. Click Manage Project and select Edit Project from the popup menu. The Edit Project page opens.
3. Select the Scan Settings tab.
4. Enable or disable Automatically publish system-created inventory items. When you enable this option, additional auto-publish options are made available for configuration. See Edit Project: Scan Settings Tab for a description these options.
5. When you have set the auto-publish feature, click Save. The Summary tab is opened.

Updating Inventory Review and Remediation Settings for a Project

You can overwrite default settings that configure the automation of the review, remediation, and status notification processes for published inventory in your project. These settings, which work in conjunction with the set of policies in the project’s policy profile, are used to set up the following in your project:

- The policy profile to associate with the project. The policies in the selected profile work in conjunction with the review, remediation, and notification configuration defined on this tab.
- Automatic creation of manual review tasks for inventory items not reviewed by policy during publication performed as part of a scan. The tasks are automatically assigned to the default legal or security contact that you specify.
- Automatic creation of remediation tasks and associated external work items for inventory that is rejected either automatically by policy or during manual publication by an analyst. The tasks are automatically assigned to the default engineering contact that you specify.
- Automatic rejection of published inventory impacted by new vulnerabilities detected in the latest scan or Electronic Update.
- The automatic generation of email notifications only (instead of assigned tasks), which are sent to the Project Owner as alerts concerning the rejected or non-reviewed published inventory items.

Task  To update settings that automate review, remediation, and status notification processes for published inventory, do the following:

1. As the Project Owner, navigate to the Summary tab (see Opening the Project Summary Tab).
2. Click Manage Project and select Edit Project from the popup menu. The Edit Project page opens.
3. Select the Review and Remediation Settings tab.
4. Update the fields as needed. Refer Edit Project: Review and Remediation Settings Tab to for field descriptions.
5. Click Save to save the changes.
Connecting the Project to Remote Data Sources

If your system is configured to connect to a remote data source, you will have access to update the following:

- Version Control Settings
- ALM Settings

Version Control Settings

Use the Version Control Settings tab on the Edit Project page to connect to one or more Source Code Management (SCM) repositories directly from FlexNet Code Insight so you can scan and audit code without manually moving that data to the Scan Server. For information about connecting to a remote data sources, see the Configuring Source Code Management chapter.

ALM Settings

FlexNet Code Insight integrates with application lifecycle management (ALM) systems, enabling Code Insight users to create and manage external work items associated with inventory directly from Code Insight. In this way, inventory requiring further review and remediation can be tracked externally as part of the user’s existing issue-tracking system.

For example, a Code Insight scan might uncover security vulnerabilities or “copyleft” licenses requiring further review by the Security and Legal teams. With an ALM integration, these issues can be quickly converted into work items that point to corresponding issues in the ALM instance.

Integration with a specific ALM system is enabled through a corresponding Code Insight connector that supports pre-populated data (in the form of one or more instances) used to connect to the ALM system and to set up work items. Additionally, a given ALM instance controls the synchronization of data between Code Insight and the server based on a configured synchronization frequency.

To configure an ALM connector, the system or application administrator defines one or more of these instances in Code Insight, a process described in the “Integrating with Application Life Cycle Management” chapter in the FlexNet Code Insight Installation and Configuration Guide.

Then, in order to create and manage work items for a given project, you must associate the project with a specific ALM instance. The following sections describe how to associate (and unassociate) a project with an ALM instance. Currently, Code Insight is installed with a Jira connector. Future releases will provide additional support for other ALM systems.

- Associating a Jira Instance to a Project
- Using Code Insight Variables
- Unassociating an ALM Instance from a Project

Associating a Jira Instance to a Project

Use the following instructions to associate a Code Insight project with a Jira instance.
To associate a Jira instance to a project, do the following:

1. As the Project Owner, navigate to the Summary tab (see Opening the Project Summary Tab).

2. Click Manage Project and select Edit Project from the popup menu. The Edit Project page opens.

3. Select the ALM Settings tab.

4. From the ALM Instance dropdown, select the Jira instance to associate to this project. The current settings for the Jira instance are displayed on ALM Settings tab.

   If no instances are available in the dropdown, ensure that at least one instance is configured at the application level. Instructions for configuring a Jira instance are found in the FlexNet Code Insight Installation and Configuration Guide.

5. Complete the fields on the ALM Settings tab. See the inline help for explanations of the fields.

   - Certain fields might already contain a value based on the global application defaults set when the Jira instance was created (as described in the FlexNet Code Insight Installation and Configuration Guide.) However, you can override any global defaults with the information you enter here. For example, if you change the Default Issue Type from Task to Bug, the value Bug becomes the new default for this project. See ALM Tab for field details.

   - You can include (or override) Code Insight variables in the Default Summary and Default Description fields. These variables will be replaced by actual values in descriptive text that displays for a newly created Jira issue and work item. For more information, see the next section, Using Code Insight Variables.

6. When you have completed the settings, click Save to associate the Jira instance to the project.

   Validation for these field values takes place during work item creation. If the information entered here is invalid (for example, the Assignee value does not exist in the Jira system), the information will still be saved, but users will not be able to create the work item in the future.

   Once you have associated the Jira instance with the project, all work items created in this project will have a corresponding Jira issue on the provided instance.

Using Code Insight Variables

The Default Summary Text and Default Description Text fields support Code Insight variables that communicate details about the Code Insight project, inventory item, and other relevant information in the work item and associated Jira issue.

Supported Variables

The following table lists the available variables for use in the text entered in the Default Summary Text and Default Description Text fields:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$PROJECT_NAME</td>
<td>Name of the Code Insight project containing the issue</td>
</tr>
<tr>
<td>$INVENTORY_ITEM_NAME</td>
<td>Name of the inventory item containing the issue</td>
</tr>
<tr>
<td>$COMPONENT_NAME</td>
<td>Name of the component associated with the inventory item</td>
</tr>
</tbody>
</table>
Table 2-9 • Supported Code Insight Variables for Use in Work Item Summary and Description Text (cont.)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$VERSION_NAME</td>
<td>Version of the component associated with the inventory item</td>
</tr>
<tr>
<td>$LICENSE_NAME</td>
<td>Name of the selected license for the inventory item</td>
</tr>
<tr>
<td>$NUMBER_VULNERABILITIES</td>
<td>Total number of security vulnerabilities associated with the inventory item</td>
</tr>
<tr>
<td>$NUMBER_FILES</td>
<td>Total number of files associated with the inventory item</td>
</tr>
<tr>
<td>$INVENTORY_URL</td>
<td>Link to the inventory item</td>
</tr>
</tbody>
</table>

When the work item is created, the included variables are replaced by their respective values.

**Example Use of Variables**

The following is example text you might enter in the Default Summary Text field. The text includes some of the available variables:

The $INVENTORY_ITEM_NAME inventory item in the project $PROJECT_NAME contains $NUMBER_VULNERABILITIES vulnerabilities that require review. Go to $INVENTORY_URL to see the vulnerable inventory item.

If your Code Insight project name is MySampleProject and the name of the inventory item name for which you create a work item is Apache Commons BeanUtils, the work item and Jira issue will display the following summary:

The Apache Commons BeanUtils 1.7.0 (Apache 2.0) inventory item in the project MySampleProject contains 18 vulnerabilities that require review. Go to https://my.sample.server:8888/codeinsight to see the vulnerable inventory item.

**Unassociating an ALM Instance from a Project**

The Project Owner may unassociate an ALM instance from a project at any time. If the association is removed, any existing work items will remain with the project, but the Create Work Item option becomes disabled.

**Task**

To unassociate an ALM instance from a project, do the following:

1. As the Project Owner, navigate to the Summary tab (see Opening the Project Summary Tab).
2. Click Manage Project and select Edit Project from the popup menu. The Edit Project page opens.
3. Select the ALM Settings tab.
4. In the ALM Instance dropdown, change the selection to None.
Changing Project Owners

FlexNet Code Insight provides the ability to change the owner of a project. This feature enables you to transfer the ownership of a project to a new user when the current Project Owner is unavailable to administer the project. Any user who is an Administrator or the current Project Owner can change the owner. (The user who created the project automatically becomes the initial Project Owner.)

Note • Changing a Project Owner is a silent transaction. No email notifications will be sent as part of this operation.

Task

To change the Project Owner, do the following:

1. Log into FlexNet Code Insight as an Administrator or the current Project Owner.
2. Navigate to the Summary tab (see Opening the Project Summary Tab).
3. Open the Manage Project dropdown menu and select Change Owner, or click the Change Owner button, whichever is visible. The Select new project owner dialog appears.

Note • If you have not logged in as Administrator or Project Owner, neither the Manage | Change Owner menu option nor the Change Owner button is visible.

4. Highlight a name in the list and click Apply. The Summary tab is opened with the selected name displayed in the Owner field.

Note • If you change the owner to a user without Administrator or Project Management permissions, only the Generate Audit Report option will be available at the bottom of the Summary tab.

Rescanning Your Codebase

During a codebase scan, FlexNet Code Insight uses a combination of Automated Analysis and Advanced Analysis techniques to identify open-source and third-party code in your product (see What Is a FlexNet Code Insight Scan?). Advanced Analysis is performed only if the Compliance Library (CL) has been installed in your Code Insight system and the scan settings for your project have enabled this type of analysis.

Each analysis type runs its own scan. When you run the initial scan on your codebase, both analysis types perform a full scan (that is, a scan on all codebase files). For any subsequent codebase rescan that a user initiates, each analysis type performs either a full rescan, an incremental rescan (that is, a scan on only changed codebase files), or no rescan. The type of rescan executed for an analysis type depends on changes that might have occurred in your codebase, in your scan settings, or with your Code Insight or CL version prior to the rescan.

You always have the option to force a full rescan when necessary if no codebase, scan configuration, or Code Insight version changes have occurred that would normally result in a full rescan. However, keep in mind that a full rescan can be costly.
The following topics provide information you should know about the rescan process and includes instructions on initiating a rescan:

- Change Events Resulting in Full or Incremental Rescans
- Effects of Scan-Setting Changes on Rescans
- Handling of Edited Inventory During Rescans
- Initiating a Codebase Rescan
- Forcing a Full Codebase Rescan

Change Events Resulting in Full or Incremental Rescans

The following table shows the types of change events that result in a full or an incremental rescan for Automated Analysis and Advanced Analysis should you initiate a rescan on your codebase:

<table>
<thead>
<tr>
<th>Changes to...</th>
<th>Automated Analysis</th>
<th>Advanced Analysis</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codebase files</td>
<td>Incremental rescan</td>
<td>Incremental rescan</td>
<td>Changes in codebase files are determined by the MD5 hash digest of the files.</td>
</tr>
<tr>
<td>Automated Analysis rule set</td>
<td>Full rescan</td>
<td>No rescan</td>
<td>Rules are automatically pushed to your Code Insight server through an internal process and the weekly Electronic Update.</td>
</tr>
<tr>
<td>FlexNet Code Insight version</td>
<td>Full rescan</td>
<td>No rescan</td>
<td>This change usually involves an upgrade in the Code Insight version.</td>
</tr>
<tr>
<td>Scan profile settings</td>
<td>Full rescan</td>
<td>Full rescan</td>
<td>Depending on the scan profile settings that were changed, one or both analysis types will perform a full rescan. Note that changes to settings that apply to source-code matching result in an expensive Advanced Analysis full rescan. See Effects of Scan-Setting Changes on Rescans for more information. Scan profiles are configured by the Administrator as described in the FlexNet Code Insight Installation and Configuration Guide.</td>
</tr>
</tbody>
</table>

Note • Custom detected rules are applied only during the initial codebase scan and during a forced full rescan. These rules are not applied during a normal rescan, whether incremental or full.
Effects of Scan-Setting Changes on Rescans

One type of change event that does effect a full rescan by either Automated Analysis or Advanced Analysis (or both) is an update to settings in the scan profile associated with the rescan. Depending on which settings have changed, the full rescan could be more expensive (requiring more time and resources) than other full rescans.

Note • Keep in mind that, if you have applied a new scan profile to your project, only those profile settings that are different from the settings in the previously associated profile will impact the rescan.

The following table provides a list of the scan profile settings and the type of full rescan to expect should any of the settings be updated prior to a codebase rescan.

Table 2-11 • Types of Full Rescan to Expect Should Scan Profile Settings Change

<table>
<thead>
<tr>
<th>Scan Profile Settings</th>
<th>Automated Analysis</th>
<th>Advanced Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>A change to any of these settings:</td>
<td>Full rescan</td>
<td>—</td>
</tr>
<tr>
<td>• Perform Package/License Discovery in Archive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Dependency Support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Automatically Add Related Files to Inventory</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A change to any of these settings: Full rescan (expensive)

• Source Code Matches

Related fields:

• Include System Identified Files
• Include Files with Exact Matches
• Minimum Source Code Matches
**Handling of Edited Inventory During Rescans**

FlexNet Code Insight enables you to make changes to inventory both in *Analysis Workbench* and on the *Project Inventory* tab. You create inventory items as well as edit both user-created and system-generated inventory. Edits to existing inventory can include changes to the following elements in an inventory item:

- The component version string or the associated license.
- Codebase-file associations (only in *Analysis Workbench*).
- Inventory properties, Notices text, and notes.

However, normal Code Insight rescan behavior can result in actions that impact your inventory changes. For example, an updated Automated Analysis rule set might associate codebase files to an inventory item different from the one to which you have manually associated these files. Logically, the rescan should remove the associations you defined and re-apply them to the inventory item identified in the rule set. However, losing the manual changes might not be desirable.

The following topics describe how the rescan process handles edited inventory:

- **Rescan Rules to Preserve Inventory Data**
- **Rescan Scenario: Handling of Files Manually Disassociated from Inventory Before Rescan**

**Rescan Rules to Preserve Inventory Data**

In general, a full or incremental rescan can add or disassociate files and overwrite properties for any existing system-generated inventory that has not been manually updated. However, the rescan does retain the existing status and priority for such inventory items, as well as any existing notes or Notices text (although the scan can append new notes or Notices text).

For inventory that you have manually edited or created, the rescan applies the following rules:

- All the user-created inventory, its file associations, and edits are considered not system-updatable and therefore are preserved.
- Any manual change to a system-generated inventory item (including updates to the associated component) results in the inventory item being classified as user-created and therefore not system-updatable (see the previous rule.) However, the rescan can add additional files to the inventory item if the component, version, and license match.
- If one or more files were manually disassociated from a system-generated inventory item before the rescan, rescan logic assumes that these files were erroneously associated with the component initially. Therefore, the rescan does not attempt to re-associate these files to the inventory item; nor does it associate the files with another inventory item that uses the same component name (with a different version or license). The following example scenario illustrates this rule.
Rescan Scenario: Handling of Files Manually Disassociated from Inventory Before Rescan

The following scenario demonstrates how the rescan process handles files that you manually disassociated from a system-generated inventory item before the rescan.

In this scenario, the initial scan on your codebase generated the inventory item `log4j 2.6` and associated the files `file1.jar` and `file2.jar` with the item.

However, after analyzing the inventory, you realize that `file2.jar` should be associated instead with `log4j 2.11`, an inventory item that does not exist in your current inventory. To remedy this, you perform the following steps:

1. Create an inventory item named `log4j 2.11`.
2. Disassociate the `file2.jar` from `log4j 2.6`.
3. Associate `file2.jar` with the inventory item `log4j 2.11` that you just created.

On rescan, your edits remain intact:

- The file `file1.jar` remains associated with the inventory item `log4j 2.6`.
- The inventory item `log4j 2.11` that you created is preserved along with its association with the file `file2.jar`.

The rescan also results in the creation of a new system-generated inventory item, `log4j 2.10`. However, the rescan does not associate the file `file2.jar` with the new inventory item.

Initiating a Codebase Rescan

Use the following procedure to rescan your codebase.

Refer to the FlexNet Code Insight User Roles and Permissions appendix for role requirements to scan a codebase.

<table>
<thead>
<tr>
<th>Task</th>
<th>To start the rescan, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to the Summary tab (see Opening the Project Summary Tab).</td>
</tr>
<tr>
<td>2.</td>
<td>Perform either step:</td>
</tr>
<tr>
<td></td>
<td>• Click the Start Scan button. If a scan is currently running or the Scan Server is currently not active, this button is disabled. You can use the second option (see next bullet) to schedule a scan.</td>
</tr>
<tr>
<td></td>
<td>• Click the link in Scan Status to schedule a scan. If other scans are running, the scan is queued and will automatically run based on queue order. If the Scan Server is inactive, the scan will automatically start based on queue order once the server is running again. (Click the link in Past Scans to view details about the scheduled scan.)</td>
</tr>
</tbody>
</table>

Information about the scan's progress is shown in the Scan Status section on the Summary tab.
When the scan completes, the **Scan Status** will display one of the following messages:

- **Completed**—The scan succeeded with no warnings during scan or analysis. This message appears on screen in green.
- **Completed with warnings**—The scan succeeded but the analysis has warnings.
- **Failed**—The scan failed. This message appears on screen in red.

**Note** • If the scan completed with a warning or if it failed, check your scan log for more information.

For an overall understanding of the scan results, see **Overview of Scan Results**.

### Forcing a Full Codebase Rescan

A forced full-codebase rescan enables you to scan your entire codebase at any time even if no change has occurred in your codebase, in your scan settings, or with the FlexNet Code Insight or Compliance Library (CL) version. Such a rescan might be required, for example, to view the latest changes to inventory or to apply any new custom detection rules. See the following topics for more information:

- **Forcing a Full Rescan**
- **Custom-rule Application During a Forced Full Rescan**

Keep in mind that a full rescan can be costly.

For general information about how any rescan handles existing system-generated inventory and manually created or updated inventory, see **Handling of Edited Inventory During Rescans**. For specific information about how the forced full rescan applies custom rules to existing system-generated inventory, see **Custom-rule Application During a Forced Full Rescan**.

### Forcing a Full Rescan

Use the following procedure to initiate a full codebase rescan.

**Task**

To force a full project rescan, do the following:

1. Navigate to the **Summary** tab (see **Opening the Project Summary Tab**).
2. Click the drop-down arrow next to the **Start Scan** button.
3. Select **Full Rescan**.
   
   A confirmation message box is displayed asking you to confirm that you want to continue with the rescan.

4. Select **Yes**.

   Information about the scan’s progress and its completion status is shown in the **Scan Status** section. For details, see the last step in *Initiating a Codebase Rescan*.

**Custom-rule Application During a Forced Full Rescan**

Custom rules are applied only during the initial codebase scan and during a forced full rescan. During the forced full rescan, if a previously scanned file now matches a new custom rule, the existing system-generated inventory item for that file is overwritten with the custom-rule data. The following two scenarios describe this over-write process.

---

**Note** • *Custom rules affect only system-generated inventory items that have not been manually updated. The rules have no impact on manually-created (custom) inventory items and on system-generated inventory items that users have updated.*

---

**Scenario 1: The custom-rule data identifies the same component version and license as the existing inventory item**

In this case, the scan applies the custom rule by updating the existing inventory item as follows:

- Appends new detection notes to reflect the custom rule.
- Updates the **Created by** field value for the inventory item to **High Confidence Custom Auto-WriteUp Rule** in the **Analysis Workbench**.

Note that, in this scenario, the scan retains the **Audit Notes**, **As-Found License Text**, or **Notices Text** content defined in the existing inventory item. It does not append custom-rule data to these fields.

**Scenario 2: The custom-rule data identifies a component version and license different from the existing inventory item**

In this case, the scan applies the custom rule as follows:

- Creates a new inventory item based on the custom-rule data.
- Retains the existing inventory item, but disassociates its files and adds them to the new inventory item.
- Applies the status and priority of the existing inventory to the new inventory item.
- Appends any **Audit Notes**, **As-Found License Text**, or **Notices Text** content defined in the custom rule.

---

**Exporting Project Data**

FlexNet Code Insight allows you to export your project data to a JSON data file for use elsewhere. The following procedure describes how to export project data using the Code Insight Web UI.

For complete information about the export feature (including how to export project data using the public REST API), see the *Exporting and Importing Project Data* chapter.
Managing a Project from the Summary Tab

**Task**  
**To export project data, do the following:**

1. As Project Owner, navigate to the **Summary** tab (see **Opening the Project Summary Tab**).
2. Click **Manage Project** and select **Export Project Data** from the dropdown menu.
3. When prompted, select a location to store the exported data. FlexNet Code Insight creates a JSON data file, archives it in a .zip file and saves it in to a location specified in your browser settings.

**Importing Project Data**

FlexNet Code Insight allows you to import data from one FlexNet Code Insight project into another project. The data to be imported must be in a properly formatted and archived JSON file, such the archive resulting from an export described in **Exporting Project Data**. The following procedure describes how to import project data using the Code Insight Web UI.

For complete information about the import feature (including how to import project data using the public REST API), see the **Exporting and Importing Project Data** chapter.

**Task**  
**To import project data, do the following:**

1. As Project Owner, navigate to the **Summary** tab (see **Opening the Project Summary Tab**).
2. Click **Manage Project** and select **Import Project Data** from the dropdown menu.
3. Complete the fields as described in **Import Project Data Dialog**.
4. Click **OK** to perform the import.
   - If the import fails for some reason, an error dialog is displayed. Click **OK** and attempt the import again.
   - If the import completes successfully, a message dialog is displayed, stating as such. Click **OK**.

**Deleting a Project**

Project Owners can use this procedure to delete any of their projects.

**Task**  
**To delete a project, follow these steps:**

1. As Project Owner, navigate to the **Summary** tab (see **Opening the Project Summary Tab**).
2. Click **Manage Project** and select **Delete Project** from the dropdown menu.
3. When prompted, select **Yes** to proceed with the deletion. If the Scan Server associated with the project is temporarily inactive or is disabled, a pop-up is displayed to inform you that the server is down.
Creating a Private Project

Security-conscious Project Owners can control access to their projects within the enterprise by setting a project’s visibility to Private. This feature gives Project Owners the ability to hide sensitive information from general view and select specific users who can view the project. The default project visibility is Public, which means that all FlexNet Code Insight users can view all projects. For information about assigning roles, see Assigning Project Roles to Users.

Note • Users who have Administrator privileges but are not part of a Private project can see the project in the Projects list, view the Summary tab for the project, and change the owner of the project.

Task  
To create a private project, do the following:

1. If you are not viewing the Project list, navigate to it.
2. Click Add New. The Add Project dialog appears with default values appearing in all the fields but Name.
3. In the Name field, enter a name for the new private project.
4. From the Project Visibility dropdown, select Private.
5. Complete the other fields as described in Creating a Project.
6. Click Save to save the new private project.

If the user is not a Project Owner, Project Analyst, Project Reviewer, or Project Observer for this Private project, the project will not be visible on the Project Folders page; and the project and vulnerability ID searches will not return private projects unless the user has the rights to see these projects.

7. (Optional) Assign roles to users who will interact with the private project. For more information, see Assigning Project Roles to Users.

Managing Policy Profiles

This section describes the purpose of policies in FlexNet Code Insight and provides procedures for adding, editing, copying, and deleting policies. The following topics are included:

- Understanding Policy Profiles
- Adding or Editing a Policy Profile
- Copying a Policy Profile

Understanding Policy Profiles

Policy profiles are used by FlexNet Code Insight to automate the inventory review process—that is, automatically mark published inventory items as approved, rejected, or requiring a manual review—without the need for a manual review. Policy profiles can be defined up-front or revised during the manual inventory review process. The Code Insight Administrator grants the Manage Policy role to users who have rights to manage policy profiles. Typically, these would be legal or security users.
Code Insight provides a default policy profile (called Default License Policy Profile) that can be used as is, modified, or copied to fit your need. This policy profile contains typical settings for a team who is distributing software. You can also create policies from scratch.

The topics covered in this section include:

- How Policy Profiles Work in the Automated Inventory-Review Process
- Adding or Editing a Policy Profile
- Copying a Policy Profile
- Associating a Policy Profile with a Project

How Policy Profiles Work in the Automated Inventory-Review Process

A policy profile is defined with a set of policy criteria based on components, licenses, or security vulnerabilities. Any conflicting criteria are resolved in favor of an automated rejection of the inventory item. In other words, rejections will always take precedence over approvals. A criterion in the policy profile can also optionally include usage guidance text as a way to communicate with the developer any obligations or best-practices related to a given inventory item. The policy criteria are evaluated when an inventory item is published. If none of the criteria in the profile applies to a given inventory item, the system leaves the inventory item in a Not Reviewed (requiring a manual review) state.

You can further automate the inventory review process by setting policies that define what action Code Insight takes once an item is rejected or assigned a Not Reviewed status. See Updating Inventory Review and Remediation Settings for a Project for details.

Adding or Editing a Policy Profile

The following procedure describes how to add a new policy profile or edit an existing one.

Note • If the FlexNet Code Insight administrator changes the CVSS version for Code Insight, policies you defined in this profile might have changed. For more information, see Impact on Policies When CVSS Version Changes on System for details.

Task • To add a new policy profile or edit an existing one, do the following:

1. Click the Open Menu icon in the upper right of any FlexNet Code Insight page:

2. Select Policy from the menu to open the Policies page, showing the list of current policy profiles.

3. To edit an existing policy profile, select it from the list, and click the Edit icon .

   or

   To add a new policy profile, click Add Policy.
The **Policy Details** page is displayed.

4. Refer to the associated help (or to Policy Details Page) for details about the fields used to define the policy profile.

5. Click **Save** to save the updates or to add the new policy profile.

## Copying a Policy Profile

The following procedure describes how to create a copy an existing policy profile. This can be useful for providing a template to create a new policy profile or for backing up an existing one.

<table>
<thead>
<tr>
<th>Task</th>
<th>To copy an existing policy, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click the <strong>Open Menu</strong> icon in the upper right of any FlexNet Code Insight page:</td>
</tr>
<tr>
<td>2.</td>
<td>Select <strong>Policy</strong> from the menu to open the <strong>Policies</strong> page, showing the list of current policy profiles.</td>
</tr>
<tr>
<td>3.</td>
<td>Select the policy profile to copy from the policy list, and click <strong>Copy</strong> icon.</td>
</tr>
</tbody>
</table>

A new policy with the name **Copy of policy name** is added to the **Policy** list. You can then edit the new policy to change its name or update its criteria. See Adding or Editing a Policy Profile.

## Associating a Policy Profile with a Project

The Project Owner can associate a project with a policy profile when the project is created (see Creating a Project) or later by editing the project (see Updating Inventory Review and Remediation Settings for a Project). If no policy is explicitly selected for a project, the Default License Policy Profile is used.

## Managing Authorization Tokens

FlexNet Code Insight uses a JSON Web Token (JWT) to authorize user access to the Code Insight public REST interface. You might be required to explicitly enter an authorization token for certain functionality that uses this REST interface directly (that is, not through Code Insight web UI), such as the following:

- Project import and export processes (see the Exporting and Importing Project Data chapter)
- The execution of remote scan agents (see Performing Inventory-Only Scanning)

Code Insight enables you to generate and manage one or more of these authorization tokens.

An authorization token is for use by the Code Insight user account that creates it. Thus, an authorization token that your user account generates will give you REST access to only the Code Insight functionality for which your account has permissions. Additionally, you can view and manage only those authorization tokens for the user account under which you are logged in.

Authorization tokens are created and managed from **Preferences** page, as described in the following procedures:

- Accessing the Preferences Page
Chapter 2  Using FlexNet Code Insight
Managing Authorization Tokens

- Generating an Authorization Token
- Copying the Authorization Token to the Clipboard
- Editing the Token Name
- Deleting an Authorization Token

Accessing the Preferences Page

Use these steps to open the Preferences page.

<table>
<thead>
<tr>
<th>Task</th>
<th>To open the Preference page, use these steps:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Ensure</td>
</tr>
<tr>
<td></td>
<td>2. Click the Open Menu icon in the upper right of any FlexNet Code Insight page:</td>
</tr>
<tr>
<td></td>
<td>3. Select Preferences to open the Preferences page.</td>
</tr>
</tbody>
</table>

Generating an Authorization Token

Use the following procedure to generate an authorization token.

<table>
<thead>
<tr>
<th>Task</th>
<th>To generate an authorization token, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Access the Preferences page (see Accessing the Preferences Page).</td>
</tr>
<tr>
<td></td>
<td>2. From the AUTH Tokens pane, click Add Token.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a name for the new token and specify an expiration date (or choose Never Expires).</td>
</tr>
<tr>
<td></td>
<td>4. Click Save.</td>
</tr>
</tbody>
</table>

Copying the Authorization Token to the Clipboard

Use the following procedure to copy an authorization token to the clipboard so that you can paste it in your REST API interface.

<table>
<thead>
<tr>
<th>Task</th>
<th>To copy an authorization token to the Clipboard, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Access the Preferences page (see Accessing the Preferences Page).</td>
</tr>
<tr>
<td></td>
<td>2. From the AUTH Tokens pane, locate the token you want to copy, and click the Copy to clipboard icon ( bölümü in the Actions column.</td>
</tr>
</tbody>
</table>
3. Click **Select Token Text** to select the entire token value, and then press Ctrl + C to copy it.

4. Paste token in the appropriate location for use by the REST interface.

## Editing the Token Name

You can edit only the name of an authorization token, not its expiration date or value.

<table>
<thead>
<tr>
<th>Task</th>
<th>To edit the token name, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Access the <strong>Preferences</strong> page (see Accessing the Preferences Page).</td>
</tr>
<tr>
<td>2.</td>
<td>From the <strong>AUTH Tokens</strong> pane, locate the token you want to edit, and click the Edit icon (📝).</td>
</tr>
<tr>
<td>3.</td>
<td>Update the token name as needed.</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional) To copy the token value to the Clipboard for pasting into the REST interface, click <strong>Select Token Text</strong> to select the entire token value, and then press Ctrl + C to copy it.</td>
</tr>
</tbody>
</table>

## Deleting an Authorization Token

Use the following procedure to delete an authorization token.

<table>
<thead>
<tr>
<th>Task</th>
<th>To delete an authorization token, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Access the <strong>Preferences</strong> page (see Accessing the Preferences Page).</td>
</tr>
<tr>
<td>2.</td>
<td>From the <strong>AUTH Tokens</strong> pane, locate the token you want to edit, and click the Edit icon (✗).</td>
</tr>
</tbody>
</table>
Performing Advanced Searches

This chapter discusses FlexNet Code Insight’s advanced inventory searching capabilities:

- Advanced Searches
- Dependencies in Advanced Searches

Advanced Searches

Although you could use the simple search on the Project Inventory tab to find inventory items that match text strings, FlexNet Code Insight provides the ability to use additional criteria to display only the items that are of interest. (Simply click the Advanced Search button on this tab to access the Advanced Search dialog.) Many combinations of search criteria are available, depending upon the type of inventory you want to find. The following table, which is arranged by persona (job function or department), presents a number of advanced searches and their typical results.

For details about using the Advanced Search dialog and all its available search fields, see Searching Published Inventory and Advanced Inventory Search Dialog

Table 3-1 • Sample Advanced Searches

<table>
<thead>
<tr>
<th>Persona</th>
<th>Search Type</th>
<th>Finds...</th>
<th>Example</th>
</tr>
</thead>
</table>
| Any     | By inventory, component, or license keyword | Inventory of interest based on full or partial inventory, component or license name. Useful when you want a quick search for a specific component or license across all of your inventory items. | Inventory Name = zlib 1.2.8 (zlib/libpng License)  
Inventory Name = zlib  
License Name = EPL |
### Table 3-1 • Sample Advanced Searches

<table>
<thead>
<tr>
<th>Persona</th>
<th>Search Type</th>
<th>Finds...</th>
<th>Example</th>
</tr>
</thead>
</table>
| Any | By criticality (priority) | Most critical inventory that requires security or legal review based on presence of high-severity vulnerabilities or P1 licenses. Useful when you want to prioritize your inventory review by most important findings. | **Option 1:**  
Inventory Priority = P1  
**Option 2:**  
Security Vulnerability Severity = High or License Priority = P1 - Viral/Strong Copyleft |
| Any | By review status | Inventory that requires further review (Not Reviewed), is Approved, or is Rejected. Useful to identify items that are yet to be reviewed. Also when you are further qualifying other search criteria with an additional expression based on review status. | Inventory Review Status = Approved |
| Any | By dependencies | Only dependency inventory items (both first-level and transitive dependencies), only top-level inventory items (excluding all dependency inventory items), or all inventory items. Useful for focusing on or filtering out dependency inventory items. | Dependency Options = All Inventory Items  
Dependency Options = Only Top-Level Inventory Items  
Only Dependency Inventory Items = Only Dependency Inventory Items |
| Any | By inventory age | Inventory created within the specified time range. Useful to filter to recent inventory items, which is especially valuable when a user logs into FlexNet Code Insight at a regular interval (daily, weekly, etc.). | Inventory Age = Last 7 Days |
Table 3-1 • Sample Advanced Searches

<table>
<thead>
<tr>
<th>Persona</th>
<th>Search Type</th>
<th>Finds...</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>By notification</td>
<td>Published inventory items that have new security vulnerability alerts or that have been rejected due to new non-compliant security vulnerabilities. You can select one or both options. Useful for filtering to published inventory items that have important new security information or that have been rejected due to new security issues that are non-compliant with policy.</td>
<td>Inventory with Open Alerts = checked Inventory Rejected Due to New Non-Compliant Security Vulnerabilities = checked</td>
</tr>
<tr>
<td>Any</td>
<td>By task status</td>
<td>Inventory tasks by their Open or Closed status. Useful for determining the work required before the inventory review process can be completed. Also useful for locating inventory whose closed tasks might need to be reopened for extra work.</td>
<td>Task Status = Open Task Status = Closed</td>
</tr>
<tr>
<td>Any</td>
<td>By task type</td>
<td>Inventory tasks by their type. Useful for filtering to inventory that requires a manual legal or security review (Manual Inventory Review), source-code changes to make it compliant or secure (Remediate Inventory), or another type of effort (Miscellaneous).</td>
<td>Task Type = Manual Inventory Review Task Type = Remediate Inventory Task Type = Miscellaneous Task Type = Any</td>
</tr>
<tr>
<td>Any</td>
<td>By inventory task age</td>
<td>Inventory tasks created within the specified date range. Useful for keeping track of new work to be performed on inventory and old work still needs to be addressed.</td>
<td>Inventory Tasks Age = Last 7 days Inventory Tasks Age = Custom Date Range From: 09/05/2018 To: 10/31/2018</td>
</tr>
<tr>
<td>Any</td>
<td>By inventory task owner</td>
<td>Inventory tasks owned by a specific user. Useful for determining the workload of a specific user.</td>
<td>Inventory Tasks Owner = Any Inventory Tasks Owner = Only mine (current user) Inventory Tasks Owner = &lt;Username&gt; (selected user)</td>
</tr>
</tbody>
</table>
**Table 3-1 • Sample Advanced Searches**

<table>
<thead>
<tr>
<th>Persona</th>
<th>Search Type</th>
<th>Finds...</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyst, Reviewer</td>
<td>By Confidence Level</td>
<td>Inventory generated with a specific level of confidence (High, Medium, or Low). The level is based on the measure of the strength of the discovery technique used to generate the item. (See Inventory Confidence in the “Using FlexNet Code Insight” chapter.) Useful for determining whether the item should be triaged or reviewed to validate or further refine the finding.</td>
<td>Inventory Confidence Level = <em>High</em> (or <em>Medium</em> or <em>Low</em>)</td>
</tr>
<tr>
<td>Security Analyst</td>
<td>By vulnerability ID</td>
<td>Inventory with a specific vulnerability (NVD CVE or Secunia Advisory).</td>
<td>Security Vulnerability ID = SA71946</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Useable when you are looking for inventory exposing you to a specific security issue, typically a newsworthy event.</td>
<td></td>
</tr>
<tr>
<td>Security Analyst</td>
<td>By security risk exposure</td>
<td>Inventory containing security vulnerabilities of a specified severity.</td>
<td>Security Vulnerability Severity = <em>High</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Useable to filter to inventory items that require immediate attention based on your corporate security policy. For example, we must address all high-severity security issues in the current release.</td>
<td></td>
</tr>
<tr>
<td>Security Analyst</td>
<td>By security vulnerability age</td>
<td>Inventory with new security vulnerabilities since a specified date.</td>
<td>Security Vulnerability Age = <em>Last day</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Useful to see which inventory items have new security vulnerabilities reported against them based on the specified date range.</td>
<td></td>
</tr>
<tr>
<td>Security Analyst</td>
<td>By security risk exposure and vulnerability age</td>
<td>Inventory with new security vulnerabilities of a specified severity since a specified date.</td>
<td>Security Vulnerability Age = <em>Last day</em> and Security Vulnerability Severity = <em>High</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Useable to see which inventory items have new security vulnerabilities reported against them based on the specified date range and a certain severity.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 3-1 • Sample Advanced Searches

<table>
<thead>
<tr>
<th>Persona</th>
<th>Search Type</th>
<th>Finds…</th>
<th>Example</th>
</tr>
</thead>
</table>
| Security Analyst          | By inventory alert                   | Published inventory items that have new security vulnerability alerts or that have been rejected due to new non-compliant security vulnerabilities. You can select one or both options. | Inventory with Open Alerts = **checked**
|                           |                                      |                                                                        | Inventory Rejected Due to New Non-Compliant Security Vulnerabilities = **checked** |
|                           |                                      | **Useful for filtering to inventory items that have important new security information or that have been rejected due to new security issues that are non-compliant with policy.** |                                                                        |
| Security Analyst          | By new vulnerabilities (requires re-review) | Inventory that has gained a new security vulnerability since a specified date. | **Review Status = Approved and Security Vulnerability Age = Last 7 days** |
|                           |                                      | **Useful to determine which inventory items require another look from a security analyst due to new associated vulnerabilities.** |                                                                        |
| Legal                     | By license risk exposure              | Most critical inventory that requires legal review (contains a P1 license - Viral/Strong Copyleft). | **License Priority = P1 - Viral/Strong Copyleft** |
|                           |                                      | **Useful to prioritize legal work based on license classification.** |                                                                        |
| Analyst                   | Requires re-review based on missing license | Approved inventory with a missing license. | **Inventory Review Status = Approved and License Priority = No License Found** |
|                           |                                      | **Useful to catch scenarios where items were approved without an associated license. This should be a rare event.** |                                                                        |
| Eng. Mgr./Final Reviewer  | Stop shipment!                        | Approved inventory that may require a stop shipment due to high severity vulnerability or P1 license. | **Inventory Review Status = Approved or License Priority = P1 - Viral/Strong Copyleft or Security Vulnerability Severity = High** |
|                           |                                      | **Useful to identify cases that would break the build. These are items that were approved at the time of review, but since then have a different license or high-severity vulnerability.** |                                                                        |
Dependencies in Advanced Searches

FlexNet Code Insight is able to scan archived and multi-layer codebases. When inventory items from these codebases are published, dependencies can be published as well. However, when performing searches on published inventory, the amount of data returned can be immense. So it is important to consider whether to include or exclude them in your inventory searches.
Exporting and Importing Project Data

The following sections describe the project export and import functionality in FlexNet Code Insight:

- About Exporting and Importing
- Prerequisites When Using the REST Interface
- Exporting Project Data
- Importing Project Data

About Exporting and Importing

FlexNet Code Insight provides export and import functionality for project data. The export-import process can be performed on the same server or across servers. Project data can be quickly imported into an empty project to create inventory or imported into a scanned project to create inventory with file associations. The imported inventory in both cases is “live”—that is, ready to be reviewed and edited.

Export and import functionality is useful in any of these following scenarios:

- **Backup of project and audit data**—Use export to create a full backup of a Code Insight project. The backup data file includes project and scan details, all inventory (with inventory details, field values, file associations, and inventory status), the review status of files, and any custom data. The project data can be restored to a new project for an archived view or for ongoing scanning and auditing.

- **Copying or branching a project**—Use the export-import process to create an exact copy of a project for future scanning and audit work. To do this, export the data from the source project, scan the target project (pointed to the same codebase), and import the data into the target project. The target project can be used for continued scanning and analysis work while the source project remains unchanged.

- **Versioning a project**—Use the export-import process to apply analysis work performed on one product version to the next product version. For example, you can apply the analysis work performed on project “foo-v1” to project “foo-v2”. To do this, export the data from “foo-v1”, scan “foo-v2”, and import the data into “foo-v2”.
Prerequisites When Using the REST Interface

The following are prerequisites when using the FlexNet Code Insight REST interface to execute an export or import:

- **REST Client or Command-Line Tool Supporting cURL**
- **Authorization Token**
- **Project ID**

These prerequisites are not needed if you are performing an export or import using the FlexNet Code Insight Web UI.

**REST Client or Command-Line Tool Supporting cURL**

A REST client or command-line interface with cURL support is required to execute the cURL commands that call the REST API to export or import project data.

To download cURL, go to https://curl.haxx.se/download.html. Once cURL is installed, ensure that it is added to your PATH environment variable so that you can use it with batch or PowerShell scripts and call it from the command prompt of any working directory.

**Authorization Token**

Using the REST interface requires a valid JSON Web Token (JWT) for the owner of the project from which data is to be exported or to which data is to be imported. For instructions on obtaining the JWT, see Managing Authorization Tokens in the “Using FlexNet Code Insight” chapter. The token is not required if using the Web UI.
Project ID

When using the REST interface to execute an import or export, you need to provide the ID of the project from which you are exporting data or the project to which you are importing data.

You can obtain the project ID visually through the FlexNet Code Insight Web UI or programmatically through the REST interface.

**Obtaining the Project ID from the FlexNet Code Insight Web UI**

The following are just a few options you can use to obtain the project ID from the Web UI.

**Task**

*To obtain the project ID through the Web UI, do either of the following:*

- Locate the **Name** value on the **Project Summary** page for the project. The ID is displayed in parentheses:

![FlexNet Code Insight](image)

- Locate the project ID included in the URL on any of the project pages, as shown in this example:

![FlexNet Code Insight](image)

**Obtaining the Product ID Through the REST Interface**

Obtain the project ID by issuing a cURL command that calls the **Get Project Id** REST API.

**Important** • If copying the cURL command directly from the following instructions for your own use, copy it to a text editor first to remove formatting and any line breaks or extra spaces.

**Task**

*To obtain the project ID by calling the Get Project Id REST API, do the following:*

Execute the following cURL command that invokes the **Get Project Id** REST API using the GET method. Replace the highlighted variables with your server host ID (hostname or IP address) and port, project name, and authorization token.

```
curl -X GET "HOST:PORT/codeinsight/api/project/id?projectName=PROJECT_NAME" -H "accept: application/json" -H "Authorization: Bearer JWT_TOKEN"
```
The following is an example:

curl -X GET "http://localhost:8888/codeinsight/api/project/id?projectName=AllTypes" -H "accept: application/json" -H "Authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbiIsInVzZXJJZCI6MSwiaWF0IjoxNTY2ODU5NTg2fQ.qV2j8ZLhGNeOsTsT8OdPRwE0-8y1x7w-0zr3h752d9uqY8mvAcV68posEU9tdh-XYl6xznX-1GnnpDQ87G3w"

**Note** • If the project name contains a space or special character, replace the character with its encoded version. For example, use project%20foo for a project named project foo.

The response contains the project ID (in this example, 164):

```
{"Content":164}
```
Types of Data Exported

The export always processes project data in full—that is, there is no way to limit the exported data. Thus, the data file containing the exported data for a given project includes the following content:

- **Export information**—The project owner, the FlexNet Code Insight version from which data is being exported, the most recent Compliance Library and Electronic Update versions used by the project, the date and time of the export, and more.

- **Project details and scan settings**—The name, description, scan profile, policy profile, and scanroot path of the project from which data is being exported.

- **Inventory**—All data for the project’s inventory, including inventory fields, publication and review statuses, associated codebase files, and associated repository items.

- **Reviewed files**—The absolute file path and MD5 for each codebase file marked as reviewed.

- **Custom data**—Custom versions, licenses, and custom mappings between these entities.

**Note** • Some data contained in the exported data file is for informational purpose only and is not necessarily processed during an import.

Prerequisites for Exporting Data

To export data, ensure that the following prerequisites are met:

- A FlexNet Code Insight v7 instance that is currently running.

- An existing, non-empty project (containing at least one inventory item) on that instance.

- Items listed in Prerequisites When Using the REST Interface (if performing the export using REST API).

Exporting Project Data Using the Web UI

Use the following instructions to export project data using the FlexNet Code Insight Web UI.

<table>
<thead>
<tr>
<th>Task</th>
<th>To export project data using the Code Insight Web UI, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Ensure that all requirements in Prerequisites for Exporting Data are met.</td>
</tr>
<tr>
<td>2.</td>
<td>Log into Code Insight as the owner of the project you want to export.</td>
</tr>
<tr>
<td>3.</td>
<td>Navigate to the Project Summary tab (see Opening the Project Summary Tab).</td>
</tr>
<tr>
<td>4.</td>
<td>Open the Manage Project dropdown and select Export Project Data.</td>
</tr>
</tbody>
</table>

Depending on your browser configuration for downloads, either process can happen:

- You are prompted to enter a new name used for both the .zip archive and the data file (or keep the default name, which includes the project ID and export timestamp) and to select a download location for the archive. When you save the information, Code Insight creates the .zip archive with the name and in the location you specified.
The .zip archive is created with the default name and saved to the download location configured for your browser.

The following shows an example export archive generated on a Windows system. In this case, the archive uses the default name:

```
C:\Users\kdr\Downloads\55-export-12-22-2020_10-42.zip
```

The archive content would include the following data file:

```
55-export-12-22-2020_10-42.json
```

**Note** • If an archive with the same name exists in the export data directory, the archive is overwritten with the new data.

5. Verify that the export process completed successfully. See Verifying a Successful Export.

### Exporting Project Data Using the REST Interface

Use the following information to export project data by using a cURL command that calls the `exportProjectData` REST API.

**Important** • If copying the cURL command directly from the following instructions for your own use, copy it to a text editor first to remove formatting and any line breaks or extra spaces.

**Task** To export project data by calling the `exportProjectData` REST API, do the following:

1. Ensure that all requirements in Prerequisites for Exporting Data and Prerequisites When Using the REST Interface are met.

2. To initiate the export process, execute the following cURL command to invoke the `exportProjectData` REST API using the GET method. Replace the highlighted variables with your server host name and port, the project ID, and the authorization token. Also, replace `PROJECT_DATA_FILE` with the name that you want to give to both the JSON file containing the exported data and the .zip file in which the data file will be compressed.

```
```

The following is an example:

```
curl -X GET "http://localhost:8888/codeinsight/api/project/exportProjectData?projectId=164" -H "accept: application/json" -H "Authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbiIsInVzZXJJZCI6Miwi TWvW0joxNTV2DU5NTg2fQ_qV2j8ZLgNGJ8T8OdPRwvE8-9y1x7w-02z5h7z2d9uqY8tACsV68posEU9tD-YXlXzXnX-IGmnpDU7G3w" > ProjectKDR.zip
```

The status of the export process appears in the command prompt window:
When the export completes, Code Insight generates a .zip archive containing the project data in JSON format and saves it to the directory from which the statement was executed. The archive file name and data file name are the same (except for their extensions). For example, if the export command is executed from the C:/fnci/project_export directory and the output redirect value is ProjectKDR-export-12-22-2020_10-42.zip, the path and file name for the archive would be this:

C:/fnci/project_export/ProjectKDR-export-12-22-2020_10-42.zip

The data file within the archive would be this:

ProjectKDR-export-12-22-2020_10-42.json

**Note** • If an archive with the same name exists in the export data directory, the archive is overwritten with the new data.

3. Verify that the export process completed successfully. See Verifying a Successful Export.

### Verifying a Successful Export

Use this procedure to verify that the export process completed successfully.

1. Unzip the archive.

   If the export process was not successful, the .zip archive includes a file containing the appropriate status code and error message.

2. (Optional) Open the JSON data file with a utility that supports JSON, such as Textpad or Notepad++, to determine noticeable errors.

3. If errors exist, resolve them, delete the invalid archive file, and run the export script again.

   Otherwise, the contents of the .zip file are ready to be imported into a target project or used for backup purposes.

### Importing Project Data

The following sections provide the details about importing project data:

- About an Import
- Comparison of Standard and Inventory-Only Imports
- Prerequisites for Importing Data
- Import Behavior and Configuration
- Importing Project Data Using the Web UI
- Importing Project Data Using the REST API
- Verifying the Import Results
**Important** • The instructions in this section assume that you are importing data to the FlexNet Code Insight version for which this current documentation was published. These instructions might not apply to other Code Insight versions. If importing project data to a different Code Insight version, consult the documentation included with that version for import instructions.

### About an Import

Project data import is accessible through either of these methods:

- Importing Project Data Using the Web UI
- Importing Project Data Using the REST API

The following sections provide overview information about the import process.

#### Input Used in the Import Process

The input for the import is an archived JSON data file containing project data. The archive is first decompressed and the included data file is then applied to the specified target project (that is, the project to which the data is imported).

You can create the JSON data file for input by performing an export from a FlexNet Code Insight v7 project (according to the instructions in Exporting Project Data) or by performing an export from a Code Insight v6 project and then using the Audit Migration Tool to convert the data into the required format. You can also create the JSON file manually from data exported from an external system. In all cases, the input for the import must be a data file of the expected JSON data format.

#### Target Project Types

Import is typically performed on a target project that was created as a “standard” project and is associated with an already-scanned codebase. A scan of the target project codebase is required prior to the import in order to build the codebase file tree and to prepare the project for storing file information. This type of import creates inventory with file associations and provides access to these codebase files through the Analysis Workbench for the target project once the import completes. The inventory is live—that is, ready to be edited and reviewed.

Alternatively, an import can be performed on a target project that was created as an “inventory only” project, which does not require a scanned codebase. This type of import creates live inventory without any file associations and does not provide access to the codebase files since none are imported. (No Analysis Workbench is available in the target project.)

For more information about the import types and the data imported for each, see the next section, Comparison of Standard and Inventory-Only Imports.

### Comparison of Standard and Inventory-Only Imports

The data that is imported is controlled by the **Type** of the target project (that is, the project to which data is imported). For example, if the target project was created as a standard project (that is, its **Type** attribute is **Standard**), then the import will be a standard import. If the project was created as an inventory-only project (that is, its **Type** attribute is **Inventory Only**), then the import will be an inventory-only import.
The following table highlights the basic differences between the two import types.

**Table 4-1 • Comparison of Standard and Inventory-Only Imports**

<table>
<thead>
<tr>
<th>Import Behaviors and Usage</th>
<th>Standard Import</th>
<th>Inventory-only Import</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Import scope</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Import scope              | Performs a full import (that is, both inventory and codebase files are processed):  
|                           | • Processes all inventory items (published and unpublished).  
|                           | • Per inventory item, provides inventory details, status, and associated repository item (component-version-license).  
|                           | • Lists associated file paths for inventory.  
|                           | Performs a partial import:  
|                           | • Processes inventory only.  
|                           | • Does not process codebase files (reviewed or unreviewed).  |
| **File processing**       |                 |                       |
| File processing           | Does the following:  
|                           | • Processes all files marked as reviewed in the data file to be imported.  
|                           | • Provides absolute file paths and MD5s for processed files.  
|                           | • Does not import unreviewed files.  
|                           | Does not process files (reviewed or unreviewed).  |
| **Custom-data processing**| Imports custom versions, custom licenses, and custom mappings.* | Imports custom versions, custom licenses, and custom mappings.* |
| **Required type for target project** | Requires a project created with the Standard attribute. | Requires a project created with the Inventory Only attribute. |
| **Target project codebase requirement** | Requires a codebase that is uploaded (or synchronized) to the target project and scanned. | Requires no codebase. |
| **Access to imported inventory and codebase files** | Provides direct access to the following in the target project once the import completes:  
|                           | • The imported inventory, displayed in Project Inventory and Analysis Workbench.  
|                           | • Imported codebase files, displayed in Analysis Workbench.  
|                           | Provides direct access to imported inventory in Project Inventory only.  |
**Prerequisites for Importing Data**

To import data, ensure that the following prerequisites are met:

- A FlexNet Code Insight v7 instance that is currently running.
- An existing Code Insight project to which data will be imported. The type of import you want to perform determines the type of project needed (and vice versa):
  - To perform a standard import, you need a standard project with an uploaded and scanned codebase. The scanned codebase can be the same or similar to the one whose project data you intend to import.
  - To perform an inventory-only import, you need an inventory-only project with no scanned codebase. You are most likely to have an inventory-only project if the project was created as part of a remote scan on an external system using the FlexNet Code Insight Jenkins plugin or another Code Insight scan agent plugin. Additionally, when importing a scanned codebase into an inventory-only project, ensure that the import is configured to generate empty inventory (see Option to Process and Create Empty Inventory).

For more information about import types and project types, see Comparison of Standard and Inventory-Only Imports. For instructions on creating a standard or inventory-only project, refer to Creating a Project.

---

**Table 4-1 • Comparison of Standard and Inventory-Only Imports (cont.)**

<table>
<thead>
<tr>
<th>Import Behaviors and Usage</th>
<th>Standard Import</th>
<th>Inventory-only Import</th>
</tr>
</thead>
</table>
| Usage                      | Produces a full project copy that can be used for the following (for ongoing scanning and analysis):  
  - Full project backups.  
  - Application of analysis work from one product version to another (for branching or versioning purposes). | Provides a means to create inventory from the following:  
  - An external system.  
  - A Code Insight inventory-only project that is configured to scan remotely using a Jenkins or other scan agent plugin. |

* The import does not process custom components. Instead, to represent inventory with custom components, FlexNet Code Insight creates target inventory of either the work-in-progress (WIP) type or the license-only type.

---

**Note** • Running an import on a project currently being scanned is not recommended.

- A valid .zip archive containing the JSON data file with the project data to be imported.
- A completed Electronic Update.
- Items listed in Prerequisites When Using the REST Interface (if performing the import using REST API).
Import Behavior and Configuration

The following sections provide information you should know about the default import behavior and ways to configure this behavior.

- Default File and Inventory Processing During an Import
- Available Import Options to Configure Import Behavior
- Other Import Considerations

Default File and Inventory Processing During an Import

The following information describes the default behavior for processing files and inventory during an import. (You can modify this default behavior as needed by reconfiguring options, as described in the next section, Available Import Options to Configure Import Behavior.)

During an import, the file path (and optionally the MD5) is the key for matching data in the data file with the codebase files for the target project. File paths are matched between the data file to be imported and target codebase files by subtracting the root path from the absolute path, as demonstrated in this example:

- **Absolute file path** — `/home/fnci/scanRoot/1/ePortal-1.3/src/gettext.c`
- **Root path** — `/home/fnci/scanRoot/1/`
- **File path** — `/ePortal-1.3/src/gettext.c`

The following default logic applies during the import process:

- Only those codebase files that have file paths that match in both the data file to be imported and the scanned target codebase based are processed for inventory-to-file association in the target project. See Option to Require MD5 Checks When Associating Files to Target Inventory for more information.
- Only those codebase files that have file paths and MD5s that match in both the data file to be imported and the scanned target codebase are processed when marking files as reviewed in the target project. See Option to Require MD5 Checks When Marking Target Codebase Files as Reviewed for more information. (The import REST interface applies this default logic; the Web UI might apply different default logic.)
- Only those inventory items whose associated files have file paths that match in both the data file to be imported and the scanned target codebase are processed into the target project. See Option to Process and Create Empty Inventory for more information. (The import REST interface applies this default logic; the Web UI might apply different default logic.)
- Note content in identical source and target inventory items is resolved during the import by overwriting all notes in the target inventory item with content from the source target inventory. See Option for Overwriting or Appending Inventory Notes for more information.

The default import logic is configurable, as described in the next section.

Available Import Options to Configure Import Behavior

The following options can be specified to override the default import behavior described in the previous section.

- Option to Require MD5 Checks When Associating Files to Target Inventory
Chapter 4  Exporting and Importing Project Data

Importing Project Data

• Option to Require MD5 Checks When Marking Target Codebase Files as Reviewed
• Option for Overwriting or Appending Inventory Notes
• Option to Process and Create Empty Inventory

Much of this information directly applies to the procedures on how to execute an import using the Web UI or the REST interface described later in this chapter. However, because the configuration of import behavior is a thoughtful process and certain configurations must be performed before initiating an import, the configuration options are described here.

Option to Require MD5 Checks When Associating Files to Target Inventory

The import Web UI and REST interface provide an option to specify whether the file MD5 value, in addition to the file path, should be used as a criterion when associating files to inventory in the target project during the import process. When this option is disabled, only those files whose file paths match in both the import data file and the target project codebase are associated with inventory in the target project. For example, the file `/ePortal-1.3/src/gettext.c`, listed in the data file as belonging to “Inventory Item 1”, will be considered for association to this inventory item in the target project only if the scanned target project codebase contains the file `/ePortal-1.3/src/gettext.c` with the same file path.

When this option disabled, the criteria for adding files becomes more stringent since both the MD5 value and the file path must be considered. Only those files whose MD5 value and file path in the data file have a match in the target project codebase will be associated with inventory in the target project.

For more information about matching file paths, see Matching File Paths.

Option in the Web UI

This option is displayed as the Only add files to inventory with matching MD5 field on the Import Project dialog, used to start the import process. For complete import instructions, see Importing Project Data Using the Web UI.

• The unchecked field disables the MD5 checks so that only the file-path checks are used for associating files with target inventory.
• The checked field enables the MD5 checks along with the file-path checks for file associations.

By default, this field in unchecked in the Web UI.

Option in the REST Interface

The option is available as the checkInventory parameter for the importProjectData API. For complete instructions on using this API, see Importing Project Data Using the REST API.

• If the checkInventory parameter is not explicitly included in the API syntax, its value defaults to false, meaning that the MD5-match requirement is disabled. With this configuration, only a matching file path is used as the criterion for associating files with target inventory.
• To enable the use of MD5 checks along with file-path checks when associating files with inventory in the target project, explicitly include the checkInventory=true parameter as shown:

```bash
curl -X POST --data-binary "@PROJECT_DATA_FILE.zip" "HOST:PORT/codeinsight/api/importer/importProjectData?projectId=PROJECT_ID&checkInventory=true"
```
Option to Require MD5 Checks When Marking Target Codebase Files as Reviewed

The import Web UI and REST interface provide an option to specify whether the file MD5 value should be used as criteria (in addition to the file path) when marking codebase files as reviewed in the target project during the import process. When this option is enabled, files flagged as “reviewed” in the import data file are eligible for the “reviewed” flag in the scanned target project codebase only if their file path and MD5 value match in both the data file and the target project. For example, the file `/ePortal-1.3/src/gettext.c`, which is flagged as the “reviewed” in the data file, is eligible for the “reviewed” flag in the target project only if the target project codebase contains the file `/ePortal-1.3/src/gettext.c` with the same file path and MD5 value.

When this option is disabled, files flagged as “reviewed” in the import data file are eligible for the “reviewed” flag in the scanned target project codebase if their file paths match in both the data file and the target project. The MD5 value is not used as a criterion in this file-matching process.

For more information about matching file paths, see Matching File Paths.

Option in the Web UI

This option is displayed as the **Only mark files as reviewed with matching MD5** field on the **Import Project** dialog, used to start the import process. For complete import instructions, see **Importing Project Data Using the Web UI**.

- The unchecked field disables the MD5-match requirement for marking files as reviewed in the target project.
- The checked field enables the MD5-match requirement along with the file-path requirement for marking files in the target codebase as reviewed.

By default, this field in unchecked in the Web UI.

Option in the REST Interface

This option is available as the `checkReviewed` parameter for the **importProjectData** API. For complete instructions on using this API, see **Importing Project Data Using the REST API**.

- If you do not explicitly include the `checkReviewed` parameter in the API syntax, the parameter value defaults to `true`, meaning that the MD5-match requirement is enabled. A file in the target project is marked as reviewed only if its MD5 and file path match a reviewed file in the import data file.
- To disable the use the MD5-match requirement (so that only a matching file path is required) when marking files as reviewed in the target project, explicitly include the `checkReviewed=false` parameter as shown:

```
curl -X POST --data-binary "@PROJECT_DATA_FILE.zip" "HOST:PORT/codeinsight/api/importer/importProjectData?projectId=PROJECT_ID&checkReviewed=false"
```

Option for Overwriting or Appending Inventory Notes

Two inventory items are considered identical between the source and target project if they are associated with the same Code Insight data library item (based on the unique combination of component-version-license, or CVL). The import Web UI and REST interface enable you to specify whether notes for an inventory item in the target project should be overwritten with notes from an identical inventory item in the source project. Alternatively, the notes from the source inventory are appended to existing notes in the target inventory. This option applies to the following inventory notes:

- Notices Text
- Audit Notes
- Usage Guidance
Chapter 4  Exporting and Importing Project Data
Importing Project Data

• Remediation Notes

Options in the Web UI

The selection of one of these options on the Import Project dialog configures the handling of inventory notes during the import process. For complete import instructions, see Importing Project Data Using the Web UI.

• Overwrite existing notes with imported notes—Identical inventory is resolved during the import by overwriting all notes in the target inventory item with content from the import data file. However, empty data for a given field in the source target inventory will not overwrite existing content for that same field in the target inventory item (that is, the existing target content is retained). By default, this option is selected.

• Append imported notes to existing notes—Notes from the source inventory item are appended at the end of any existing notes in the identical target inventory item. For a given note field, the appended content is separated from the existing content with a line break and the following heading:

  Copied during import from <ProjectName>::<InventoryName> (TimeStamp)

  However, if note content for a given field is the same in both the source and the target inventory item, no content is appended in the field.

Option in the REST Interface

The option is available as the overwriteInventoryNotes parameter for the importProjectData API. For complete instructions on using this API, see Importing Project Data Using the REST API.

• If you do not explicitly include the overwriteInventoryNotes parameter in the API syntax, the parameter value defaults to true, meaning that all notes in the target inventory item are overwritten with content from its identical source inventory item. However, empty data for a given field in the source inventory will not overwrite existing content for that same field in the target inventory item (that is, the existing target content is retained).

• To append notes from the source inventory item to the end of the existing notes in the identical target inventory item, explicitly include the overwriteInventoryNotes=false parameter as shown:

  curl -X POST --data-binary "@PROJECT_DATA_FILE.zip" "HOST:PORT/codeinsight/api/importer/importProjectData?projectId=PROJECT_ID&overwriteInventoryNotes=false"

  For a given note field, the appended content is separated from the existing content with a line break and the following heading:

  Copied during import from <ProjectName>::<InventoryName> (TimeStamp)

  However, if note content for a given field is the same in both the source and the target inventory item, no content is appended in the field.

Option to Process and Create Empty Inventory

The import Web UI and REST interface provide an option to specify whether “empty” system-generated inventory items are still processed in the target project during the import. Empty inventory items either have no file associations in the data file to be imported or do have associated files in the data file but no matching file paths for these files in the scanned target codebase (also see Matching File Paths).

When this option is enabled, all inventory items—with or without matching associated files in the target codebase—are created in the target project during the import.

When the option is disabled, the import process does not create empty inventory items in the target project. It creates only inventory items with matching associated files in the target codebase.
**Note** • Inventory items without file associations are never imported by default. If you are importing from a scanned project into an inventory-only project, which has no codebase, ensure this option is enabled so that inventory is generated in the new project.

**Option in the Web UI**

The option is displayed as the project setting, **On the data import or rescan, delete inventory with no associated files**, located on the Edit Project: General Tab. Ensure that this field is properly set for the import you are about to perform. (You can always reset this value for the project once the import is complete.) See Editing the Project Definition and General Settings for details. The setting values include the following:

- The unchecked field enables the creation of empty inventory in the target project.
- The checked field disables the creation of empty inventory in the target project. Only inventory with matching associated files in the target codebase are created.

The default for this setting is defined at a global level by the administrator.

**Option in the REST interface**

The option is available as the createEmptyInventory parameter for the importProjectData API. For complete instructions on using this API, see Importing Project Data Using the REST API.

- If you do not explicitly include the createEmptyInventory parameter when invoking the importProjectData API, the import process uses the value of the deleteEmptyInventory setting defined for the project. (This setting is the same as the **On the data import or rescan, delete inventory with no associated files** value on the Edit Project: General Tab.) To override this project setting for the current import process only, explicitly include the createEmptyInventory parameter in the import command. See the next two bulleted items.

- To enable the creation of empty inventory items in the target project, include `createEmptyInventory=true`, as in the following example:

  ```
  curl -X POST --data-binary "@PROJECT_DATA_FILE.zip" "HOST:PORT/codeinsight/api/importer/importProjectData?projectId=PROJECT_ID&createEmptyInventory=true"
  ```

- To disable the creation of empty inventory items in the target project, include `createEmptyInventory=false` parameter in the import command.

**Other Import Considerations**

Consider the following additional behavior during import processing.

**Matching File Paths**

When the import process considers whether to add a file to inventory or mark it as reviewed, the absolute path of the file must match between the data file and the target project. For example, the file `/ePortal-1.3/src/gettext.c`—the only file belonging to “InventoryItem1” in the import data file—is considered to be a different file from `/ePortal-2.0/src/gettext.c` in the target project. As a result, `/ePortal-2.0/src/gettext.c` cannot be associated with “InventoryItem1”; and, if the createEmptyInventory value is false, “InventoryItem1” is not created in the target project since it has no associated file. Additionally, `/ePortal-2.0/src/gettext.c` will not be marked as reviewed in the target project.
In order for a file in the target project to be treated as identical to a file in the data file, the absolute paths for the two files must match in both locations. In the case above, you can ensure that the file paths match by uploading your code without the outer ePortal directory so that the absolute file paths are /src/gettext.c. Alternatively, you can manipulate the file paths in the data file to match those in the target project. For example, the file path ePortal-1.3/src/gettext.c in the data file would need to be changed to ePortal-2.0/src/gettext.c prior to performing the import. (All other file paths in the data file would need to be modified as well.)

Identical Inventory

Two inventory items are considered identical between the source and target project if they are associated with the same repository item (based on the unique combination of component-version-license, or CVL). By default, identical inventory is resolved during the import by overriding all fields in the target inventory item with information from the import data file, with the exception of empty data in the data file. However, you can configure the import to append notes from a source inventory item to existing notes in the identical target inventory item. See Option for Overwriting or Appending Inventory Notes for details.

Manually Unreviewed Files

A codebase file that is manually “unreviewed” in the source project does not retain its unreviewed status in the target project if the target codebase scan has marked the corresponding target file as “reviewed”. This occurs because the data file to be imported stores information about only those codebase files that have been marked as reviewed in the source project. Hence, no information about the unreviewed file exists in the import data to overwrite information for this same file in the target project.

If, during a standard import, you want to retain the reviewed and unreviewed status of codebase files as defined in the source project, manually mark all of the codebase files in the target project as unreviewed before importing the data file.

Importing Project Data Using the Web UI

Use the following instructions to import project data using the FlexNet Code Insight Web UI.

<table>
<thead>
<tr>
<th>Task</th>
<th>To import project data using the Code Insight Web UI, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Ensure that all requirements in Prerequisites for Importing Data are met.</td>
</tr>
<tr>
<td>2.</td>
<td>Log into Code Insight as the owner of the project you want to which you are importing data.</td>
</tr>
<tr>
<td>3.</td>
<td>Navigate to the Project Summary tab (see Opening the Project Summary Tab).</td>
</tr>
<tr>
<td>4.</td>
<td>Open the Manage Project dropdown and select Import Project Data.</td>
</tr>
<tr>
<td>5.</td>
<td>Click Browse next to the Choose File to Import field to search for and select the .zip file containing the JSON data file you are importing.</td>
</tr>
<tr>
<td>6.</td>
<td>Under Import Settings, select options to configure the import process. For details on these options, see the following:</td>
</tr>
<tr>
<td></td>
<td>• For Only add files to inventory with matching MD5, see Option to Require MD5 Checks When Associating Files to Target Inventory.</td>
</tr>
<tr>
<td></td>
<td>• For Only mark files as reviewed with matching MD5, see Option to Require MD5 Checks When Marking Target Codebase Files as Reviewed.</td>
</tr>
</tbody>
</table>
7. Click **OK** to perform the import.
   - If the import fails for some reason, as error dialog is displayed. Click **OK** and attempt the import again.
   - If the import completes successfully, a message dialog is displayed, stating as such. Click **OK**.

8. Verify that the import results are what you expected. See **Verifying the Import Results**.

## Importing Project Data Using the REST API

Use the following information to export project data by using a cURL command that calls the `importProjectData` REST API.

**Note** • If copying the cURL command directly from the following instructions for your own use, copy it to a text editor first to remove formatting and any line breaks or extra spaces.

<table>
<thead>
<tr>
<th>Task</th>
<th>To run an import, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Ensure that all prerequisites in Prerequisites for Importing Data and Prerequisites When Using the REST Interface are met.</td>
</tr>
<tr>
<td>2.</td>
<td>Set up a cURL command to invoke the <code>importProjectData</code> REST API using the POST method:</td>
</tr>
<tr>
<td></td>
<td>Create a cURL command based on the following syntax. Replace the highlighted variables with your server host ID (hostname or IP address) and port, the project ID, and the authorization token. Also, replace <code>PROJECT_DATA_FILE</code> with the name of .zip archive containing the JSON data file you are importing.</td>
</tr>
</tbody>
</table>
|      | ```
```
|      | The following is an example: |
|      | ```
```
|      | Include API parameters in the command as needed to override default import behavior. See Available Import Options to Configure Import Behavior for complete details and examples. |
| 3.   | Execute the command. |
|      | When the import is complete, a status message with **OK** will appear in the command prompt window. If the import is not successful, a status code and error message is displayed. |
| 4.   | Verify that the import results are what you expected. See **Verifying the Import Results**.
Verifying the Import Results

Use this procedure to verify that the import process completed as expected.

To verify that the import results are as expected, do the following:

1. Open the target project in FlexNet Code Insight and navigate to the **Project Inventory** page.
2. Confirm that the total number of inventory items includes the newly imported items. (Keep in mind that, by default, only inventory with matching associated files in the target codebase are imported.)
3. Confirm that the inventory items contain accurate inventory details and file path associations.
4. If the import results are not what you expect, adjust the import behavior (see **Import Behavior and Configuration**), and run the import again.
Automated Analysis

This chapter covers the following topics to describe the Automated Analysis of features in FlexNet Code Insight:

- What is Automated Analysis?
- Supported Development Ecosystems
- Supported Archive Formats
- Additional Rule-based Detection Capabilities

What is Automated Analysis?

FlexNet Code Insight provides Automated Analysis capability to automatically inventory various package formats without the need for manual analysis. New automated detection rules are delivered to FlexNet Code Insight as part of the Electronic Update process and through internal processes.

Automated Analysis is used in both scanning scenarios outlined below:

- Traditional scanning where the codebase is uploaded to the Scan Server or synchronized using a source code management system like Git or Perforce.
- Scan agent plugins that perform a scan remotely on an Engineering build server and send results back to FlexNet Code Insight.

Supported Development Ecosystems

FlexNet Code Insight provides native support for operating in many development ecosystems (each encompassing a language, package type, and public registry). See the following topics for more information:

- Supported Ecosystems
- Notes About Ecosystem Support
- Notes about Dependencies Support
## Supported Ecosystems

The table below provides the following information about each ecosystem that Code Insight supports in the Automated Analysis process:

- **Language/File Type**—The code language or file type supported by the ecosystem.
- **Package**—The name of a package type in the ecosystem.
- **Registry**—The URL for the public registry or repository that hosts the package type.
- **Manifest File**—The file for which the Code Insight scan searches to locate a package of this type.
- **Top-level Inv.**—The indicator ✓ for “yes” or a dash (—) for “no”, showing whether the Code Insight scan supports the detection of third-party software in the package (displayed as top-level inventory).
- **Direct Dep., Trans. Dep.**—If top-level inventory is supported, the discovery of this component’s direct (first-level) dependencies and transitive dependencies (that is, dependencies of dependencies).
- **Notes**—Link to specific information pertaining to Code Insight’s support of the ecosystem.

### Table 5-1 • Supported Ecosystems

<table>
<thead>
<tr>
<th>Language/File Type</th>
<th>Package</th>
<th>Registry</th>
<th>Manifest File</th>
<th>Top-level Inv.</th>
<th>Direct Dep.</th>
<th>Trans. Dep.</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>BitBake,</td>
<td>Yocto</td>
<td>N/A</td>
<td>.bb</td>
<td>✓</td>
<td>N/A</td>
<td>N/A</td>
<td>See Yocto Ecosystems.</td>
</tr>
<tr>
<td>BitBake recipe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DLL/EXE</td>
<td>PE Header</td>
<td>N/A</td>
<td>.dll, .exe</td>
<td>✓</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Go</td>
<td>glide</td>
<td><a href="https://go-search.org">https://go-search.org</a></td>
<td>glide.yaml</td>
<td>✓</td>
<td>—</td>
<td>—</td>
<td>See Go Ecosystems.</td>
</tr>
<tr>
<td></td>
<td>godep</td>
<td></td>
<td>godeps.json</td>
<td>✓</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td></td>
<td>govendor</td>
<td></td>
<td>vendor.json</td>
<td>✓</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td></td>
<td>module</td>
<td></td>
<td>go.mod</td>
<td>✓</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Java</td>
<td>Gradle</td>
<td><a href="http://search.maven.org">http://search.maven.org</a></td>
<td>build.gradle</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Maven</td>
<td></td>
<td>pom.xml</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>—</td>
</tr>
<tr>
<td>JavaScript</td>
<td>Bower</td>
<td><a href="https://registry.bower.io/packages/">https://registry.bower.io/packages/</a></td>
<td>bower.json</td>
<td>✓</td>
<td>✓</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>.bower.json</td>
<td>✓</td>
<td>✓</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>package.json</td>
<td>✓</td>
<td>✓</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>.NET</td>
<td>NuGet</td>
<td><a href="https://api.nuget.org/v3-flatcontainer/">https://api.nuget.org/v3-flatcontainer/</a></td>
<td>.nupkg</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>.nuspec</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>—</td>
</tr>
</tbody>
</table>
Notes About Ecosystem Support

The following sections provide additional information (such as limitations, requirements, and clarifications) to consider for the various ecosystems supported in the Code Insight Automated Analysis process:

- Yocto Ecosystems
- Go Ecosystems
- NPM Ecosystems
- PyPI Ecosystems
- Ruby Ecosystems
- Git Ecosystems

**Table 5-1 • Supported Ecosystems (cont.)**

<table>
<thead>
<tr>
<th>Language/ File Type</th>
<th>Package</th>
<th>Registry</th>
<th>Manifest File</th>
<th>Top-level Inv.</th>
<th>Direct Dep.</th>
<th>Trans. Dep.</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>package-lock.json OR npm-shrinkwrap.json</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>PHP</td>
<td>Composer</td>
<td><a href="https://packagist.org/">https://packagist.org/</a></td>
<td>composer.json</td>
<td>✔️</td>
<td>✔️</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>composer.lock</td>
<td>✔️</td>
<td>✔️</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Python</td>
<td>PyPI</td>
<td><a href="https://pypi.org/">https://pypi.org/</a></td>
<td>.whl</td>
<td>✔️</td>
<td>-</td>
<td>-</td>
<td>See PyPI Ecosystems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PKG-INFO</td>
<td>✔️</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>RPM</td>
<td>RPM Header</td>
<td>N/A</td>
<td>.rpm</td>
<td>✔️</td>
<td>N/A</td>
<td>N/A</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Gemfile</td>
<td>✔️</td>
<td>✔️</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>.gemspec</td>
<td>✔️</td>
<td>✔️</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Swift, Obj-C</td>
<td>CocoaPods</td>
<td>N/A</td>
<td>Podfile.lock</td>
<td>✔️</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>.podspec</td>
<td>✔️</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Various</td>
<td>Git Repo</td>
<td><a href="https://github.com">https://github.com</a></td>
<td>config</td>
<td>✔️</td>
<td>-</td>
<td>-</td>
<td>See Git Ecosystems.</td>
</tr>
</tbody>
</table>
**Yocto Ecosystems**

Code Insight parses a .bb file only if it contains an SCR_URI property value that starts with `git://` or `https://`. If the SCR_URI property contains more than one URI, only the first supported URI is considered.

**Go Ecosystems**

Note the following for Go ecosystems:

- A golang project configured with a supported package manager must include a license file to enable Code Insight to discover it as top-level inventory.
- Currently, Code Insight supports the discovery of top-level inventory only in scans of pre-build Artifact source code.
- If the codebase is uploaded from the release section of the VCS repository, Code Insight must use the version in the name of the project’s parent folder as the version in the top-level inventory name. Any changes to the version in the parent folder name can result in the wrong version being reported in the inventory.

**NPM Ecosystems**

Note the following for NPM ecosystems:

- FlexNet Code Insight provides scan support for `package.json` alone or for `package.json` with either `package-lock.json` or `npm-shrinkwrap.json`.
- To scan `package-lock.json` or `npm-shrinkwrap.json`, it must co-exist with `package.json`. (The `package.json` file contains the component and dependency data. The `package-lock.json` or `npm-shrinkwrap.json` file is used to identify the exact dependency versions for components that Code Insight should pull from `package.json`.)
- If both `package-lock.json` or `npm-shrinkwrap.json` are present with `package.json`, Code Insight scans `npm-shrinkwrap` (along with `package.json`) and ignores `package-lock.json`.

**PyPI Ecosystems**

FlexNet Code Insight supports the discovery of top-level inventory for pre-build and post-build artifacts of a Python project. Pre-build artifacts include source packages, such as `.tar.gz`, `.zip`, and other such files. Post-build artifacts are binary packages such as `.whl` files.

**Ruby Ecosystems**

Note the following for Ruby ecosystems:

- For RubyGem projects, Code Insight shows all platform-related dependencies and those dependencies that are not part of a “test” or “dev” group as inventory. Any gems identified as “dev” or “test” are not considered for inventory.
- Only SemVer expressions in the `major.minor.patch` format are supported to resolve dependencies listed in the manifest file.

**Git Ecosystems**

FlexNet Code Insight scans configuration files inside `.git` folders encountered in a project codebase and uses identified information to create inventory items.
Notes about Dependencies Support

FlexNet Code Insight supports scanning for top-level inventory items, direct dependencies, and transitive dependencies. The scan profile, managed by the Code Insight administrator, is used to configure the desired depth of scan with respect to dependencies. See About Scan Profiles for information about scan profiles.

Note the following additional information about dependency scanning:

- Dependencies represent open-source packages that are referenced by the scanned codebase, but not necessarily present in the codebase.
- Dependency scanning is designed to be used when scanning pre-build artifacts, typically found in source-code bundles. Since this scenario relies on package-management configuration files, it is not 100% precise in the resolution of the declared dependencies. In many cases, dependencies will be resolved to the latest available version within the declared range. However, this version can differ from the actual package version pulled down as part of the build.
- Dependency scanning is not designed for scanning post-build artifacts when using the scan agent plugins to scan on the build servers as part of the build process. In such scenarios, all dependencies have already been resolved by the build system and are present in the scanned codebase.

Supported Archive Formats

The Automated Analysis process in FlexNet Code Insight uses 7-Zip to read archive files. Use the following link to view the archive formats supported by 7-Zip:

https://sevenzip.osdn.jp/chm/general/formats.htm

Additional Rule-based Detection Capabilities

Automated detection used in the Automated Analysis process can also generate findings based on other rule-based techniques that include the following:

- Search term analysis
- File name analysis
- CDN analysis
Performing Inventory-Only Scanning

This section discusses FlexNet Code Insight inventory-only scanning. The following topics are covered in this section:

- Inventory-Only Scan
- Creating a Project Without Uploading a Codebase
- FlexNet Code Insight Plugins

Inventory-Only Scan

FlexNet Code Insight has the ability to scan files on a remote system and manage the inventory items created from the remote server. This type of scan is referred to as an inventory-only scan. It allows you to integrate automatic package-level scanning into your build process using the scan agent plugins such as Jenkins. This integration includes automated package discovery and targeted components. For additional information about automated analysis, see Automated Analysis.

Note • FlexNet Code Insight does not generate email notifications for remote scan events.

Creating a Project Without Uploading a Codebase

Organizations may be reluctant to upload their codebase into FlexNet Code Insight. Instead, they want to keep their codebase in its existing development system due to security, consistency, or other concerns. To address this requirement, FlexNet Code Insight provides scan agents that can scan a codebase wherever it resides and send the results as inventory to the Code Insight server for review and remediation by users. This process requires an inventory-only project on Code Insight server for handling the returned results, but requires no codebase upload to Code Insight.

The following is the overall process for creating an inventory-only project and performing a scan on a remote codebase:

Phase 1—Create an inventory-only project in FlexNet Code Insight. See Creating a Project.
**Phase 2**—Create a valid JSON Web Token (JWT) for the user whose account will be used to connect to FlexNet Code Insight. For instructions on generating the JWT, see Managing Authorization Tokens in the “Using FlexNet Code Insight” chapter.

**Phase 3**—Install and configure the appropriate scan agent plugin. (For information how to install and configure the plugin, see the FlexNet Code Insight Plugins Guide.) As part of the configuration process, you will need to provide the name of the inventory-only project that you created, the URL of the FlexNet Code Insight core server, and the JWT.

When the plugin is invoked (for example, by a build in Jenkins) the remote codebase will be scanned, and identified inventory items will be created on the FlexNet Code Insight server. The resulting inventory can be managed in FlexNet Code Insight.

**Note** • In the case of an inventory-only project, the Analysis Workbench will not be available. However, all other inventory management functionality is supported.

**FlexNet Code Insight Plugins**

FlexNet Code Insight offers the following standard scan agent plugins:

**Table 6-1** • Overview of the Standard Plugins

<table>
<thead>
<tr>
<th>Build Environment</th>
<th>Code Insight Plugin</th>
<th>Performs automated scanning of...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IDEs</strong></td>
<td>Eclipse</td>
<td>An Eclipse workspace in the Eclipse IDE environment.</td>
</tr>
<tr>
<td></td>
<td>Visual Studio</td>
<td>A Visual Studio solution.</td>
</tr>
<tr>
<td><strong>CI Tools</strong></td>
<td>Azure DevOps</td>
<td>An Azure DevOps workspace as part of the build process.</td>
</tr>
<tr>
<td></td>
<td>Bamboo</td>
<td>A Bamboo workspace as part of the build process (on Local Agents only)</td>
</tr>
<tr>
<td></td>
<td>GitLab</td>
<td>GitLab projects as part of the build process.</td>
</tr>
<tr>
<td></td>
<td>Jenkins</td>
<td>A Jenkins workspace as part of the build process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A separate plugin is available (called the Scan Schedule Plugin) that enables you to simply schedule the scan of a codebase residing on the Code Insight Scan Server via the Jenkins scheduler.</td>
</tr>
<tr>
<td></td>
<td>TeamCity</td>
<td>TeamCity projects as part of the build process.</td>
</tr>
<tr>
<td><strong>Package Manager and Build Tools</strong></td>
<td>Ant</td>
<td>Apache Ant as part of the build process.</td>
</tr>
<tr>
<td></td>
<td>Gradle</td>
<td>Gradle projects as part of the build process.</td>
</tr>
<tr>
<td></td>
<td>Maven</td>
<td>Maven projects as part of the build process.</td>
</tr>
<tr>
<td><strong>Binary Repositories</strong></td>
<td>JFrog Artifactory</td>
<td>Artifactory repositories to identify non-compliant artifacts.</td>
</tr>
<tr>
<td><strong>Container Platforms</strong></td>
<td>Docker Images</td>
<td>Docker images on a Docker server.</td>
</tr>
</tbody>
</table>
Additionally, a generic scan agent plugin is available with Code Insight that enables you to scan arbitrary file systems of your choice. It also easily integrates with certain Engineering systems, such as TeamCity and GitLab, to perform scans as part of a build process or can serve as an example for developing your own scan agent plugin (as described in FlexNet Code Insight Plugins Guide).

**Requirement Considerations**

Refer to the *FlexNet Code Insight Plugins Guide* for a list of requirements for each scan agent plugin.
Configuring Source Code Management

FlexNet Code Insight provides a connector that allows you to use Source Code Management systems (SCM) as a source for codebase data. This section discusses the following topic:

- Managing Source Code Management (SCM) Instances
- Configuring a Git SCM Instance
- Configuring a Perforce SCM Instance
- Configuring a TFS SCM Instance

Managing Source Code Management (SCM) Instances

FlexNet Code Insight provides the ability to scan data obtained from synchronization with a remote data source. The following sections provide information on adding and managing SCM instances.

- Adding an SCM Instance to the Code Insight Project
- Testing an SCM Instance
- Synchronizing an SCM Instance
- Deleting an SCM Instance

Prerequisites

Before performing the procedures in this section, ensure that an SCM command-line client is properly installed on the FlexNet Code Insight Scan Server and that connectivity between the SCM client and the SCM server is properly configured. Refer to the “Integrating with Source Code Management” chapter in the FlexNet Code Insight Installation and Configuration Guide for details.

If Code Insight is running as a service, make sure that the user context under which the service runs has appropriate permissions to run the SCM client.
Adding an SCM Instance to the Code Insight Project

You can specify configuration information about your remote data source when you edit your Code Insight project.

**Task**

*To add an SCM instance, do the following, do the following:*

1. Navigate to the **Summary** tab for the project to which you are synchronizing codebase files.
2. Open the **Manage Project** menu and select **Edit Project**. The **Edit Project** page opens.
3. Select the **Version Control Settings** tab.
4. Select the desired connector (remote data source) from the **Application** dropdown menu.
5. Click **Add Instance**. The available fields for the selected application will appear on a new **Instance** tab. See the inline help for explanations of the fields on this tab.
6. After editing the fields for your specific instance, click **Save**. You should now test and synchronize the instance.

Testing an SCM Instance

If you add an instance or edit any of the fields associated with your SCM instance, you should test the connection to ensure the repository is responsive.

**Task**

*To test your connection, do the following:*

1. If you are not already on the **Version Control Settings** tab on the **Edit Project** page, navigate to it.
2. Select the **Instance** tab for the connection you want to test.
3. Click **Test Connection** to confirm that the repository is reachable. After a moment, FlexNet Code Insight displays a success message dialog if the connection is successful. If the connection is not successful, ensure that your entries on the **Instance** tab are correct and click **Test Connection** again.

Synchronizing an SCM Instance

After testing your SCM connection, you can synchronize the instance to get the codebase files from the selected repository.

**Task**

*To sync an SCM instance, do the following:*

1. If you are not already on the **Version Control Settings** tab on the **Edit Project** page, navigate to it.
2. Click **Sync Now** to synchronize files from the repository to the root directory of the Code Insight Scan Server associated with your project. The root directory contains directories identified by project IDs. Under each project ID directory, subdirectories with names such as `git.0` or `git.1` are generated, one for SCM instance created for your project. (The number of subdirectories under the directory for your project ID is equal to the number of instances created for your FlexNet Code Insight project.)
Note the following:

- If multiple instances have been added, clicking Sync Now will synchronize all instances. If the sync fails for one instance, the overall sync will fail as well.
- If the Scan Server assigned to the project to which you are synchronizing codebase files is disabled, the Sync Now button is also disabled. Consider reassigning the project to an enabled Scan Server. (If necessary, see your FlexNet Code Insight administrator for information about which servers are enabled).

Deleting an SCM Instance

This section shows you how to delete an SCM instance if it is no longer needed.

<table>
<thead>
<tr>
<th>Task</th>
<th>To delete an SCM instance, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>If you are not already on the Version Control Settings tab, navigate to it.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the Instance tab for the instance you want to delete.</td>
</tr>
<tr>
<td>3.</td>
<td>Click Delete Instance. The selected instance is deleted from the system.</td>
</tr>
</tbody>
</table>

Configuring a Git SCM Instance

Flexnet Code Insight provides an SCM connector that enables you to scan a codebase hosted on a Git server. To perform the scan, you must first configure a Git SCM instance for the Code Insight project. Refer to the following topics for more information:

- Adding a Git SCM Instance to the Code Insight Project
- Fields Used to Configure a Git SCM Instance

Adding a Git SCM Instance to the Code Insight Project

The following procedure describes how to add a Git SCM instance to the Code Insight project.

<table>
<thead>
<tr>
<th>Task</th>
<th>To configure a Git SCM instance, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Use the instructions in Adding an SCM Instance to the Code Insight Project to navigate to the Version Control Settings tab and add a Git SCM instance, selecting Git from the Application dropdown.</td>
</tr>
<tr>
<td>2.</td>
<td>See Fields Used to Configure a Git SCM Instance for a description of the settings used to define a Git SCM instance, or use the inline help provided for each setting on the tab.</td>
</tr>
<tr>
<td>3.</td>
<td>Once you save the Git SCM instance, test the Code Insight connection with Git SCM instance, as described in Testing an SCM Instance.</td>
</tr>
</tbody>
</table>
Fields Used to Configure a Git SCM Instance

The following settings are used to configure a Git SCM instance.

Table 7-1 • Setting Used to Configure a Git SCM Instance

<table>
<thead>
<tr>
<th>Git SCM Instance Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Git Repository URL       | Provide the repository URL in either format:  
|                          | • http(s)://<host.xz>/<path>/to/repo.git  
|                          | • <user>@<host>:<path>/repo.git  
|                          | The contents of the repository will be cloned to the following directory on the Scan Server, based on the specified branch, tag, or commit ID:  
|                          | <scanroot>/<projectID>/<instanceID> |
| Git Username             | Provide the user name for Authenticated access to the repository. |
|                          | Leave this field blank for “anonymous” or SSH access (the system automatically looks for an SSH keypair on the server). See the FlexNet Code Insight Installation and Configuration Guide for instructions on configuring Git over SSH. |
| Git Password             | Enter the password associated with the user name provided. |
| Git Branch, Git Tag, or Git Commit ID | Specify either the Git branch, tag, or commit ID to identify the source code version to which to synchronize.  
|                          | Alternatively, leave these fields blank to synchronize to the master branch. |

Configuring a Perforce SCM Instance

Flexnet Code Insight provides an SCM connector that enables you to scan a repository (codebase) hosted on a Perforce server. To perform the scan, you must first configure a Perforce SCM instance to identify this repository to the Code Insight project. Refer to the following topics for more information:

- Adding a Perforce SCM Instance to the Code Insight Project
- Fields Used to Configure a Perforce SCM Instance

Adding a Perforce SCM Instance to the Code Insight Project

The following procedure describes how to add a Perforce SCM instance to the Code Insight project.
Task

To configure a Perforce SCM instance, do the following:

1. Use the instructions in Adding an SCM Instance to the Code Insight Project to navigate to the Version Control Settings tab and add a Perforce SCM instance, selecting Perforce from the Application dropdown.

2. See Fields Used to Configure a Perforce SCM Instance for a description of the settings used to define a Perforce SCM instance, or use the inline help provided for each setting on the tab.

3. Once you save the Perforce SCM instance, test the Code Insight connection with Perforce SCM instance, as described in Testing an SCM Instance.

Fields Used to Configure a Perforce SCM Instance

The following settings are used to configure a Perforce SCM instance on FlexNet Code Insight.

Keep the following in mind as you set up the instance, especially when providing the Username and Password credentials:

- The repository identified by the instance must reside on a Perforce server that is configured with Security Level 1, 2, or 3. The FlexNet Code Insight Perforce connector does not support instances created for a Perforce server configured with Security Level 0, in which users are created without passwords.

- The Code Insight Perforce connector supports LDAP authentication on Perforce. If Perforce is configured with LDAP, you must provide the appropriate LDAP credentials for the Username and Password fields to access the Perforce repository identified by the instance.

Table 7-2 • Setting Used to Configure a Perforce SCM Instance

<table>
<thead>
<tr>
<th>Perforce SCM Instance Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL (P4PORT)</strong></td>
<td>Provide the URL of the Perforce instance with which to synchronize. Note the following example URL formats:</td>
</tr>
<tr>
<td></td>
<td><strong>For a TCP connection</strong></td>
</tr>
<tr>
<td></td>
<td>tcp:&lt;p4ServerHostID&gt;:&lt;p4Port&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>For an SSL connection</strong></td>
</tr>
<tr>
<td></td>
<td>ssl:&lt;p4ServerHostID&gt;:&lt;p4Port&gt;</td>
</tr>
<tr>
<td>p4ServerHostID and p4Port identify the hostID (hostname or IP address) and port of the Perforce server.</td>
<td></td>
</tr>
<tr>
<td><strong>Username (P4USER)</strong></td>
<td>Provide the user name that has access to the Perforce depot to which this instance is synchronizing. If Perforce is configured with LDAP authentication, provide the LDAP user name.</td>
</tr>
<tr>
<td><strong>Password (P4PASSWD)</strong></td>
<td>Provide the password associated with the user name (see the previous field). If Perforce is configured with LDAP authentication, provide the LDAP password associated with the LDAP user name.</td>
</tr>
<tr>
<td></td>
<td>If you are using a P4 ticket provided by the Perforce administrator, this field is optional.</td>
</tr>
</tbody>
</table>
Configuring a TFS SCM Instance

Flexnet Code Insight provides an SCM connector that enables you to scan a codebase hosted on a Team Foundation Server (TFS) instance. To perform the scan, you must first configure a TFS SCM instance for the Code Insight project. Refer to the following topics for more information:

- Adding a TFS SCM Instance to the Code Insight Project
- Fields Used to Configure a TFS SCM Instance

Adding a TFS SCM Instance to the Code Insight Project

The following procedure describes how to add a TFS SCM instance to the Code Insight project.

1. Use the instructions in Adding an SCM Instance to the Code Insight Project to navigate to the Version Control Settings tab and add a TFS SCM instance, selecting TFS from the Application dropdown.
2. See Fields Used to Configure a TFS SCM Instance for a description of the settings used to define a TFS SCM instance, or use the inline help provided for each setting on the tab.
3. Once you save the TFS SCM instance, test the Code Insight connection with the TFS SCM instance, as described in Testing an SCM Instance.

### Table 7-2 • Setting Used to Configure a Perforce SCM Instance

<table>
<thead>
<tr>
<th>Perforce SCM Instance Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch Spec (P4CLIENT)</td>
<td>Provide the path to the branch to which this instance is synchronizing.</td>
</tr>
<tr>
<td>Changelist No</td>
<td>(Optional) Provide a changelist number only if this instance is synchronizing to a particular changelist. Otherwise, this value defaults to the latest revision.</td>
</tr>
<tr>
<td>Label</td>
<td>(Optional) Provide a label for the perforce branch.</td>
</tr>
</tbody>
</table>
Fields Used to Configure a TFS SCM Instance

The following settings are used to configure a TFS SCM instance for the Code Insight project.

**Table 7-3 • Settings Used to Configure a TFS SCM Instance**

<table>
<thead>
<tr>
<th>Perforce SCM Instance Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **TFS URL**                   | Provide the URL of the TFS with which to synchronize. Note the following example URL formats.  
For the latest version of TFS:  
<protocol>:<tfs_host>:<port>/<collection>/<project>  
For earlier versions of TFS:  
<protocol>:<tfs_host>:<port>/<collection>/<tfsroot>/<project> |
| **Username**                  | Provide the user name that has access to the TFS collection to which this instance is synchronizing.  
If you are synchronizing with a VSTS project in TFS, enter the user name from the alternate authentication credentials enabled in VSTS. For details about enabling alternate credentials, refer to “Special Requirement for a VSTS Project in TFS” in the “Integrating with Source Code Management” chapter in the *FlexNet Code Insight Installation and Configuration Guide*. |
| **Password**                  | Provide the password associated with the user name provided.  
If you are synchronizing with a VSTS project in TFS, enter the password from the alternate authentication credentials enabled in VSTS. |
| **Changeset**                 | (Optional) Provide a changeset number to which the TFS SCM instance is synchronizing. Otherwise, this value defaults to the latest revision.  
If a changeset and label are both specified (see the **Label** description next), the label is ignored, and the instance synchronizes to the changeset instead. |
| **Label**                     | (Optional) Provide a specific label to which the TFS SCM instance is synchronizing.  
If a label and changeset (see the previous **Changeset** description) are both specified, the label is ignored, and the instance synchronizes to the changeset instead. |
Pages and Panels

Reference information for the following pages and panels in FlexNet Code Insight appears in this section:

- The FlexNet Code Insight Dashboard
- Users/Permissions Tab
- Add User Dialog
- Edit User Dialog
- Electronic Updates Tab
- Email Server Tab
- LDAP Tab
- ALM Tab
- Scan Servers Tab
- Scan Server Dialog
- Scan Profiles Tab
- Create/Edit Scan Profile Dialog
- Project Defaults Tab
- Projects List Page
- Project Summary Tab
- Edit Project: General Tab
- Edit Project: Scan Settings Tab
- Edit Project: Review and Remediation Settings Tab
- Edit (Default) Project Users Page
- Scan History Dialog
The FlexNet Code Insight Dashboard

The Dashboard is displayed when you access FlexNet Code Insight. The Dashboard contains the following options:

**Table 8-1 • FlexNet Code Insight Dashboard**

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>analyzed</td>
<td>Displays the number of lines of code that have been analyzed since FlexNet Code Insight was installed.</td>
</tr>
<tr>
<td>scanned</td>
<td>Displays the number of lines of code that have been scanned since FlexNet Code Insight was installed.</td>
</tr>
</tbody>
</table>
Note • If this is the first time FlexNet Code Insight has been accessed or if no codebase has been analyzed, the analyzed, scanned, and identified fields will be empty.

See Also
Projects List Page
Policy Page
Users/Permissions Tab
Electronic Updates Tab
Email Server Tab
LDAP Tab
ALM Tab
Scan Servers Tab
Scan Profiles Tab

Users/Permissions Tab

The Users/Permissions tab on the Administration page allows you to add and edit users who can work in FlexNet Code Insight. The tab contains the following columns and fields:

Table 8-2 • Users tab

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add User</td>
<td>Click to display the Add User dialog.</td>
</tr>
<tr>
<td>Manage Permissions</td>
<td>Click to display the Manage Permissions dialog used to assign the following permissions to users: Administrator, Manage Policy, and Create Projects.</td>
</tr>
<tr>
<td>Login</td>
<td>Displays the login of each user that has been added.</td>
</tr>
<tr>
<td>First Name</td>
<td>Displays the first name of each defined user.</td>
</tr>
<tr>
<td>Last Name</td>
<td>Displays the last name of each defined user.</td>
</tr>
<tr>
<td>Email</td>
<td>Displays the email address of the user associated with the login.</td>
</tr>
</tbody>
</table>
Add User Dialog

The Add User dialog on the Administration page allows you to add new users to the FlexNet Code Insight system. The dialog contains the following columns and fields:

Table 8-3 • Add User dialog

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Enter the login of the new user.</td>
</tr>
<tr>
<td>First Name</td>
<td>Enter the first name of new user.</td>
</tr>
<tr>
<td>Last Name</td>
<td>Enter the last name of new user.</td>
</tr>
<tr>
<td>Email</td>
<td>Displays the email address of the user associated with the login. To change the user's email address, type over the existing email address.</td>
</tr>
<tr>
<td>Password</td>
<td>The current password is not displayed in this field. A user with Administrator permission can type a new password in this field.</td>
</tr>
<tr>
<td>Password Confirm</td>
<td>The current password is not displayed in this field. A user with Administrator permission can type a new password in this field.</td>
</tr>
<tr>
<td>Question</td>
<td>The prompt that the user must answer to retrieve a forgotten password.</td>
</tr>
<tr>
<td>Answer</td>
<td>The answer to the question in the previous field.</td>
</tr>
<tr>
<td>Submit</td>
<td>Select Submit to have the system save your user edits. A prompt appears to notify you that your edits have been saved.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Select Cancel to return to the Administration Users tab without saving your changes.</td>
</tr>
</tbody>
</table>
Edit User Dialog

The Edit Users dialog is where you can edit users who are already in the FlexNet Code Insight system. The dialog contains the following columns and fields:

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Displays the login of the selected user. This field is read-only and cannot be changed.</td>
</tr>
<tr>
<td>First Name</td>
<td>Displays the first name of the selected user. To change the user’s first name, type over the existing name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>Displays the last name of the selected user. To change the user’s last name, type over the existing name.</td>
</tr>
<tr>
<td>Email</td>
<td>Displays the email address of the user associated with the login. To change the user’s email address, type over the existing email address.</td>
</tr>
<tr>
<td>Password</td>
<td>The current password is not displayed in this field. A user with Administrator permission can type a new password in this field.</td>
</tr>
<tr>
<td>Password Confirm</td>
<td>The current password is not displayed in this field. A user with Administrator permission can type a new password in this field.</td>
</tr>
<tr>
<td>Question</td>
<td>The prompt that the user must answer to retrieve a forgotten password.</td>
</tr>
<tr>
<td>Answer</td>
<td>The answer to the question in the previous field.</td>
</tr>
<tr>
<td>Submit</td>
<td>Select Submit to have the system save your user edits. A prompt appears to notify you that your edits have been saved.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Select Cancel to return to the Administration Users tab without saving your changes.</td>
</tr>
</tbody>
</table>

See Also
Users/Permissions Tab
Electronic Updates Tab

An initial full Electronic Update is run automatically after your initial startup of FlexNet Code Insight. It provides the basis of a local data library used by FlexNet Code Insight to identify OSS and third-party code in your codebase. The **Electronic Updates** tab on the **Administration** page enables you to configure how and when subsequent Electronic Updates are run to keep this library up to date. Refer to the following topics for more information:

- **Overview of Electronic Update Setup**
- **Field Descriptions**

For detailed instructions on how to schedule and run Electronic Updates, see “Configuring FlexNet Code Insight” in the *FlexNet Code Insight Installation & Configuration Guide*.

### Overview of Electronic Update Setup

The following describes the basics for configuring electronic updates:

- **Specifying an Update as Server or Local**
- **Scheduling Electronic Updates**

#### Specifying an Update as Server or Local

The **Electronic Update Type** field (see **Field Descriptions** below) on the **Electronics Update** tab enables you to configure the Electronic Update to run as either a server or local update. The difference between the two methods is the means by which the FlexNet Code Insight server obtains the files required to run the update:

- During a **server** Electronic Update, the most recent Electronic Update files are automatically downloaded from Flexera to the FlexNet Code Insight server prior to processing the update.

- For a **local** Electronic Update, you must manually download the Electronic Update files from Flexera to a location that is locally accessible to the Code Insight server, such as a shared drive or a local USB drive. Then, when an update is triggered, the Code Insight server automatically uploads the files and proceeds with the update. This type of Electronic Update is useful when the Code Insight server has no external Internet access or when a specific Electronic Update version is needed for testing or demo purposes.

#### Scheduling Electronic Updates

The remaining fields (see **Field Descriptions** below) on the **Electronic Updates** tab allow you either to schedule an Electronic Update to run automatically at regular intervals or to manually request an update as needed. By default, an update is **incremental** (that is, the update applies on changes from the previous update). However, you have the option force a **full** Electronic Update, which replaces all data from the previous update. (A full update might be necessary, for example, if the most recent update did not complete properly.)

In summary, you can schedule the following:

- An incremental Electronic Update (server type only) that runs automatically at a regular frequency that you define.

- An incremental Electronic Update (server or local type) that you manually run as needed.

- A full Electronic Update (server or local type) that you manually run when necessary. Use this option with caution as forcing a full update to run will take several hours to complete, similar to the initial update run when FlexNet Code Insight was first installed.
Note • Codebase scans cannot be performed during the Electronic Update process, but a scan that is already underway will not be interrupted when an update is scheduled to begin. The Electronic Update will be queued and automatically run based on queue order.

Field Descriptions

The tab contains the following columns and fields:

Table 8-5 • Electronic Updates tab

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>The initial step in running an Electronic Update is to determine whether you are running it as a local or server update. For more information about these two types of updates, see Specifying an Update as Server or Local.</td>
</tr>
<tr>
<td>Electronic Update Type</td>
<td>Select the type of Electronic Update to run based how the FlexNet Code Insight server obtains the Update Manifest and Update Data files required to perform the update:</td>
</tr>
<tr>
<td></td>
<td>- Local—As part of the Electronic Update process, the Code Insight server uploads each of these files from a locally accessible location (to which you have manually downloaded the appropriate files from Flexera prior to the update). Use the Update Manifest File and Update Data File fields to identify the locations from which Code Insight server will upload the files.</td>
</tr>
<tr>
<td></td>
<td>- Server—The most recent Electronic Update files are automatically downloaded from Flexera to the Code Insight server as part of the Electronic Update process.</td>
</tr>
</tbody>
</table>
If you intend to run a local Electronic Update, you must specify the location of the two required “update” files that you manually downloaded from Flexera. The location of each file must be locally accessible. To run the update, use the Run Update Now option.

Update Manifest File
Click Select File to search for and select the Update Manifest file (update_manifest.txt) to upload to the Code Insight server. The manifest file contains the following:

- Information that Code Insight uses to determine whether to perform the update.
- The expected hash value for each data file stored in the update.zip file (see the Update Data File field description). This information will be compared with the hash values of actual files in the archive to ensure that the files have not changed or been tampered with.

Update Data File
Click Select File to search for and select the data archive (update.zip) file to upload to the Code Insight server. This archive contains data files that provide the CVSS information used by Code Insight to perform update.

Code Insight uses the hash information in the manifest file (see the Update Manifest File field description) to ensure that the data files are the expected ones and have not changed or been tampered with.

Configuration for automatic Electronic Updates (server update only)
FlexNet Code Insight enables you to configure server incremental updates to run automatically at a frequency you define, as described below.

Note that you can always manually force an incremental or full update between the scheduled updates, or you can disable scheduled automatic updates altogether and manually run updates as needed. In either case, you would need to use the Run Update Now option to run an Electronic Update.

Update Frequency
Select from one of the available frequencies for running an incremental Electronic Update automatically:

- **Never**—If you select Never, Electronic Updates will not be run automatically. (Selection of this option hides any further dropdowns.) You can always manually schedule an incremental or full update as needed using the Run Update Now option.
- **Daily**—If you select Daily, a second dropdown is displayed to choose the time of day when you want the Electronic Update to occur.
- **Weekly**—If you select Weekly, both the “time of day” dropdown and the Select a day... dropdown are displayed. Select both the time of day and the day of the week when you want the Electronic Update to occur.

Save Schedule
Click this button to save the schedule. Your future incremental updates will run automatically according to the frequency you defined.
Email Server Tab

The Email Server tab on the Administration page allows you to enable email notifications and set email options. The tab contains the following columns and fields:

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Email Server</td>
<td>Select Yes to enable FlexNet Code Insight to use the email server or No to leave it disabled. The default is No. The rest of the fields on this page are not available until you select Yes.</td>
</tr>
<tr>
<td>Sender's Email Address</td>
<td>Enter the email address of the sender.</td>
</tr>
<tr>
<td>SMTP Host Name</td>
<td>Enter the Simple Mail Transfer Protocol (SMTP) host name.</td>
</tr>
<tr>
<td>SMTP Host Port</td>
<td>Enter the port number of the SMTP host.</td>
</tr>
<tr>
<td>SMTP User Name</td>
<td>Enter the SMTP user name. This field is optional. Leave it blank if you are using anonymous SMTP.</td>
</tr>
</tbody>
</table>
LDAP Tab

FlexNet Code Insight supports user authentication and authorization through LDAP (Lightweight Directory Access Protocol). The LDAP tab on the Administration page configures the synchronization of user identification data from LDAP to FlexNet Code Insight, thus enabling LDAP user authentication for Code Insight. For detailed information about the fields on this tab and about the configuration in general, see “Configuring Code Insight for LDAP” in the FlexNet Code Installation and Configuration Guide.

The tab contains the following columns and fields:

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP User Password</td>
<td>Enter the SMTP user password. This field is optional. Leave it blank if you are using anonymous SMTP.</td>
</tr>
<tr>
<td>Enable SMTP over TLS</td>
<td>Select Yes to use Transport Layer Security (TLS) to secure email over SMTP or select No to leave this option disabled.</td>
</tr>
</tbody>
</table>

Table 8-7 • LDAP tab

<table>
<thead>
<tr>
<th>Section</th>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[LDAP enablement]</td>
<td>Enable LDAP</td>
<td>This option enables the use of LDAP for your FlexNet Code Insight system. When LDAP is enabled, the settings used to configure Code Insight for LDAP are made available for editing on this tab. You can use this option to turn off LDAP whenever necessary.</td>
</tr>
</tbody>
</table>

Select Yes or No to determine if LDAP will be used for user authentication. The default is No.
These settings configure the FlexNet Code Insight connection to the LDAP server. This connection is required for each synchronization process of LDAP user information to Code Insight and for authentication each time a user logs into Code Insight.

**LDAP URL**

Specify the URL of the LDAP server in the following format:

`ldap://<ldap_server_host>:<ldap_port>`

where `<ldap_server_host>` is either the hostname or IP address of the LDAP server; and `<ldap_port>` is the port on which the server listens for requests. The following is an example URL, which uses the standard LDAP server port 389:

`ldap://acme.com:389`

If using SSL to provide data encryption security for user information passed over the network, specify the `ldaps://` protocol with the port 636, which is the default dedicated port for SSL:

`ldaps://acme.com:636`

**Authentication Type**

Select the type of LDAP authentication used to establish a connection with the LDAP server:

- **Anonymous**—FlexNet Code Insight will establish a connection with the LDAP server without the use of user credentials. (When this option is selected, the LDAP Username and LDAP Password fields in this section are disabled.) This authentication type is generally used for testing purposes.

- **Authenticated**—Code Insight requires the user credentials provided in the LDAP Username and LDAP Password fields to authenticate and establish a connection with the LDAP server.

**LDAP Username**

Depending on your LDAP setup, enter either of the following to identify the user used connect to the LDAP server:

- The user's login ID, such as `mburns`
- The user's Distinguished Name (DN), such as:

  `CN=Monty Burns,OU=usa,DC=acme,DC=com`

  For more information about providing the DN, see “Distinguished Name for an Object” in the FlexNet Code Installation and Configuration Guide.

This identification, along with the associated password (see the next field), is used to authenticate the connection to the LDAP server. Note that the user must have READ permissions to query the LDAP server (and therefore does not need to be an administrator).

This field is disabled if Anonymous is selected for Authentication Type.
### LDAP Tab

#### LDAP Query Details

The following fields define the query that identifies the subset of users on the LDAP server to be synchronized to FlexNet Code Insight. This query is used for the initial synchronization process and for each subsequent synchronization performed per the **LDAP User Sync Frequency** value.

<table>
<thead>
<tr>
<th>Section</th>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Base</td>
<td></td>
<td>Specify the Distinguished Name (DN) of the LDAP base domain in the Directory Information Tree (DIT) on your LDAP server. This domain is the top-level directory to which all other objects in the directory structure belong; it typically represents your organization. The base domain is identified by domain controller objects (DCs), which make up its DN. For example, the base domain in the example DIT in Figure 2-1 is the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DC=acme,DC=com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In some cases, a sub-domain can be a part of the base domain:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DC=software,DC=acme,DC=com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information, see “LDAP Base” in the <em>FlexNet Code Installation and Configuration Guide</em>.</td>
</tr>
<tr>
<td>LDAP Search Base</td>
<td></td>
<td>Specify the DIT directory, relative to the LDAP base directory, under which you store all Code Insight objects on the LDAP server and from which you search for Code Insight users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In reference to the example DIT in Figure 2-1, if you enter <strong>OU=usa</strong> for the search base, all searches for user information will be performed below the directory “usa”. (LDAP internally identifies the DN for this directory as the <strong>LDAP Base + LDAP Search Base</strong> value.) For more information, see “Setting Up a User Search” in the <em>FlexNet Code Installation and Configuration Guide</em>.</td>
</tr>
<tr>
<td>LDAP Search Query</td>
<td></td>
<td>Specify the search query used to retrieve the users from <strong>LDAP Search Base</strong> directory to synchronize to Code Insight. Each attribute in a query is listed in parenthesis in the format <strong>(attribute=value)</strong>, such as in the following, which searches for only those users belonging to the “engineering” group under the “usa” node:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&amp;(&lt;objectClass=person)(memberOf=CN=engg,OU=usa,DC=acme,DC=com))</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For other search query examples, see “Setting Up a User Search” in the <em>FlexNet Code Installation and Configuration Guide</em>.</td>
</tr>
</tbody>
</table>
Table 8-7 • LDAP tab (cont.)

<table>
<thead>
<tr>
<th>Section</th>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Paging</td>
<td></td>
<td>Select Yes if the LDAP server has paging enabled for synchronization results. If you select Yes, the LDAP Page Size field is enabled, enabling you to customize the page size. Select No if the server does not have paging enabled. If you select No, the server sends 1000 elements per page by default unless this behavior is changed at the organization level on the LDAP server.</td>
</tr>
<tr>
<td>LDAP Page Size</td>
<td></td>
<td>Indicate the page size you want for the synchronization results. The default page size is 1000 elements.</td>
</tr>
<tr>
<td>LDAP User Sync Frequency</td>
<td></td>
<td>Specify the frequency at which FlexNet Code Insight will synchronize user data with the LDAP server:</td>
</tr>
<tr>
<td></td>
<td>Never</td>
<td>Select this option to disable the automatic user synchronization. A synchronization occurs only if the user clicks the Sync Now button. For all other values, automatic user synchronization is enabled per the configured frequency. (This is the default value.)</td>
</tr>
<tr>
<td></td>
<td>Hourly</td>
<td>Enter an integer value representing the number of hours between user synchronizations.</td>
</tr>
<tr>
<td></td>
<td>Daily</td>
<td>Select a time at which the user synchronization will run every day.</td>
</tr>
<tr>
<td></td>
<td>Weekly</td>
<td>Select a day of the week and a time of the day when the user synchronization will run each week.</td>
</tr>
<tr>
<td>Search Sub-tree</td>
<td></td>
<td>Select this checkbox to enable deep searches through the subtree of the path defined by LDAP Base + LDAP Search Base. Note that, while helpful in locating users in certain cases, a deep search can negatively affect performance (and therefore, by default, is not enabled). For more information, see “Setting Up a User Search” in the FlexNet Code Installation and Configuration Guide.</td>
</tr>
</tbody>
</table>
The ALM tab on the Administration page allows you to configure Jira and other ALM (Application Lifecycle Management) instances for integration with Code Insight for the purpose of creating work items in external workflow systems. The tab contains the following columns and fields:

Table 8-8 • ALM tab

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Name of the ALM application for which to add an instance.</td>
</tr>
<tr>
<td>Add Instance</td>
<td>Click to open a new Instance tab to configure an instance to point to a server in the ALM system.</td>
</tr>
</tbody>
</table>
Table 8-8 • ALM tab (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Existing Issues Sync Frequency | Click the ♦️ to the right of this field, and select the synchronization frequency that will apply to all the configured ALM instances. (The default value is Hourly repeated every 1 hour.)  
  • Never  
  • Hourly (enter number of hours)  
  • Daily (enter time of day)  
  • Weekly (enter day of the week and time of day)  
  Click ✔️ to accept the updated synchronization frequency or ✖️ to restore the previous frequency. |
| Test Connection               | Click to validate that Code Insight can connect to the current instance based on the supplied **ALM_type Instance Name**, **ALM_type Server URL**, **ALM_type Username**, and **ALM_type Password**. |
| Delete Instance               | Click to delete the current ALM instance after verifying that no project references to this instance exist.                                      |
| **ALM_type Instance Name**    | Unique name of the ALM instance.                                                                                                             |
| **ALM_type Server URL**       | URL of the ALM server to which to connect in the format http(s):<server_name_or_ip>.                                                          |
| **ALM_type Username**         | Credentials of ALM instance user for authentication on the ALM server. This user is also the designated reporter on work items (issues) created for the instance. |
| **ALM_type Password**         |                                                                                                                                               |
| Default Project Key           | Key for the project for which issues will be created on the ALM server.                                                                       |
| Default Issue Type            | The default issue type created on the ALM server.                                                                                            |
| Default Priority              | Default priority of the issued created on the ALM server.                                                                                      |
| Default Assignee              | The default user to whom to assign work items created for this instance.                                                                     |
| Default Summary Text          | Default text to display as a summary for the issue on the ALM server. The text supports the following Code Insight variables: $PROJECT_NAME, $INVENTORY_ITEM_NAME, $COMPONENT_NAME, $VERSION_NAME, $LICENSE_NAME, $NUMBER_VULNERABILITIES, $NUMBER_FILES, or $INVENTORY_URL. |
| Default Description Text      | Default text to display as a description for the issue on the ALM server. The text supports the following Code Insight variables: $PROJECT_NAME, $INVENTORY_ITEM_NAME, $COMPONENT_NAME, $VERSION_NAME, $LICENSE_NAME, $NUMBER_VULNERABILITIES, $NUMBER_FILES, or $INVENTORY_URL. |
Scan Servers Tab

The Scan Servers tab on the Administration page lists the Scan Servers that you have identified to your FlexNet Code Insight system. Each entry in the list shows basic information about the given Scan Server including its status. From a given entry, you can access a separate dialog to edit server properties as well as refresh the entry itself to see the latest server status. The tab also lets you define a new Scan Server. The tab contains the following columns and buttons to identify and manage Scan Servers:

Table 8-9 • Scan Servers tab

<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Scan Server entry]</td>
<td>The following columns for each entry in the Scan Server list provide information about the given Scan Server, as well as a means to refresh the Scan Server status and edit server properties.</td>
</tr>
<tr>
<td>Alias</td>
<td>The user-defined name for the Scan Server, as well as the server’s current status. The following icons represent the server status:</td>
</tr>
<tr>
<td></td>
<td>The green icon indicates that the Scan Server is “enabled” for scanning and is currently running (turned on). Scans are run in queue order.</td>
</tr>
<tr>
<td></td>
<td>The red icon indicates that the Scan Server is “enabled” for scanning but is currently not running (that is, it is turned off). Any attempts to associate a project with the Scan Server or upload a codebase to the server generates an error. Additionally, any attempt to initiate a scan will result in the scan’s being queued. However, once the server is active, the scan will start based on queue order. (Users can click the Past Scans link on the project Summary page to view details about the scheduled scan.)</td>
</tr>
<tr>
<td></td>
<td>The gray icon indicates that the Scan Server is “disabled” (that is, cannot be used for scanning). Whether or not the server is running has no effect on this status. If an enabled server is needed for scans on a project assigned to a disabled Scan Server, you must create a new project.</td>
</tr>
<tr>
<td>Host</td>
<td>The localhost value is used if the Scan Server is on the same instance as the Core Server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port used by the Scan Server on the host instance. By default, the port is 8888.</td>
</tr>
</tbody>
</table>
Before a user can assign project codebases to a Scan Server in order to scan them, the Scan Server must first be installed either on the same instance as the Code Insight Core Server or on a separate instance, as described in the FlexNet Code Insight Installation and Configuration Guide. (The Scan Server must have the same version as the Core Server.) As administrator, you must then use the Scan Server dialog to “add”—that is, identify—the server to the FlexNet Code Insight system to make it available for scanning purposes.

In addition to adding a new Scan Server, you use the Scan Server dialog to edit an existing Scan Server’s properties. For detailed instructions on adding or editing a Scan Server, see “Adding or Editing Scan Servers” in the FlexNet Code Insight Installation and Configuration Guide.

Table 8-9 • Scan Servers tab (cont.)

<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>CL Path</td>
<td>The path for the FlexNet Code Insight Compliance Library (CL). If the path is specified, the CL is accessed as part of the scan to perform exact-file and source-code fingerprint (snippet) matching. Elements of scanned codebase files are compared with information contained in the CL to generate file-level evidence on which you can take action. If the path is not specified, the codebase is scanned without using the CL. This type of scan generates inventory from Code Insight’s Automated Analysis feature but has limitations. For more information about the Compliance Library, see What Is a FlexNet Code Insight Scan?.</td>
</tr>
<tr>
<td>Codebase Path</td>
<td>The path on the Scan Server where FlexNet Code Insight will store and manage all uploaded code for projects that use this Scan Server. Once the Scan Server is added to the Code Insight system, this field cannot be edited.</td>
</tr>
</tbody>
</table>
| [actions for scan server entry] | Select the appropriate icon for the desired action:  
  - The (Edit) icon to edit the configuration for the given Scan Server. The Scan Server dialog is opened, enabling you to make edits.  
  - The Refresh icon (visible when you hover over the Scan Server entry) to refresh the Scan Server entry, including its status. |
| [action] | Use the following button to add a new Scan Server to the Code Insight system—that is, identify the server to the FlexNet Code Insight Core Server to make it available for scanning purposes. To add a Scan Server, ensure that it has been installed and is running. See the FlexNet Code Insight Installation and Configuration Guide for instructions for installing and starting a Scan Server. |
| Add Scan Server | Click this button to add a new Scan Server. The Scan Server dialog is displayed. |

See Also
Scan Server Dialog
Multiple Scan Servers

If multiple Scan Servers have been installed, you can identify more than one of these servers to the system, thus enabling users to distribute codebase scans. Keep in mind that, when multiple Scan Servers are installed, each should be installed on a different instance with a unique host ID and port. The codebase for a given project can be assigned to only one of the Scan Servers (but multiple project codebases can be assigned to a single Scan Server). All codebases assigned to a given Scan Server are stored on that server in a location that you specify.

Prerequisite for Adding or Editing a Scan Server

Ensure that the Scan Server that you are adding or editing is currently running and that the Scan Server you are adding has the same version as the Core Server.

Dialog Fields

The Scan Server dialog contains the following fields:

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>Enter a common name for the Scan Server.</td>
</tr>
<tr>
<td>Host</td>
<td>Provide the hostname (such as kr1.eng.companyA.com) or IP address of the instance hosting the Scan Server. If the Scan Server is on the same instance as the Core Server, enter localhost. The same host-and-port combination must be unique among the enabled Scan Servers. (See Status is this table for a description of enabled Scan Servers.)</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the port used by the Scan Server on the host instance. By default, the port is 8888. The same host-and-port combination must be unique among the enabled Scan Servers. (See Status is this table for a description of enabled Scan Servers.)</td>
</tr>
</tbody>
</table>
Table 8-10 • Scan Server dialog (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **CL Path**      | Provide the path for the FlexNet Code Insight Compliance Library (CL), downloaded from the Flexera Product and License Center. The CL is a database used by the Scan Server to perform exact-file and source-code fingerprint (snippet) matching. Code Insight compares elements of scanned codebase files with information contained in the CL to generate file-level evidence on which you can take action. The validity of the entered path is checked when you click **Save**. Alternatively, leave this field blank to scan your codebase without using the CL. (Code Insight provides the scan profile “Basic Scan Profile (without CL)” to perform the scan.) This type of scan generates inventory from Code Insight’s Automated Analysis feature but has limitations, as described in “About Scanning without the Compliance Library” in the *FlexNet Code Insight Installation and Configuration Guide*. Keep in mind that, when you run a scan using the CL (that is, by specifying a valid CL path), you obtain a deeper, more comprehensive scan on your codebase. For additional information, see the following:  
  - “Managing Scan Profiles” in the *FlexNet Code Insight Installation and Configuration Guide* for more information about the “Basic Scan Profile (without CL)” and about creating and managing scan profiles in general.  
  - **Applying a Scan Profile** in the “Using FlexNet Code Insight” chapter in this book for instructions on associating a scan profile with a project.  
| **Codebase Path** | Provide the path on the Scan Server where FlexNet Code Insight will store and manage all uploaded code for projects that use this Scan Server. Ensure you have adequate disk space to store the codebases. The recommended starting size for this directory is 500GB. The directory must already exist. The validity of the entered path is checked when you click **Save**. Once the Scan Server to added to the Code Insight system, this field cannot be edited. |
By default, the Scan Server is enabled for scanning. However, if necessary for an existing Scan Server, select **Disabled** to make the Scan Server unavailable for further scans. Once disabled, the server is no longer displayed in the **Scan Server** dropdown during project creation or when setting global project defaults. Additionally, this field becomes read-only on the **Edit Project** dialog.

Note the following about disabling a Scan Server:

- If this Scan Server is the system default Scan Server (as defined on the **Project Defaults** tab), you must change this default to another server before you can disable the current server. See [Project Defaults Tab](#) for instructions on updating the default Scan Server.

- If this Scan Server is associated with one or more projects, a warning is displayed before you can disable the server. Once you click **Yes**, the **Start Scan** and **Upload Project Codebase** options are disabled on the **Summary** page for each project associated with the server.

If you attempt to re-enable a disabled Scan Server when another currently enabled Scan Server has the same host-and-port combination or alias, you receive an error when you click **Save**.

### Table 8-10 • Scan Server dialog (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Status**   | By default, the Scan Server is enabled for scanning. However, if necessary for an existing Scan Server, select **Disabled** to make the Scan Server unavailable for further scans. Once disabled, the server is no longer displayed in the **Scan Server** dropdown during project creation or when setting global project defaults. Additionally, this field becomes read-only on the **Edit Project** dialog. Note the following about disabling a Scan Server:

- If this Scan Server is the system default Scan Server (as defined on the **Project Defaults** tab), you must change this default to another server before you can disable the current server. See [Project Defaults Tab](#) for instructions on updating the default Scan Server.

- If this Scan Server is associated with one or more projects, a warning is displayed before you can disable the server. Once you click **Yes**, the **Start Scan** and **Upload Project Codebase** options are disabled on the **Summary** page for each project associated with the server.

If you attempt to re-enable a disabled Scan Server when another currently enabled Scan Server has the same host-and-port combination or alias, you receive an error when you click **Save**. |

- **Save** | Click this button to save any changes you made to the Scan Server properties. Errors are generated when the following conditions exist:

  - The Scan Server you are adding or editing is not running.

  - The version of the Scan Server you are adding is different from the Core Server version.

  - The codebase path or CL path is invalid. |

- **Cancel** | Click this button to cancel any changes you made to the fields on the Scan Server dialog. |

### See Also

- [Project Defaults Tab](#)
- [Edit Project: Scan Settings Tab](#)
- [Scan Servers Tab](#)
- [What Is a FlexNet Code Insight Scan?](#)
Scan Profiles Tab

The Scan Profiles tab on the Administration page allows you to add a scan profile and edit information about an existing scan profile. The tab contains the following columns and fields:

Table 8-11 • Scan Profiles tab

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Profiles list</td>
<td>A list (in grid format) of available scan profiles. The following are the predefined scan profiles:</td>
</tr>
<tr>
<td></td>
<td>• Standard Scan Profile</td>
</tr>
<tr>
<td></td>
<td>• Basic Scan Profile (without CL)</td>
</tr>
<tr>
<td></td>
<td>• Comprehensive Scan Profile</td>
</tr>
<tr>
<td></td>
<td>The list will contain additional profiles if you have added them.</td>
</tr>
<tr>
<td></td>
<td>The following are key attributes shown for each scan profile in the list. These attributes are described in detail in Create/Edit Scan Profile Dialog.</td>
</tr>
<tr>
<td></td>
<td>• Scan Archives—Whether the Scan Server will perform package discovery and license detection within all archive files in the project codebase.</td>
</tr>
<tr>
<td></td>
<td>• Dependencies—The level of component-dependency scanning to be performed by the Scan Server.</td>
</tr>
<tr>
<td></td>
<td>• Exact Matches—Whether Scan Server is enabled to identify those codebase files that exactly match file data in the CL (Compliance Library).</td>
</tr>
<tr>
<td></td>
<td>• Source Code Matches—Whether the Scan Server is enabled to identify source-code strings (snippets) in the scanned codebase files that match exact strings in the CL.</td>
</tr>
<tr>
<td>Edit icon</td>
<td>To edit a scan profile, click this icon at the end of the profile entry in the list. The Edit Scan Profile dialog is opened, enabling you to edit profile settings. See Create/Edit Scan Profile Dialog for setting descriptions.</td>
</tr>
<tr>
<td>Add Scan Profile button</td>
<td>Select this button to create a new scan profile. The Create Scan Profile dialog is opened. See Create/Edit Scan Profile Dialog for setting descriptions.</td>
</tr>
</tbody>
</table>

See Also
Create/Edit Scan Profile Dialog
What Is a FlexNet Code Insight Scan?
Applying a Scan Profile to the Project
Create/Edit Scan Profile Dialog

Both the Create Scan Profile dialog and the Edit Scan Profile dialog contain the fields described in this table to define or update a scan profile. Administrators access either dialog from the Scan Profiles tab on the Administration page.

In addition to letting you create your own scan profiles, FlexNet Code Insight ships with the following pre-defined scan profiles, which you can modify, assign to projects, or use as templates for creating your own profiles. For your reference, the table below indicates which scan settings are enabled for each pre-defined profile. For example, to view the settings enabled for:

- The Basic Scan Profile (without CL), see the Basic column in the table.
- The Standard Scan Profile, see the Standard column.
- The Comprehensive Scan Profile, see the Comprehensive column.

Note the following about the pre-defined scan profiles:

- The Comprehensive and Standard Scan Profiles rely on data stored in the Compliance Library (CL) to detect evidence for Exact Matches and Source Code Matches.
- The Standard Scan Profile cannot be modified.

**Table 8-12 • Scan Profile Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Basic</th>
<th>Standard</th>
<th>Comprehensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter or edit the profile name.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Perform Package/License Discovery in Archives</td>
<td>Select this option to have the Scan Server recursively perform package discovery and license detection within all archive files encountered in the project codebase. By default, this option is selected.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Dependency Support</td>
<td>Determine the level of dependency scanning to be performed by the Scan Server. The available options include:</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>• <strong>No Dependencies</strong>: Only top-level inventory items are reported without any dependencies. (Default)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Only First Level Dependencies</strong>: Only first-level (or direct) dependencies are reported along with top-level inventory items.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>All Transitive Dependencies</strong>: All first-level and transitive dependencies are reported along with top-level inventory items. The Scan Server calls out to the relevant package management repository to obtain transitive dependency information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For a description of Code Insight dependency support for supported ecosystems, see the “Automated Analysis” chapter in the FlexNet Code Insight User Guide.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatically Add Related Files to Inventory</td>
<td>Select this option to have the system associate additional files to existing inventory items based on the data available in automatic detection rules.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Table 8-12 • Scan Profile Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Basic</th>
<th>Standard</th>
<th>Comprehensive</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Exact Matches</strong></td>
<td>Select this option to enable the detection and recording of scanned files that exactly match entire-file data in the Compliance Library (CL).</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Source Code Matches</strong></td>
<td>Select this option to enable the detection and recording of any source-code snippets in the scanned files that match data in the Compliance Library (CL).</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Include System-Identified Files</td>
<td>Select this option if you want the Scan Server to perform source-code matching for files that have already been associated with one or more inventory items during automated analysis.</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Include Files with Exact Matches</td>
<td>Select this option if you want the Scan Server to perform source-code matching for files that have already been identified as having exact-file matches in the CL.</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Minimum Source Code Matches</td>
<td>Enter the minimum number of source-code matches that the scan needs to detect in a given codebase file before reporting the file as having such matches. <em>(A source-code match is a snippet of code in a codebase file that matches an open-source code snippet found in the CL data.)</em> Enter a new minimum value from 1 to 32767. <em>(The default is 3.)</em> For example, if this value is increased to 10, ten code snippets in a given codebase file must match data in the CL before the scan reports the file as having source-code matches. In general, the higher this value, the fewer source-code matches an analyzer has to review.</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Search Terms</td>
<td>Provide a list of search terms to be used in the scan. Use the + button to add a term and the - button to remove a term.</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Scan Exclusions</td>
<td>Provide a list of file extensions to be excluded from the scan. Use the + button to add an exclusion term and the - button to remove an exclusion. <em>Also see “Creating Exclusion Patterns for Scan Profiles” in the FlexNet Code Insight Installation and Configuration Guide.</em></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

**See Also**
- Scan Profiles Tab
- What Is a FlexNet Code Insight Scan?
- Applying a Scan Profile to the Project
- Edit Project: Scan Settings Tab
Project Defaults Tab

The settings on Project Defaults tab on the Administration page work provide a convenient way to default fields used to configure new projects to ensure consistency and enable an easier project creation experience for users. Although the settings you define here are global across all projects, they can be overridden at the project level as needed. See the following field descriptions for more information.

Table 8-13 • Project Defaults tab

<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Options</td>
<td>These options set defaults for project creation and assign default users to project roles. Users can change these defaults when creating a project or when editing a project or its users using Manage Project</td>
</tr>
<tr>
<td>Project Type</td>
<td>Select the default project type based on scan requirements:</td>
</tr>
<tr>
<td></td>
<td>• Standard—A project whose scans require that its codebase be uploaded to FlexNet Code Insight or be synchronized pre-scan using an SCM plugin (such as Bitbucket, Git, Perforce, or TFS). This is the initial system default. This is the initial system default.</td>
</tr>
<tr>
<td></td>
<td>• Inventory Only—A project whose scans are performed through a remote scan agent, thus eliminating the need to upload the codebase to FlexNet Code Insight. These scans generate project inventory only. Consequently, the Analysis Workbench is not available for codebase analysis. For details about inventory-only projects, see Performing Inventory-Only Scanning.</td>
</tr>
<tr>
<td>Project Visibility</td>
<td>Select the default for visibility status—Public or Private—for projects. (The initial system default is Public.)</td>
</tr>
<tr>
<td></td>
<td>For public projects, users who are not the Project Owner nor directly assigned the Reviewer or Analyst role have read-only access to the project inventory. However, private projects are hidden from all users except the Project Owner and those users assigned as Analysts, Reviewers, and Observers of the project.</td>
</tr>
<tr>
<td>Project Risk</td>
<td>Select the default risk value (Low, Medium, or High) for projects. To edit, select another value from the dropdown. The initial system default is Medium.</td>
</tr>
<tr>
<td>Project Users</td>
<td>Click the Edit Project Users link to open the Edit Default Project Users page. From here you assign project roles—Analysts, Reviewers, and Observers—that will default for any new project created (but which can then be edited at the project level). See Edit (Default) Project Users Page for details.</td>
</tr>
</tbody>
</table>
**Table 8-13 • Project Defaults tab (cont.)**

<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the data import or rescan, delete inventory with no associated files</td>
<td>This option determines whether “empty” system-generated inventory items are deleted in the target project during project imports and rescans. Empty inventory items have no associated files.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Selected</strong>—Deletes empty inventory items from the target project during project imports and rescans. Only inventory items with associated files are retained/created.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Unselected</strong>—Retains/creates all inventory items—with or without matching associated files in the target codebase—in the target project during imports and rescans. For example, you might want to retain inventory items to save their analysis details. (Users will need to manually delete inventory that is not applicable to the current project.)</td>
</tr>
<tr>
<td></td>
<td>This configuration (unselected) is required if when importing a scanned codebase into an inventory-only project, which has no codebase, to ensure inventory is generated in the target project.</td>
</tr>
</tbody>
</table>

| Scan Settings                                  | These options identify the default Scan Server and scan profile for projects. Users can change these settings at the project level by navigating to Manage Project | Edit Project | Scan Settings from the project Summary tab. |
| Scan Profile                                  | Select the scan profile to default for projects. Click ![View Details](#) to view the details of the scan profile. |
| Scan Server                                   | Select the Scan Server to default for projects. Note that only those Scan Servers in an “enabled” state are available for selection. If only one Scan Server has been identified to the system, this server is automatically selected as the default. |

| Automated Inventory Publish Options            | These options enable and configure the automatic publication of project inventory as part of the project scan process. Users can change these settings at the project level by navigating to the project Summary tab and selecting Manage Project | Edit Project | Scan Settings. |
|                                               | If the **Auto-publish system-created inventory items meeting this minimum Confidence Level** is selected to enable auto-publication, the other auto-publish options are made available. |
Auto-publish system-created inventory items meeting this minimum Confidence Level

Select this option to enable the auto-publication of system-generated inventory items. (By default, the option is selected.) Then select the minimum Inventory Confidence level required to determine which items to auto-publish:

- **Low**—Automatically publish all system-generated inventory.
- **Medium**—Automatically publish only those system-generated inventory items with Medium and High confidence levels.
- **High**—Automatically publish only those system-generated inventory items with a High confidence level.

For a description of the Confidence levels and how they are used, see Inventory Confidence.

Do not auto-publish inventory items with an undetermined license

Select this option to not auto-publish any system-generated inventory item with an undetermined license (that is, an inventory item whose License value is I don’t know). An undetermined license can occur under the following conditions:

- The scan was not able to identify a license for the given component during the scan and therefore set the I don’t know license value.
- The inventory item has multiple possible disjunctive licenses (for example, “GPLv2 or MIT”). However, the scan could find no evidence of the desired selected license and therefore set the I don’t know license value.
- The inventory item has multiple possible conjunctive licenses (for example, “GPLv2 and MIT”). However, since Code Insight currently supports only a single selected license, the scan automatically set the I don’t know value for the inventory item.

This option is available only if Auto-publish system-created inventory items meeting this minimum Confidence level is selected. By default, when you first open FlexNet Code Insight instance after it has been installed or migrated, this option is unselected, allowing the auto-publication of inventory with undetermined licenses.

Mark associated file as reviewed

Select this option if you want Code Insight to automatically mark the files associated with each automatically published inventory item as “reviewed”.

This option is available only if Auto-publish system-created inventory items meeting this minimum Confidence level is selected.
**Chapter 8  Pages and Panels**

**Project Defaults Tab**

### Automated Review Options

These options configure defaults for enabling policies that automatically accept or reject inventory when it is published. Users can change these settings at the project level by navigating to Manage Project | Edit Project | Review and Remediation Settings from the project Summary tab.

<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy Profile</strong></td>
<td>Select the default policy profile to associate with all new projects. (The system default is Default License Policy Profile.) The policy profile contains a set of policies that use components, versions, licenses, and vulnerability scores and severities as criteria to automatically reject or approve inventory items during a codebase scan (or post-scan). For more information about policy profiles in general, see Managing Policy Profiles.</td>
</tr>
</tbody>
</table>
| **Automatically reject inventory items impacted by a new vulnerability that violates your policy** | Indicate the default action to take for published inventory affected by a new security vulnerability downloaded as part of an Electronic Update. The selected action applies to both non-reviewed and previously approved inventory items on the Project Inventory tab.  
- Select this checkbox to automatically reject those project inventory items impacted by a new security vulnerability only if this vulnerability has a CVSS score or severity greater than the thresholds configured as policy for the Code Insight project. For each inventory item rejected due to a new security vulnerability, the icon and a tip are added to indicate the status change and its reason.  
  
  If a new vulnerability does not exceed policy thresholds, the current status of the inventory item is not affected.  
- Leave the checkbox unselected to retain the current status of inventory items impacted by the new vulnerability.  

For information about setting policies that define CVSS-score and severity thresholds used to reject or approve inventory items automatically, see Policy Page and Policy Details Page. For information about associating these policies with a project, see Managing Policy Profiles. |
These options configure defaults for project inventory not automatically reviewed by policy. Users can change these settings at the project level by navigating to Manage Project | Edit Project | Review and Remediation Settings from the project Summary tab.

What should happen if inventory items are not reviewed by policy?

- **do nothing**—Simply show the status of the inventory item as Not Reviewed on the Project Inventory tab.
- **send an email notification to the project owner**—Automatically send an email to the Project Owner, stating the need for a manual review of the item. The value for Select the minimum priority... (described in the next table entry) affects this option.
- **automatically create a manual review task**—Automatically create a manual review task assigned to the default legal or security reviewer (or both reviewers), and send an email, notifying the reviewer(s) about assigned task.

Information about managing such a task to track the progress of a manual review is found in Creating and Managing Tasks for Project Inventory.

The value for Select the minimum priority... (described in the next table entry) affects this option.

<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Review Options</td>
<td>These options configure defaults for project inventory not automatically reviewed by policy. Users can change these settings at the project level by navigating to Manage Project</td>
</tr>
<tr>
<td>What should happen if inventory items are not reviewed by policy?</td>
<td>Indicate the default action to trigger for those inventory items that are not affected by policy (and therefore have a Not Reviewed status) during the publication of inventory either as part of a scan or manually by a user:</td>
</tr>
<tr>
<td></td>
<td>• <strong>do nothing</strong>—Simply show the status of the inventory item as Not Reviewed on the Project Inventory tab.</td>
</tr>
<tr>
<td></td>
<td>• <strong>send an email notification to the project owner</strong>—Automatically send an email to the Project Owner, stating the need for a manual review of the item. The value for Select the minimum priority... (described in the next table entry) affects this option.</td>
</tr>
<tr>
<td></td>
<td>• <strong>automatically create a manual review task</strong>—Automatically create a manual review task assigned to the default legal or security reviewer (or both reviewers), and send an email, notifying the reviewer(s) about assigned task.</td>
</tr>
<tr>
<td></td>
<td>Information about managing such a task to track the progress of a manual review is found in Creating and Managing Tasks for Project Inventory.</td>
</tr>
<tr>
<td></td>
<td>The value for Select the minimum priority... (described in the next table entry) affects this option.</td>
</tr>
<tr>
<td>Select the minimum priority to perform the action selected above</td>
<td>(Enabled when an option other than do nothing is selected for the previous field.) Select the default minimum inventory priority (P1, P2, P3, or P4) to which the value for the previous field applies.</td>
</tr>
<tr>
<td></td>
<td>For example, if the previous field is set to send an email notification to the project owner and minimum priority is set to P3, then the email notification will be sent for only those non-reviewed inventory items with a P1, P2, or P3 priority. No email notification will be sent for P4 inventory items.</td>
</tr>
</tbody>
</table>

**Note** • This option has no effect when the do nothing value is selected.
**What type of manual reviews will be performed on this project?**

Set the default type of manual review tasks to be generated:

- **Legal Only**—Review tasks are generated for those non-reviewed inventory items that do not meet legal policy criteria. The tasks are automatically assigned to the default Legal reviewer.

- **Security Only**—Review tasks are generated for only those non-reviewed inventory items that have security vulnerabilities. The tasks are automatically assigned to the default Security reviewer.

- **both Legal and Security**—Review tasks are generated for all non-reviewed inventory items that do not meet legal policy criteria; these are assigned to the default Legal reviewer. Additionally, review tasks are generated for those non-reviewed inventory tasks associated with security vulnerabilities and are assigned to the default Security reviewer.

With this value, a single inventory item might have both a legal review task and security review task generated. However, if the default reviewers are the same user, a single task is created, describing the requirement for both a legal and security manual review.

**Select reviewers for this project**

If desired, designate a new default Legal reviewer or Security reviewer (or both) to which to assign manual review tasks. (The Project Owner is the designated as the initial system default for both reviewers.)

Then, depending on the type of manual review selected for the project (see the **What type of manual reviews will be performed...** option described previously), Code Insight determines which reviewer (Legal or Security or both) is assigned the task and then notified of the task by email. The reviewer(s) can then manage the task accordingly, possibly reassigning it to another user. For details about managing and reassigning tasks, see Creating and Managing Tasks for Project Inventory.

To select a new default reviewer, click **Change User** next to the name of the current Legal reviewer or Security reviewer assignee, then select a user from the **Select new...contact** dialog, and click **Apply**. (To reset the reviewer to the Project Owner, click **Reset**.)

When a new default reviewer is selected, that user is automatically given the role of project “reviewer” should the user not currently have this role. However, should the current reviewer reassign a specific task to another user, the “reviewer” role is not automatically assigned to that user.

If the Project Owner is specified as a default reviewer, the owner’s actual name is displayed for the reviewer at the project level.

<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>What type of manual reviews will be performed on this project?</td>
<td>Set the default type of manual review tasks to be generated:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Legal Only</strong>—Review tasks are generated for those non-reviewed inventory items that do not meet legal policy criteria. The tasks are automatically assigned to the default Legal reviewer.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Security Only</strong>—Review tasks are generated for only those non-reviewed inventory items that have security vulnerabilities. The tasks are automatically assigned to the default Security reviewer.</td>
</tr>
<tr>
<td></td>
<td>- <strong>both Legal and Security</strong>—Review tasks are generated for all non-reviewed inventory items that do not meet legal policy criteria; these are assigned to the default Legal reviewer. Additionally, review tasks are generated for those non-reviewed inventory tasks associated with security vulnerabilities and are assigned to the default Security reviewer.</td>
</tr>
<tr>
<td>Select reviewers for this project</td>
<td>If desired, designate a new default Legal reviewer or Security reviewer (or both) to which to assign manual review tasks. (The Project Owner is the designated as the initial system default for both reviewers.)</td>
</tr>
<tr>
<td></td>
<td>Then, depending on the type of manual review selected for the project (see the <strong>What type of manual reviews will be performed...</strong> option described previously), Code Insight determines which reviewer (Legal or Security or both) is assigned the task and then notified of the task by email. The reviewer(s) can then manage the task accordingly, possibly reassigning it to another user. For details about managing and reassigning tasks, see Creating and Managing Tasks for Project Inventory.</td>
</tr>
<tr>
<td></td>
<td>To select a new default reviewer, click <strong>Change User</strong> next to the name of the current Legal reviewer or Security reviewer assignee, then select a user from the <strong>Select new...contact</strong> dialog, and click <strong>Apply</strong>. (To reset the reviewer to the Project Owner, click <strong>Reset</strong>.)</td>
</tr>
<tr>
<td></td>
<td>When a new default reviewer is selected, that user is automatically given the role of project “reviewer” should the user not currently have this role. However, should the current reviewer reassign a specific task to another user, the “reviewer” role is not automatically assigned to that user.</td>
</tr>
<tr>
<td></td>
<td>If the Project Owner is specified as a default reviewer, the owner’s actual name is displayed for the reviewer at the project level.</td>
</tr>
</tbody>
</table>
Chapter 8  Pages and Panels

Project Defaults Tab

These options configure defaults for rejected project inventory. Users can change these settings at the project level by navigating to Manage Project | Edit Project | Review and Remediation Settings from the project Summary tab.

<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
</tr>
</thead>
</table>
| What should happen if inventory items are rejected? | Indicate the default action to trigger for those inventory items that are automatically rejected by policy during the publication of inventory either as part of a scan or manually by a user:  
  - **do nothing**—Simply show the status of the inventory item as Reject on the Project Inventory tab.  
  - **send an email notification to the project owner**—Automatically send an email to the Project Owner, stating the need for remediation work on the inventory item.  
  - **automatically create a remediation task**—Automatically create a remediation task assigned to the default development contact (see the Assignee for remediation work option) and send an email, notifying the contact about the assigned task.  
  - **automatically create a remediation task and an external work item**—Automatically do the following:  
    - Create a remediation task assigned to the default development contact (see the Assignee for remediation work option) and send an email, notifying the contact about the assigned task. (See the previous bulleted item for more information.)  
    - Associate a work item with the task, creating the work item in an Application Lifecycle Management (ALM) system (such as an issue in Jira). The work item is created and assigned using the settings defined for the ALM instance to which the Code Insight project is associated. For more information about configuring an ALM instance for the project, see ALM Settings.  
  
| Assignee for remediation work | If desired, designate a new default development contact—for example, an engineering manager—to which to assign remediation tasks. (The Project Owner is the initial system default.) This contact can then manage the task accordingly—for example, reassigning it to another user or manually creating an external work item and assigning it to someone on the development team. For details about managing and reassigning tasks, see Creating and Managing Tasks for Project Inventory.  
  
To select a new contact, click **Change User** next to the name of the current assignee, select a user from the **Select new...contact** dialog, and click **Apply**. (To reset the reviewer to the Project Owner, click **Reset**.)  
If the Project Owner is specified as the default, the owner’s actual name is displayed as the remediation assignee at the project level.
System Settings Tab

The System Settings tab is used to define settings that configure your FlexNet Code Insight system. The tab provides the following configuration settings:

Table 8-14 • System Settings Tab

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Vulnerability</td>
<td>Select the CVSS (Common Vulnerability Scoring System) version—CVSS v3.0 or CVSS v2 in which to display security vulnerability scores and severities in the Code Insight Web UI. Initially, CVSS v 2.0 is the default. If you switch versions, the CVSS scores and severity values displayed for vulnerabilities will be impacted, as will policies based on these values. For more information, see Security Vulnerabilities Associated with Inventory and Managing Policy Profiles.</td>
</tr>
</tbody>
</table>

Projects List Page

The Project List page enables you to search for, view, and add FlexNet Code Insight projects. The page contains the following fields:

Table 8-15 • Projects List page

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tree view</td>
<td>Click to change the display to a tree view.</td>
</tr>
</tbody>
</table>
### Table 8-15 • Projects List page (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List view</td>
<td>Click to change the display to a list view.</td>
</tr>
<tr>
<td>Add New</td>
<td>Click to add a new folder or project to the list. (This button is displayed only if you have permission to create projects.)</td>
</tr>
<tr>
<td>My Projects</td>
<td>Click to show only those projects with which you are associated, either as Project Owner or with a project role (Analyst, Reviewer, or Observer).</td>
</tr>
<tr>
<td>Projects (x)</td>
<td>Lists the number of projects in the system. If the list is filtered, the filtered count is shown in relation to the full count (for example, “(19 of 123)”.)</td>
</tr>
</tbody>
</table>
| Project Search fields | From the search filters on the left, select the filter based on the type of search you want to perform (Project Name, Project Inventory, or Security Vulnerability). In the field on the right, enter the string criterion for the search:  
  - When searching for a project name, enter a partial string or full project name.  
  - When searching for project inventory, enter the inventory name, component name, license name, or SPDX short identifier of the inventory item. The characters must be consecutive in the search string. A partial string is supported.  
  - When searching for a security vulnerability, enter the exact vulnerability ID.  
Press Enter to view the filtered list. If no inventory items meet the specified criterion, the Projects list shows “No Projects”. To clear the search filter and restore the full project list, click in the criterion field. See for Searching the System for full details. |
| Name               | A hyperlinked list of the names of all projects in the system. When you select a project from the list, information about the project appears in the panes of the Summary tab. Click the arrow to toggle the list from A to Z or from Z to A. |
| Selected Project Name | When you select a project from the list, the name of the selected project appears in this field. You can click the selected project name to open the project. |
| Owner              | The hyperlinked name of the person who owns the project. Click the name to open your default email program to send an email to the Project Owner. |
| Profile            | Displays the name of the profile attached to the selected project. If no profile is attached to the project, “No profile selected” appears. |
| Created            | Displays the data that the project was created. |
| Last Scan          | Displays the date that the codebase was last scanned. |
The Summary tab for the project allows you to add and edit users who can work in FlexNet Code Insight, view scan settings and status, generate reports, and manage projects. The page contains the following fields:

Table 8-16 • Project Summary tab

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project Details</strong></td>
<td>These field describe the project attributes. You can edit these details using the Manage Project</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The name given to the selected project and its Id number.</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>The hyperlinked name of the person who owns the project. Click the name to open your default email program to send an email to the Project Owner.</td>
</tr>
</tbody>
</table>

See Also
Creating a Project
Project Summary Tab
Using the Project Dashboard
Searching the System
<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Contact</td>
<td>The hyperlinked name of the default legal contact assigned to tasks created to review legal issues in the project inventory. Click the name to open your default email program to send an email to the contact. Initially, this default contact is the Project Owner. This field appears only if a new default legal contact is assigned. See Updating Inventory Review and Remediation Settings for a Project for details.</td>
</tr>
<tr>
<td>Security Contact</td>
<td>The hyperlinked name of the default security contact assigned to tasks created to review security issues in the project inventory. Click the name to open your default email program to send an email to the contact. Initially, this default contact is the Project Owner. This field appears only if a new default legal contact is assigned. See Updating Inventory Review and Remediation Settings for a Project for details.</td>
</tr>
<tr>
<td>Developer Contact</td>
<td>The hyperlinked name of the default development contact assigned to remediation tasks created to take action on code-related issues in the project inventory. Click the name to open your default email program to send an email to the contact. Initially, this default contact is the Project Owner. This field appears only if a new default legal contact is assigned. See Updating Inventory Review and Remediation Settings for a Project for details.</td>
</tr>
<tr>
<td>Description</td>
<td>A description, if entered, of the project appears in this field.</td>
</tr>
<tr>
<td>Project Type</td>
<td>The type of project:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Inventory Only</strong>—Processes all published inventory, providing inventory details and file associations.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Standard</strong>—Processes all inventory (published or unpublished), providing inventory details and file associations and marking appropriate files as reviewed based on policy.</td>
</tr>
<tr>
<td>Project Visibility</td>
<td>The visibility of the project:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Public</strong>—All users in the system can view this project. Users assigned to roles in the project can perform various maintenance functions based on permissions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Private</strong>—Only users assigned to roles in this project have access to it.</td>
</tr>
</tbody>
</table>
The current status of the project that can be manually updated through the Manage Project | Edit Project menu option available on this tab. Available status types include:

- **Not Started**—Indicates that the project scan results are not available for manual analysis. This value automatically defaults when the initial project scan has not been run or when the initial scan fails. However, you can manually change this status.

- **Analysis in Progress**—Indicates that the project scan results are available for manual analysis, or a manual analysis is underway. This value is automatically set when the initial project scan is complete. (For a project import, however, the status of the target project is retained.) You can manually change this status.

- **Analysis Completed**—Indicates that manual analysis is finished; and the published inventory is ready for legal, security, or software-engineering review. (You must manually set this value.)

- **Project Complete**—Indicates that the project analysis and review processes are complete, and notices content for all OSS and third-party software is finalized. (You must manually set this value.)

For more information, see Editing the Project Definition and General Settings and Edit Project: General Tab.

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project Status</strong></td>
<td>The current status of the project that can be manually updated through</td>
</tr>
<tr>
<td></td>
<td>the Manage Project</td>
</tr>
<tr>
<td></td>
<td>- Not Started—Indicates that the project scan results are not available for manual analysis. This value automatically defaults when the initial project scan has not been run or when the initial scan fails. However, you can manually change this status.</td>
</tr>
<tr>
<td></td>
<td>- Analysis in Progress—Indicates that the project scan results are available for manual analysis, or a manual analysis is underway. This value is automatically set when the initial project scan is complete. (For a project import, however, the status of the target project is retained.) You can manually change this status.</td>
</tr>
<tr>
<td></td>
<td>- Analysis Completed—Indicates that manual analysis is finished; and the published inventory is ready for legal, security, or software-engineering review. (You must manually set this value.)</td>
</tr>
<tr>
<td></td>
<td>- Project Complete—Indicates that the project analysis and review processes are complete, and notices content for all OSS and third-party software is finalized. (You must manually set this value.)</td>
</tr>
<tr>
<td><strong>Project Risk</strong></td>
<td>The project vulnerability risk value (Low, Medium, or High).</td>
</tr>
<tr>
<td><strong>Scan Settings</strong></td>
<td>The following fields show scan configuration details. You can edit these details on the Scan Settings tab accessed using the Manage Project</td>
</tr>
<tr>
<td><strong>Policy Profile</strong></td>
<td>The name of the profile associated with this project.</td>
</tr>
<tr>
<td><strong>Scan Profile</strong></td>
<td>The name of the scan profile associated with this project. Click ![icon] to view the details of the scan profile.</td>
</tr>
<tr>
<td><strong>Scan Paths</strong></td>
<td>The location of your codebase. Click ![icon] to view the details about the Scan Server.</td>
</tr>
<tr>
<td><strong>Scan Status</strong></td>
<td>The following fields provide information about the currently running scan, most recent scan, and historical scans.</td>
</tr>
</tbody>
</table>
Table 8-16 • Project Summary tab (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Scan Status** | The scan status as follows:  
  • If you have started a scan, but the scan has been placed in queue, this field shows “Scan Scheduled”. The **Scan Progress** field provides a link to view the scan queue and other details (see the “Scan Progress” description below).  
  • If the scan you scheduled is running, this field shows “Project being scanned”. The **Scan Progress** field keeps track of the number of files that have been scanned.  
  • When the scan completes, this field shows “No scan scheduled” and provides link to schedule another scan. (If the Scan Server is disabled, the link is also disabled.) The **Scan Progress** field is not available when this status is in effect. |
| **Scan Progress** | (Available only when a scan is scheduled or is running) The progress of the scan as follows:  
  • If the scan has been placed in queue, this field shows “In Scan Queue” and provides a **Show Details** link to open the **Scan Server Status** window. This window identifies the scan server, shows the project currently being scanned by the server, lists the other project scans (if any) currently waiting in queue order (up to 25 scans), and provides an email link for the owner of each project listed. You cannot sort or reorganize the queue list.  
  • If the scan you scheduled is running, this field keeps track of the number of files whose scan is complete against the total number of files to scan in the project. |
| **Last Scan** | The final status of the last scan and provides a statistical summary of what was scanned. |
| **Past Scans** | Click the hyperlinked term **here** to view the scan history for the selected project. A dialog appears with a list of scans performed on the project. If a scan has not yet been performed for the project, the list will be empty. |
These fields provide access to reports. If the report has been generated, the field shows the report generation timestamp and provides links to view or download the report. If the report has not been generated, select the report from the **Select Report** dropdown and click **Generate Report**. The standard Code Insight reports available are described below. If custom reports have been created, they are also available on the **Select Report** dropdown.

### Project Report
Provides status information about and access to the Project Report. This report summarizes the inventory, vulnerabilities, remaining scan evidence, and review and remediation tasks for the current project.

### Audit Report
Provides status information about and access to the Audit Report. This report provides one means to distribute your research and findings to others in your organization. Only published inventory items appear in Audit reports.

### Notices Report
Provides status information about and access to the Notices Report. This report is a compilation of the license (notices) content for all the open source/third-party components contained in the product.

**[Actions]**

The following buttons enable to perform functions on your project.

- **Start Scan**
  Click to start your codebase scan or rescan.
  
  If the Scan Server is disabled, this button is disabled.
  
  Optionally, to force a full codebase rescan, click the drop-down arrow to the right of this button and select **Full Rescan**. (This option is enabled only if a successful initial scan has been run on the project codebase.)
  
  For more information about scans and rescans, see **Scanning the Codebase** and **Rescanning Your Codebase**.

- **Generate Report**
  Click to generate a Project, Audit, Notices, or custom report in the background.

- **Upload Project Codebase**
  Click to upload the codebase that will be scanned for the selected project. You can also use this option to overwrite the current codebase with the most recent version.
  
  If the current project is not associated with a Scan Server or the Scan Server is disabled, this button is disabled.

- **Manage Project**
  A dropdown menu that allows you to edit project settings, assign user roles for the project, export and import project data, delete a project, or change the project owner.
See Also
Creating a Project
Editing the Project Definition and General Settings
Edit Project: General Tab
Projects List Page
Uploading a Project Codebase
Exporting and Importing Project Data chapter

Edit Project: General Tab

The General tab on the Edit Project dialog displays information about the selected project that you can edit. The tab contains the following fields:

Table 8-17 • Edit Project: General tab

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Name</td>
<td>The name of the selected project. You can change the name by typing over the current project name.</td>
</tr>
<tr>
<td>Description</td>
<td>A freeform text field in which you can enter a description for the project. This field provides enough space to add as much detail about the project as necessary.</td>
</tr>
<tr>
<td>Project Visibility</td>
<td>The visibility status—Public or Private—of the project. For public projects, users who are not the Project Owner nor directly assigned the Reviewer or Analyst role have read-only access to the project inventory. However, private projects are hidden from all users except the Project Owner and those users assigned as Analysts, Reviewers, and Observers of the project.</td>
</tr>
<tr>
<td>Project Risk</td>
<td>The current vulnerability risk value (Low, Medium, or High) for the project. To edit, select another value from the dropdown.</td>
</tr>
</tbody>
</table>
Chapter 8  Pages and Panels
Edit Project: General Tab

Table 8-17 • Edit Project: General tab (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Status</td>
<td>The current status of the project. The following statuses are available and their suggested definitions are provided here. However, you can apply these statuses as appropriate for your site:</td>
</tr>
<tr>
<td>Not Started</td>
<td>Indicates that the project scan results are not available for manual analysis. This value automatically defaults when the initial project scan has not been run or when the initial scan fails. However, you can manually change this status.</td>
</tr>
<tr>
<td>Analysis in Progress</td>
<td>Indicates that the project scan results are available for manual analysis, or a manual analysis is underway. This value is automatically set when the initial project scan is complete. (For a project import, however, the status of the target project is retained.) You can manually change this status.</td>
</tr>
<tr>
<td>Analysis Completed</td>
<td>Indicates that manual analysis is finished; and the published inventory is ready for legal, security, or software-engineering review. (You must manually set this value.)</td>
</tr>
<tr>
<td>Project Complete</td>
<td>Indicates that the project analysis and review processes are complete, and notices content for all OSS and third-party software is finalized. (You must manually set this value.)</td>
</tr>
</tbody>
</table>

On the data import or rescan, delete inventory with no associated files

- Selected—Deletes empty inventory items from the target project during project imports and rescans. Only inventory items with associated files are retained/created.
- Unselected—Retains/creates all inventory items—with or without matching associated files in the target codebase—in the target project during imports and rescans. For example, you might want to retain inventory items to save their analysis details. (You will need to manually delete inventory that is not applicable to the current project.)

This configuration (unselected) is required if you are importing a scanned codebase into an inventory-only project, which has no codebase, to ensure inventory is generated in the target project.

Project Folder

- The folder in the Projects list under which the project is currently grouped. To edit the project location in the list, select one of the following:
- Clear Project Folder button—Click this button to remove the project from the current folder in the Projects list and place it in the root folder.
- Select a New Folder dropdown—Click the down arrow to locate and select an available folder to which to move the project.
See Also

Editing the Project Definition and General Settings

Edit Project: Scan Settings Tab

The Edit Project: Scan Settings tab on the Edit Project dialog displays information about the scan settings defined for the selected project. You can edit the following information on this tab. (See also the Edit Project: General Tab to configure the project setting that determines whether the scan retains inventory that has no files associations.)

Table 8-18 • Edit Project: Scan Settings tab

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td>These fields identify the Scan Server and profile used to run a project scan.</td>
</tr>
<tr>
<td><strong>Scan Profile</strong></td>
<td>The scan profile associated with the project. You can select a different scan profile from the dropdown list. Click to view the properties of the currently selected scan profile.</td>
</tr>
<tr>
<td><strong>Scan Server</strong></td>
<td>The Scan Server assigned to this project. This field is not editable. Click to view the properties of the currently selected Scan Server.</td>
</tr>
</tbody>
</table>

**Auto-Publish**

These options enable and configure the automatic publication of project inventory as part of the project scan process.

If the Auto-publish system-created inventory items meeting this minimum Confidence Level is selected to enable auto-publication, the other auto-publish options are made available.

| Auto-publish system-created inventory items meeting this minimum Confidence Level | Select this option to enable the auto-publication of system-generated inventory items. (By default, the option is selected.)
---|---
| | Then select the minimum Inventory Confidence level required to determine which items to auto-publish:
| Low | Auto-publish all system-generated inventory.
| Medium | Auto-publish only those system-generated inventory items with Medium and High confidence levels. (This is the default value.)
| High | Auto-publish only those system-generated inventory items with a High confidence level.

For a description of the Confidence levels and how they are used, see Inventory Confidence in the “Using FlexNet Code Insight” chapter.
### Table 8-18 • Edit Project: Scan Settings tab (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Do not auto-publish inventory items with an undetermined license** | Select this option to *not* auto-publish any system-generated inventory item with an undetermined license (that is, an inventory item whose **License** value is *I don't know*). An undetermined license can occur under the following conditions:  
  - The scan was not able to identify a license for the given component during the scan and therefore set the *I don't know* license value.  
  - The inventory item has multiple possible disjunctive licenses (for example, “GPLV2 or MIT”). However, the scan could find no evidence of the desired selected license and therefore set the *I don't know* license value.  
  - The inventory item has multiple possible conjunctive licenses (for example, “GPLv2 and MIT”). However, since Code Insight currently supports only a single selected license, the scan automatically set the *I don't know* value for the inventory item.  
  
By default, this option is *not* selected, allowing the auto-publication of inventory with undetermined licenses.  

The option is available only if **Auto-publish system-created inventory items meeting this minimum Confidence level** is selected.  

| **Mark associated files as reviewed** | Select this option to automatically mark the files associated with each auto-published inventory item as “reviewed”. (By default, the option is selected.)  

This option is available only if **Auto-publish system-created inventory items meeting this minimum Confidence level** is selected.  


Edit Project: Review and Remediation Settings Tab

The **Review and Remediation Settings** tab on the **Edit Project** dialog enables you to overwrite default settings that configure the automation of the review, remediation, and status notification processes for published inventory in your project. These settings, which work in conjunction with the set of policies in the project’s policy profile, are used to set up the following in your project:

- The policy profile to associate with the project. The policies in the selected profile work in conjunction with the review, remediation, and notification configuration defined on this tab.

### Table 8-18 • Edit Project: Scan Settings tab (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Codebase for Scan Server</td>
<td>These settings enable you to limit which directories are scanned in your codebase.</td>
</tr>
<tr>
<td>Path</td>
<td>From the interactive directory tree representing the project’s codebase on the Scan Server, select the checkbox next to one or more top-level directories that you want to scan. To scan only specific subdirectories in a top-level directory, drill down in that directory and select the desired subdirectories.</td>
</tr>
<tr>
<td>Add</td>
<td>The pane showing the path for each directory currently selected for the scan. As a quick method for removing a given directory from the scan without having to drill down in the tree to locate it, simply click the X next to the directory in this pane. If the Scan Server is down, this pane is blank.</td>
</tr>
<tr>
<td>Path</td>
<td>These buttons control whether you save your updates to scan settings.</td>
</tr>
<tr>
<td>Save</td>
<td>Click this button to save your edits to the scan settings and return to the <strong>Summary</strong> tab.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Click this button to return to the <strong>Summary</strong> tab without saving your edits.</td>
</tr>
</tbody>
</table>

**See Also**
- Editing the Project Definition and General Settings
- Updating Scan Settings for a Project
- Automatically Publishing Inventory
• Automatic creation of manual review tasks for inventory items not reviewed by policy during publication performed as part of a scan.

• Automatic assignment of review tasks to the default legal or security contact that you specify.

• Automatic creation of remediation tasks and associated external work items for inventory that is rejected either automatically by policy or during manual publication by an analyst.

• Automatic assignment of remediation tasks to the default engineering contact that you specify.

• Automatic rejection of published inventory impacted by new vulnerabilities detected in the latest scan or Electronic Update.

• The automatic generation of email notifications that alert the Project Owner of rejected or non-reviewed published inventory items that need attention.

See the following field descriptions for more information.

Table 8-19 • Edit Project: Review and Remediation Settings tab

<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated Review Options</td>
<td>Select policy profile you want to associate with your project. The policy profile contains a set of policies that use vulnerability scores and severities, license types, and component versions as criteria to automatically reject or approve inventory items during a codebase scan (or post-scan). For more information about policy profiles in general, see Managing Policy Profiles in the “Using FlexNet Code Insight” chapter.</td>
</tr>
</tbody>
</table>
| Automatically reject inventory items impacted by a new vulnerability that violates your policy | Determine what action the system should take for published inventory affected by a new security vulnerability discovered during a post-publication scan or an Electronic Update. The selected action applies to both non-reviewed and previously approved inventory items on the Project Inventory tab.  
- Select this checkbox to automatically reject those project inventory items impacted by a new security vulnerability only if this vulnerability has a CVSS score or severity greater than the thresholds configured as policy for the Code Insight project. For each inventory item rejected due to a new security vulnerability, the icon and a tip are added to indicate the status change and its reason. If a new vulnerability does not exceed policy thresholds, the current status of the inventory item is not affected.  
- Leave the checkbox unselected to retain the current status of inventory items impacted by the new vulnerability. For information about setting policies that define CVSS-score and severity thresholds used to reject or approve inventory items automatically, see Policy Page and Policy Details Page. For information about associating these policies with a project, see Managing Policy Profiles. |
**Table 8-19 • Edit Project: Review and Remediation Settings tab (cont.)**

<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Manual Review Options                              | Determine what action should be triggered for those inventory items that are not affected by policy (and therefore have a Not Reviewed status) during the publication of inventory either as part of a scan or manually by a user:  
  - do nothing — Simply show the status of the inventory item as Not Reviewed on the Project Inventory tab.  
  - send an email notification to the project owner — Automatically send an email to the Project Owner, stating the need for a manual review of the item. The value for Select the minimum priority... (described in the next table entry) affects this option.  
  - automatically create a manual review task — Automatically create a manual review task assigned to the default security or legal contact, and send an email, notifying the contact about the assigned task. (Information about managing such a task to track the progress of a manual review is found in Creating Inventory from the Project Inventory Tab in the “Using FlexNet Code Insight” chapter.) The value for Select the minimum priority... (described in the next table entry) affects this option. |
| Select the minimum priority to perform the action selected above | (Enabled when an option other than do nothing is selected for the previous field.) Select the minimum inventory priority (P1, P2, P3, or P4) to which the value for the previous field applies.  
  For example, if the previous field is set to send an email notification to the project owner and minimum priority is set to P3, then the email notification will be sent for only those non-reviewed inventory items with a P1, P2, or P3 priority. No email notification will be sent for P4 inventory items. |

Note • This option has no effect on the do nothing value.
What type of manual reviews will be performed on this project?

Determine the type of manual review tasks to be generated:

- **Legal Only**—Review tasks are generated for those non-reviewed inventory items that meet no policy criteria. The tasks are automatically assigned to the default Legal reviewer.

- **Security Only**—Review tasks are generated for only those non-reviewed inventory items that have security vulnerabilities. The tasks are automatically assigned to the default Security reviewer.

- **both Legal and Security**—Review tasks are generated for all non-reviewed inventory items meeting no policy criteria and are assigned to the default Legal reviewer. Additionally, review tasks are generated for those non-reviewed inventory tasks associated with security vulnerabilities and are assigned to the default Security reviewer.

With this value, a single inventory item might have both a legal review task and security review task generated. However, if the default reviewers are the same user, a single task is created, describing the requirement for both a legal and security manual review.

Select reviewers for this project

If desired, designate a new default Legal reviewer or Security reviewer to which to assign manual review tasks.

Then, depending on the type of manual review selected for the project (see the What type of manual reviews will be performed... option described previously), Code Insight determines which reviewer (Legal or Security) is assigned the task and then notified of the task by email. The reviewer can then manage the task accordingly, possibly reassigning it to another user. For details about managing and reassigning tasks, see Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.

To select a new reviewer, click Change User next to the name of the current Legal reviewer or Security reviewer assignee, select a user from the Select new...contact dialog, and click Apply.

When a new default reviewer is selected, that user is automatically given the role of project “reviewer” should the user not currently have this role. However, if the current reviewer reassigns a specific task to another user, the “reviewer” role is not automatically assigned to that user.
Chapter 8  Pages and Panels
Edit Project: Review and Remediation Settings Tab

Table 8-19  Edit Project: Review and Remediation Settings tab (cont.)

<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What should happen if inventory items are rejected?</strong></td>
<td>Determine what action should be triggered for those inventory items that are automatically rejected by policy during the publication of inventory either as part of a scan or manually by a user:</td>
</tr>
<tr>
<td>• do nothing</td>
<td>Simply show the status of the inventory item as Reject on the Project Inventory tab.</td>
</tr>
<tr>
<td>• send an email notification to the project owner</td>
<td>Automatically send an email to the Project Owner, stating the need for remediation work on the inventory item.</td>
</tr>
<tr>
<td>• automatically create a remediation task</td>
<td>Automatically create a remediation task assigned to the default development contact (see the Assignee for remediation work option) and send an email, notifying the contact about the assigned task. (Information about managing such a task to track the remediation progress is found in Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.)</td>
</tr>
<tr>
<td>• automatically create a remediation task and an external work item</td>
<td>Automatically do the following:</td>
</tr>
<tr>
<td></td>
<td>• Create a remediation task assigned to the default development contact (see the Assignee for remediation work option) and send an email, notifying the contact about the assigned task. (Information about managing such a task to track the remediation progress is found in Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.)</td>
</tr>
<tr>
<td></td>
<td>• Associate a work item with the task, creating the work item in an Application Lifecycle Management (ALM) system (such as an issue in Jira). The work item is created and assigned using the settings defined for the ALM instance to which the Code Insight project is associated. For more information about configuring an ALM instance for the project, see ALM Settings in the “Using FlexNet Code Insight” chapter.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assignee for remediation work</th>
<th>If desired, designate a new default development contact to which to assign remediation tasks.</th>
</tr>
</thead>
<tbody>
<tr>
<td>This contact can then manage the task</td>
<td>If desired, designate a new default development contact to which to assign remediation tasks. For example, reassigning it to another user or manually creating an external work item and assigning it to someone on the development team. For details about managing and reassigning tasks, see Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.</td>
</tr>
<tr>
<td>To select a new contact, click Change User next to the name of the current assignee, select a user from the Select new...contact dialog, and click Apply.</td>
<td>To select a new contact, click Change User next to the name of the current assignee, select a user from the Select new...contact dialog, and click Apply.</td>
</tr>
</tbody>
</table>
See Also
Editing the Project Definition and General Settings
Policy Page
Policy Details Page
Project Defaults Tab
Managing Policy Profiles
Creating Inventory from the Project Inventory Tab
Creating and Viewing External Work Items for a Project Inventory Task
Updating Inventory Review and Remediation Settings for a Project
ALM Settings

Edit (Default) Project Users Page

The Edit Project Users page, accessed from the Manage Project menu on the Summary tab for a specific project, is used to assign Code Insight users to various roles for the project.

The Edit Default Project Users page, available from the Project Defaults tab on the Administration page, is used to set project role assignments that default for any new project created (but which can then be edited at the project level on the Edit Project Users page).

For a description of the project roles and more information about the procedures used to manage them on the Edit Project Users page, see Assigning Project Roles to Users. (These same procedures basically apply to the Edit Default Project Users page.) Additionally, for a description of the permissions enabled for each project role, see the appendix FlexNet Code Insight User Roles and Permissions.

The following describes the fields on the Edit Project Users and Edit Default Project Users page:

Table 8-20 • Edit (Default) Project Users page

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Users</td>
<td>The list of all users defined for your FlexNet Code Insight system. From this list, you select the users to which you want to assign project roles.</td>
</tr>
<tr>
<td>Add User</td>
<td>Select one or more users in the Select Users pane, and then select the appropriate option—Add to Analysts, Add to Reviewers, or Add to Observers—from the Add User dropdown to add the users to the desired “role” pane. This procedure is an alternative to dragging and dropping users to the appropriate “role” pane.</td>
</tr>
<tr>
<td>Search</td>
<td>Enter a full or partial user name to search for a user in the system.</td>
</tr>
<tr>
<td>Analysts</td>
<td>The pane listing users who are currently assigned to the Analyst role. To assign additional users to this role, drag and drop one or more users from the Select Users list to this pane. (Alternatively, select Add to Analysts from the Add User dropdown to add the selected users to the pane.) To remove a user from this role, click ✗ next to the user name in the pane.</td>
</tr>
</tbody>
</table>
Table 8-20 • Edit (Default) Project Users page (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reviewers</td>
<td>The pane listing users who are currently assigned to the Reviewer role. To assign additional users to this role, drag and drop one or more users from the Select Users list to this pane. (Alternatively, select Add to Reviewers from the Add User dropdown to add the selected users to the pane.) To remove a user from this role, click ( \times ) next to the user name in the pane.</td>
</tr>
<tr>
<td>Observers</td>
<td>The pane listing users who are currently assigned to the Observer role. To assign additional users to this role, drag and drop one or more users from the Select Users list to this pane. (Alternatively, select Add to Observers from the Add User dropdown to add the selected users to the pane.) To remove a user from this role, click ( \times ) next to the user name in the pane.</td>
</tr>
</tbody>
</table>

**Note** • On the Edit Project Users page, the Observers pane is visible only for private projects. On the Edit Default Project Users page, this pane is always visible, enabling you to assign observers that will default for any private project that might be created. For more information, see Creating a Private Project.

Close

Click this button to save your changes.

See Also

Assigning Project Roles to Users

Scan History Dialog

The Scan History dialog displays a list of previous scans that have been performed on the selected project. The dialog contains the following fields:

Table 8-21 • Scan History dialog

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click</td>
<td>Click to view messages about the scan. If no messages were generated during the scan, the message field will be blank.</td>
</tr>
<tr>
<td>Scheduled On</td>
<td>The date and time that the scan was scheduled.</td>
</tr>
<tr>
<td>Started On</td>
<td>The date and time that the scan was started.</td>
</tr>
<tr>
<td>Completed On</td>
<td>The date and time that the scan completed.</td>
</tr>
<tr>
<td>Duration</td>
<td>The amount of time the scan took.</td>
</tr>
</tbody>
</table>
Select a New Project Owner Page

The Select a new project owner page is where you can change the owner of a selected project. The page contains the following fields:

Table 8-22 • Select a New Project Owner page

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of Users</td>
<td>The names of all the users in the system are listed in this field. Highlight a name and click Apply to change the project’s owner.</td>
</tr>
<tr>
<td>Apply</td>
<td>Click this button to assign the selected owner to the project.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Click this button to cancel changes without saving.</td>
</tr>
</tbody>
</table>

See Also
Analyzing (Auditing) Scan Results
The **Analysis Workbench** is where you can interact with the items in your project inventory. The **Analysis Workbench** has the following fields:

---

**Table 8-23 • Analysis Workbench**

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legend</strong></td>
<td>A color-coded and hyperlinked guide to the files and inventory in your scanned codebase:</td>
</tr>
<tr>
<td></td>
<td>• <strong>New Evidence</strong>: Click this link to filter the search results to display only files that are new since the last scan. If only a single scan took place, all files with evidence are displayed in the <strong>Files Search Results</strong> pane.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reviewed</strong>: Click this link to display files in the <strong>File Search Results</strong> pane that have been reviewed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Exact</strong>: Click this link to display files in the <strong>File Search Results</strong> pane that are exact matches.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Copyrights</strong>: Click this link to display files in the <strong>File Search Results</strong> pane that contain copyright text.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Email/URLS</strong>: Click this link to display files in the <strong>File Search Results</strong> pane that contain email addresses and URLs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Licenses</strong>: Click this link to display files in the <strong>File Search Results</strong> pane that contain licenses.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Search Terms</strong>: Click this link to display files in the <strong>File Search Results</strong> pane that match default search terms.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Source</strong>: Click this link to display files in the <strong>File Search Results</strong> pane that match</td>
</tr>
</tbody>
</table>

---

**Codebase Files Panel**

**Enter Path**

To display codebase files in the **Analysis Workbench**, enter a directory path that contains the codebase files you are interested in or click the browse button to navigate to the path. If no path is entered, FlexNet Code Insight defaults to the path that was specified during the scan.

**Path/Folder/File Tree**

A tree displaying the path where your codebase files are located. Unless you chose a different path in the Enter Path field, this is the location of your codebase that you specified when you scheduled the scan.

---

**File Details**

---

**Note** • Some panes do not contain data until you choose a file in another pane.
**File Search Results Pane**

The **File Search Results** pane displays the results of your file search. The **File Search Results** pane has the following fields.

---

**Note**  • Some panes do not contain data until you choose a file in another pane.
The **Advanced File Search** dialog allows you to select a standard search, create your own search, or delete an existing search. The dialog has the following fields:

### Table 8-24 • File Search Results pane

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click to refresh the search.</td>
<td></td>
</tr>
<tr>
<td><strong>Advanced Search</strong></td>
<td>Click to open the <strong>Advanced File Search</strong> dialog on which you can choose a standard search or add a new one.</td>
</tr>
<tr>
<td><strong>Clear Search Results</strong></td>
<td>Click to clear the results of the search.</td>
</tr>
<tr>
<td><strong>Current Search</strong></td>
<td>Displays the criteria for the current search.</td>
</tr>
<tr>
<td><strong>Results Tree</strong></td>
<td>The results of the current search.</td>
</tr>
</tbody>
</table>

### Advanced File Search Dialog

The **Advanced File Search** dialog allows you to select a standard search, create your own search, or delete an existing search. The dialog has the following fields:

### Table 8-25 • Advanced File Search dialog

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add New</strong></td>
<td>Click this button to access the <strong>Advanced File Search Add</strong> dialog.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The name of the search. For example, <em>Files not in inventory</em>.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>A short description of the search. For example, <em>Files not associated with inventory items</em>.</td>
</tr>
<tr>
<td><strong>X</strong></td>
<td>Click to delete a search.</td>
</tr>
<tr>
<td><strong>Search</strong></td>
<td>Click to execute the selected search.</td>
</tr>
<tr>
<td><strong>Close</strong></td>
<td>Click to close the Search Files dialog without searching.</td>
</tr>
</tbody>
</table>
Advanced File Search Add Dialog

The Advanced File Search Add dialog allows you to select a standard search, create your own search, or delete an existing search. The dialog has the following fields:

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the search. For example, <em>Files not in inventory.</em></td>
</tr>
<tr>
<td>Description</td>
<td>A short description of the search. For example, <em>Files not associated with inventory items.</em></td>
</tr>
<tr>
<td>Criteria</td>
<td>Click the dropdown menu and select search criteria. To add more criteria, click <em>Add Criteria</em> and select another item from the dropdown menu. When you select search criteria from the dropdown menu, a boolean operator appears in the center dropdown, and a new dropdown appears from which you must select a criteria value to search the selected field for.</td>
</tr>
<tr>
<td>Add Criteria Group</td>
<td>Click to add a group of criteria.</td>
</tr>
<tr>
<td>Save</td>
<td>Click to save the new search.</td>
</tr>
<tr>
<td>Save and Search</td>
<td>Click to execute the new search without saving the search for future use.</td>
</tr>
<tr>
<td>Search without saving</td>
<td>Click to execute the new search without saving the search for future use.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Click to close the <em>Search Files</em> dialog without searching.</td>
</tr>
</tbody>
</table>

Inventory Details Pane in Analysis Workbench

The Inventory Details pane in the Analysis Workbench contains a sub-tab for each inventory item you have opened from the Inventory Items pane. Each sub-tab contains the following fields describing a given inventory item:

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Header information]</td>
<td>The Inventory Details pane header shows buttons that enable you take actions on the inventory item and lists attributes about the item and its associated component.</td>
</tr>
</tbody>
</table>
### Table 8-27 • Inventory Details pane (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recall</td>
<td>Click to recall (remove) a published inventory item from <strong>Inventory Items</strong> list if it does not fit the criteria for inclusion. The selected items are removed from the <strong>Project Inventory</strong> view and are only visible in the <strong>Analysis Workbench</strong>.</td>
</tr>
<tr>
<td>Create Custom Rule</td>
<td>(Available when inventory <strong>Type</strong> is <strong>Component</strong>) Click to open the <strong>Custom Detection Rule</strong> dialog to define a new detection rule for codebase files that are associated with a third-party component but not associated with inventory. For details, see Managing Custom Detection Rules.</td>
</tr>
<tr>
<td>Save</td>
<td>Click to save any changes you have made to the inventory details.</td>
</tr>
<tr>
<td>Close</td>
<td>Click to close the <strong>Inventory Details</strong> pane without saving changes. You are asked to save changes before the actual closure.</td>
</tr>
<tr>
<td>Review Status</td>
<td>The status of the inventory item:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Approved</strong>—The item is approved for use in the software project.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not Reviewed</strong>—The item has not been reviewed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Draft</strong>—This item is in the process of being reviewed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Rejected</strong>—The item is not approved for use in the software project. Instead, the item needs further review and remediation before being used in the software project.</td>
</tr>
<tr>
<td>Alerts</td>
<td>Notifies you whether or not security alerts exist for this item. If alerts exist, click the <strong>Open Alerts</strong> or <strong>Closed Alerts</strong> link to view their details. If no alerts exist, <strong>None</strong> is displayed. You can access the <strong>Alerts</strong> dialog from this pane to change the status or priority of an alert. For more information, see Managing Security Vulnerability Alerts.</td>
</tr>
<tr>
<td>Priority</td>
<td>A dropdown list showing the priority level given to this inventory item by the system, with P1 as the highest priority and P4 as the lowest. You can change the priority for this inventory item by selecting a different priority from the dropdown list and clicking <strong>Save</strong>. For more information about priorities, see Inventory Priority.</td>
</tr>
</tbody>
</table>
### Table 8-27 • Inventory Details pane (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Vulnerabilities** | A bar graph showing the count of known vulnerabilities by severity color for the inventory item. Click the graph to view the list of vulnerabilities and their details. For details about the graph and vulnerabilities in general, see Security Vulnerabilities Associated with Inventory.  
If no vulnerabilities have been found for the inventory item, the value No is displayed in place of the graph. (In Analysis Workbench, if the Type value for the inventory item is Work in Progress or License Only, the value N/A is displayed.) |
| **Created By** | The name of the person or process that created the inventory item.                                                                                                                                           |
| **Confidence** | A simple three-segment graph representing the Confidence level (High, Medium, or Low) of the inventory item. The Confidence level is the measure of the strength of the discovery technique used to generate the inventory item. The graph shows three shaded segments for High confidence, two for Medium, and one for Low.  
For more information about the Confidence levels, see Inventory Confidence in the “Using FlexNet Code Insight” chapter. |
| **Created On** | The date that the inventory item was created.                                                                                                                                                                |
| **Updated On** | The date that the inventory item was updated. If the item has not been updated since the creation date, the date shown here will be the same as the Created On date.                                             |
| **[Inventory details]** | The following attributes describe the inventory item. You can update these attributes as needed from this pane. For details, see Editing Inventory from the Analysis Workbench or Creating an Inventory Item from the Analysis Workbench. |
| **Name**       | The name of the inventory item.                                                                                                                                                                             |
| **Type**       | The type of finding of this item:                                                                                                                                                                           |
|                | - **Work in Progress**—A set of files with something in common. The work in progress will become a component or license only via manual audit work.                                                            |
|                | - **Component**—Files from a specific component version with known or unknown license. If this type is selected, the Lookup Component button becomes active, enabling you to select a new component instance for the inventory item. |
|                | - **License Only**—Files under a specific license without a known component.                                                                                                                                 |
### Table 8-27 • Inventory Details pane (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Component</strong></td>
<td>The name of the component. Click 🔍 to view publicly available information about the component; or click 🔄 to select a new version (or license) for the inventory item.</td>
</tr>
<tr>
<td><strong>License</strong></td>
<td>The name of the license associated with this component. Click 🔍 to view additional information about the license; or click 🔄 to select a new license (or version) for the inventory item.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>A description of the inventory item. You can update the description as needed.</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td>The URL of the license for this inventory item. You can update the URL as needed.</td>
</tr>
<tr>
<td><strong>Disclosed</strong></td>
<td>The <strong>Yes</strong> or <strong>No</strong> option indicating whether the third-party component or artifact represented by the inventory item known third-party dependency in your code before it was discovered by the scan or you. This field is used most often by analysts to denote information about the state of the inventory item.</td>
</tr>
</tbody>
</table>
| **Workflow URL** | The URL (or a text reference such as a Jira issue number) that points to the request data pertaining to this inventory item as found in your site's external workflow system.  
When you view this value on the **Inventory Details** tab in **Project Inventory**, the URL displays as a link (labeled as **View Associated Request**), enabling the reviewer to easily access to the workflow data that tracks the status of open tasks for the inventory item.  
A text reference entered here is not converted to a link on the **Inventory Details** tab, but it still provides direction in locating the appropriate data in the workflow system.  
The value is **None** if you enter no URL or reference.  
Additionally, when you view the **Inventory Details** tab in **Project Inventory**, an ✂️ icon will be displayed next to the URL if additional request-related details are available for the inventory item. The reviewer can then click the icon for a quick review of pertinent details about the request without having to access the workflow system. |


Table 8-27 • Inventory Details pane (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usage tab</td>
<td>The <strong>Usage</strong> tab provides details on how your product uses the OSS or third-party software. You can update this information as needed from this pane when editing an existing inventory item or creating a new one. See Viewing or Editing Inventory Usage Information from Analysis Workbench.</td>
</tr>
<tr>
<td>Distribution Type</td>
<td>The option indicating how the inventory item is distributed:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Internal</strong>—Internally only (such as test framework that might be included in the codebase but is not distributed with the product).</td>
</tr>
<tr>
<td></td>
<td>• <strong>External</strong>—Externally with the product, shipped to customers (outside of your organization, including a private cloud deployment at the customer’s site)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hosted</strong>—Hosted in your company’s data center (such as a SAAS application).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unknown</strong>—Unknown distribution type.</td>
</tr>
<tr>
<td>Part of Product</td>
<td>The <strong>Yes</strong>, <strong>No</strong>, or <strong>unknown</strong> option indicating whether the item is part of the core product or an infrastructure piece such as a build or test tool. This can affect whether third-party notices are required for this item.</td>
</tr>
<tr>
<td>Linking</td>
<td>The option indicating whether the libraries are statically linked (included in the materials), dynamically linked (brought in at runtime), or not linked at all. The <strong>Unknown</strong> value indicates that linking status is not known. Linking can affect license priority and obligations.</td>
</tr>
<tr>
<td>Modified</td>
<td>The <strong>Yes</strong>, <strong>No</strong>, or <strong>Unknown</strong> option indicating whether a project contributor, such as a developer, has modified the software from its original form. Modification can be an important factor for determining license obligations and distribution requirements that are governed by a specific license.</td>
</tr>
<tr>
<td>Encryption</td>
<td>The <strong>Yes</strong>, <strong>No</strong>, or <strong>Unknown</strong> option indicating whether the component provides the encryption capabilities used in the product. Encryption can affect export controls.</td>
</tr>
</tbody>
</table>
Chapter 8  Pages and Panels

Inventory Details Pane in Analysis Workbench

Table 8-27 • Inventory Details pane (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes tab</td>
<td>The Notes tab provides information about the automated and manual analysis of codebase as it relates to an inventory item.</td>
</tr>
<tr>
<td>Detection Notes</td>
<td>System notes that can specify the following:</td>
</tr>
<tr>
<td></td>
<td>• The automated detection technique that was used to locate the component</td>
</tr>
<tr>
<td></td>
<td>• License information in the case that the license has changed from one version to another or if the component has multiple licenses</td>
</tr>
<tr>
<td></td>
<td>• Attributes extracted from a POM or manifest file containing project and configuration details</td>
</tr>
<tr>
<td>Audit Notes</td>
<td>Any notes added to the inventory item by the auditor or reviewer, based on findings during the analysis. You can edit these notes as needed from this pane when editing an existing inventory item or creating a new one. See Viewing and Updating Detection and Auditing Notes in Analysis Workbench.</td>
</tr>
<tr>
<td>Associated Files tab</td>
<td>Click this tab to view a list of the files that are part of the inventory for this project. The file entry shows the icons representing the types of evidence found in the file (see Using the Filter Legend Options to Filter the Codebase). A check mark indicates whether the file has been reviewed. If necessary, click the X to disassociate the file from the inventory item.</td>
</tr>
<tr>
<td>Notices Text tab</td>
<td>The Notices Text tab is used to finalize the exact content to include in the Notices report. You can edit the notices content as needed from this pane when editing an existing inventory item or creating a new one. For more information, see Finalizing the Notices Text for the Notices Report.</td>
</tr>
<tr>
<td>As-Found License Text</td>
<td>The As-Found License Text field shows the license text or license references found in the scanned codebase. You cannot edit this field, but you can click Copy to Notices Text to copy the text to the Notices Text field. If content already exists in the Notices Text field, you can choose either to append the As-Found License Text content to the existing notices content or to replace the existing notices content.</td>
</tr>
</tbody>
</table>
Evidence Details Pane

The Evidence Details pane provides details about the inventory, component, and the files in the inventory. The pane has the following fields:

Table 8-28 • Evident Details pane

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand All/Collapse All</td>
<td>Click to toggle between expanded and collapsed display.</td>
</tr>
<tr>
<td>Search field</td>
<td>Enter search criteria.</td>
</tr>
<tr>
<td>Tree view</td>
<td>Click to change the display to a tree view.</td>
</tr>
<tr>
<td>List view</td>
<td>Click to change the display to a list view.</td>
</tr>
<tr>
<td>Select Evidence Types</td>
<td>Click to select evidence types to display</td>
</tr>
</tbody>
</table>

Project Inventory Review Page

The Project Inventory Review page lets you search project inventory. Once you locate and select the project inventory item, its details display in the Project Inventory Details Pane.
The **Project Inventory Review** page has the following fields:

**Table 8-29 • Project Inventory Review page**

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Items (x)</td>
<td>The title of this pane includes the number of inventory items displayed in the list below.</td>
</tr>
<tr>
<td>Search type</td>
<td>From the dropdown list, select the type of search to perform:</td>
</tr>
<tr>
<td></td>
<td>• Inventory Name</td>
</tr>
<tr>
<td></td>
<td>• Security Vulnerability</td>
</tr>
<tr>
<td></td>
<td>• Inventory with Vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>• Inventory with Open Alerts</td>
</tr>
<tr>
<td>Search criteria</td>
<td>The prompt for this field changes based upon your selection in the <strong>Search type</strong> field:</td>
</tr>
<tr>
<td></td>
<td>• If you select <strong>Inventory Name</strong> in the <strong>Search type</strong> field, you must enter a full or partial name to search for.</td>
</tr>
<tr>
<td></td>
<td>• If you select <strong>Security Vulnerability</strong> in the <strong>Search type</strong> field, you must enter a valid vulnerability ID to search for.</td>
</tr>
<tr>
<td></td>
<td>• If you select <strong>Inventory with Vulnerabilities</strong> in the <strong>Search type</strong> field, the list will automatically display the inventory items that meet your criteria.</td>
</tr>
<tr>
<td></td>
<td>• If you select <strong>Inventory with Open Alerts</strong> in the <strong>Search type</strong> field, the list will automatically display the inventory items that meet your criteria.</td>
</tr>
</tbody>
</table>

**See Also**

*Project Inventory Details Pane*
Project Inventory Details Pane

The Project Inventory Details pane is populated with the details for the inventory item currently selected in Inventory Items list on the Project Inventory tab for the current project. The pane contains the following information.

Table 8-30 • Project Inventory Details pane

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Header information]</td>
<td>The header on the Project Inventory Details pane shows buttons that enable you take actions on the inventory item and lists attributes about the item and its associated component.</td>
</tr>
<tr>
<td>Recall Item</td>
<td>Click to recall (remove) a published inventory item from Inventory Items list if it does not fit the criteria for inclusion. The selected items are removed from the Project Inventory view and are only visible in the Analysis Workbench.</td>
</tr>
<tr>
<td>Edit Item</td>
<td>Click to open the Edit Inventory dialog where you can update inventory attributes. See for Editing Inventory from the Project Inventory Tab details.</td>
</tr>
<tr>
<td>Previous Item/Next Item</td>
<td>Show the details for the previous or next inventory item in the Inventory Items list.</td>
</tr>
<tr>
<td>Confidence</td>
<td>A simple three-segment graph representing the Confidence level (High, Medium, or Low) of the inventory item. The Confidence level is the measure of the strength of the discovery technique used to generate the inventory item. The graph shows three shaded segments for High confidence, two for Medium, and one for Low. For more information about the Confidence levels, see Inventory Confidence in the “Using FlexNet Code Insight” chapter.</td>
</tr>
<tr>
<td>Encryption</td>
<td>The Yes, No, or N/A value indicating whether the component associated with the inventory item provides the encryption capabilities used in your product. Encryption can affect export controls. This attribute can be updated on the Edit Inventory dialog (see Editing Inventory from the Project Inventory Tab).</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>A bar graph showing the count of known vulnerabilities by severity color for the component associated with the inventory item. Click the graph to view the list of vulnerabilities and their details. For details about the graph and vulnerabilities in general, see Security Vulnerabilities Associated with Inventory. If no vulnerabilities have been found for the inventory item, the value No is displayed in place of the graph.</td>
</tr>
</tbody>
</table>
### Table 8-30 • Project Inventory Details pane (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>A dropdown list showing the priority level given to this inventory item by the system, with P1 as the highest priority and P4 as the lowest. You can change the priority for this inventory item by selecting a different priority from the dropdown list and clicking <strong>Save</strong>. For more information about priorities, see <strong>Inventory Priority</strong>.</td>
</tr>
</tbody>
</table>

### Status

The status of the inventory item:

- **Approved**—The item is approved for use in the software project.
- **Not Reviewed**—The item has not been reviewed.
- **Draft**—This item is in the process of being reviewed.
- **Rejected**—The item is not approved for use in the software project. Instead, the item needs further review and remediation before being used in the software project.

### Inventory Details tab

The **Inventory Details** tab lists attributes of the inventory item.

<table>
<thead>
<tr>
<th>Name</th>
<th>The name of the inventory item. This attribute can be updated on the <strong>Edit Inventory</strong> dialog (see <strong>Editing Inventory from the Project Inventory Tab</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A description of the inventory item. This attribute can be updated on the <strong>Edit Inventory</strong> dialog (see <strong>Editing Inventory from the Project Inventory Tab</strong>).</td>
</tr>
<tr>
<td>URL</td>
<td>The URL of the license for this inventory item. You can click the URL link to open the component website. This attribute can be updated on the <strong>Edit Inventory</strong> dialog (see <strong>Editing Inventory from the Project Inventory Tab</strong>).</td>
</tr>
</tbody>
</table>
Table 8-30 • Project Inventory Details pane (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclosed</td>
<td>The Yes or No option indicating whether the third-party component or artifact represented by the inventory item known third-party dependency in your code before it was discovered by the scan or you. This field is used most often by analysts to denote information about the state of the inventory item. This attribute can be updated on the Edit Inventory dialog (see Editing Inventory from the Project Inventory Tab).</td>
</tr>
<tr>
<td>Modified</td>
<td>The Yes, No, or Unknown option indicating whether a project contributor, such as a developer, has modified the software from its original form. Modification can be an important factor for determining license obligations and distribution requirements that are governed by a specific license. This attribute can be updated on the Edit Inventory dialog (see Editing Inventory from the Project Inventory Tab).</td>
</tr>
<tr>
<td>Alerts</td>
<td>Notifies you whether or not security vulnerability alerts exist for this item. If alerts exist, click the x Open Alerts or x Closed Alerts link to view their details. If no alerts exist, None is displayed. You can open the Alerts dialog from this pane to change the status or priority of an alert. For more information, see Managing Security Vulnerability Alerts.</td>
</tr>
<tr>
<td>Tasks</td>
<td>The number of open or closed tasks for this inventory item. Click the x Closed Tasks or x Open Tasks link to view and update the tasks. If no tasks are associated with this inventory item, None is displayed. You can access the Tasks dialogs from this pane to create, edit, and close tasks. See for Creating and Managing Tasks for Project Inventory details.</td>
</tr>
</tbody>
</table>
The URL link or a plain text reference (such as a Jira issue number) to request data pertaining to this inventory item in your site’s external workflow system. The link enables the reviewer to easily access the workflow data that tracks the status of open tasks for the inventory item. (The plain text reference still helps the reviewer locate the appropriate data in the workflow system.)

You can define this attribute when you edit or manually create an inventory item from Analysis Workbench or the Project Inventory tab.

If no URL or reference has been defined, the value is None.

If additional request-related details are available for this inventory item, the icon is displayed next to the URL. Click the icon to open the Workflow Request Details window for a quick review of pertinent details about the request without having to access the workflow system.

Note • These details come from the specific external workflow system associated with your site. The details can vary based on your workflow system.

### Component Details tab

The Component Details tab lists attributes of the OSS or third-party component.

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow URL</td>
<td>The URL link or a plain text reference (such as a Jira issue number) to request data pertaining to this inventory item in your site’s external workflow system. The link enables the reviewer to easily access the workflow data that tracks the status of open tasks for the inventory item. (The plain text reference still helps the reviewer locate the appropriate data in the workflow system.) You can define this attribute when you edit or manually create an inventory item from Analysis Workbench or the Project Inventory tab. If no URL or reference has been defined, the value is None. If additional request-related details are available for this inventory item, the icon is displayed next to the URL. Click the icon to open the Workflow Request Details window for a quick review of pertinent details about the request without having to access the workflow system. Note • These details come from the specific external workflow system associated with your site. The details can vary based on your workflow system.</td>
</tr>
<tr>
<td>Component</td>
<td>The name of the component. You can switch to a different component from the Edit Inventory dialog (see Editing Inventory from the Project Inventory Tab).</td>
</tr>
<tr>
<td>Version</td>
<td>The component version. You can edit the component version from the Edit Inventory dialog (see Editing Inventory from the Project Inventory Tab).</td>
</tr>
<tr>
<td>Forge</td>
<td>The external repository associated with the component. You can click the forge link to open the forge website.</td>
</tr>
<tr>
<td>Selected License</td>
<td>The name of the license selected for this component. Click to view additional information about the license. See License Details Window. You can switch to a different license from the Edit Inventory dialog (see Editing Inventory from the Project Inventory Tab).</td>
</tr>
<tr>
<td>Possible Licenses</td>
<td>Other licenses that can be associated with the component.</td>
</tr>
</tbody>
</table>
Table 8-30 • Project Inventory Details pane (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Component</td>
<td>The Yes or No value indicating whether the component was user-created.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>A bar graph showing the count of known vulnerabilities by severity color for the component. Click the graph to view the list of vulnerabilities and their details. For details about the graph and vulnerabilities in general, see Security Vulnerabilities Associated with Inventory. If no vulnerabilities have been found for the inventory item, the value No is displayed in place of the graph.</td>
</tr>
<tr>
<td>Encryption</td>
<td>The Yes, No, or N/A value indicating whether the component provides the encryption capabilities used in your product. Encryption can affect export controls. This attribute can be updated on the Edit Inventory dialog (see Editing Inventory from the Project Inventory Tab).</td>
</tr>
</tbody>
</table>

**Notices Text tab**

The Notices Text tab is used to finalize the exact content to include in the Notices report. For more information, see Finalizing the Notices Text for the Notices Report.

<table>
<thead>
<tr>
<th>As-Found License Text</th>
<th>The As-Found License Text field shows the license text or license references found in the scanned codebase. You cannot edit this field, but you can click Copy to Notices Text to copy the text to the Notices Text field. If content already exists in the Notices Text field, you can choose either to append the As-Found License Text content to the existing notices content or to replace the existing notices content.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notices Text</td>
<td>The exact content to include in the Notices report. You can edit any license text previously saved to this field or add your own license text, such as license information for rules that you developed during your manual research on the inventory item. You can also copy the As-Found License Text content to the Notices Text field and modify it as needed. Or you can leave this field empty. Click Save at the top of the field if you make any changes to this field. If you provide information in this field, the Notices report pulls the content of only this field into the report. If this field is empty, the content of the As-Found License Text field is used in the report. If both fields are empty, the report uses the license content from FlexNet Code Insight data library (see License Details from the Code Insight Data Library). For more information, see Finalizing the Notices Text for the Notices Report.</td>
</tr>
</tbody>
</table>


### Notes & Guidance tab

The **Notes & Guidance** tab provides information about the automated and manual analysis of codebase as it relates to an inventory item.

<table>
<thead>
<tr>
<th><strong>Detection Notes</strong></th>
<th>System notes that can specify the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• The automated detection technique that was used to locate the component</td>
</tr>
<tr>
<td></td>
<td>• License information in the case that the license has changed from one version to another or if the component has multiple licenses</td>
</tr>
<tr>
<td></td>
<td>• Attributes extracted from a POM or manifest file containing project and configuration details</td>
</tr>
</tbody>
</table>

| **Audit Notes** | Any notes added to the inventory item by the auditor or reviewer, based on findings during the analysis. |

| **Usage Guidance** | Notes helpful provided by a reviewer to assist other reviewers or to provide guidance to software engineers assigned tasks to fix or modify the use of the OSS or third-party software in the product code. |

### Usage tab

The **Usage** tab provides details on how your product uses the OSS or third-party software. These attributes can be updated on the **Edit Inventory** dialog (see *Editing Inventory from the Project Inventory Tab*).

<table>
<thead>
<tr>
<th><strong>Distribution Type</strong></th>
<th>The option indicating how the inventory item is distributed:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Internal</strong>—Internally only (such as test framework that might be included in the codebase but is not distributed with the product).</td>
</tr>
<tr>
<td></td>
<td>• <strong>External</strong>—Externally with the product, shipped to customers (outside of your organization, including a private cloud deployment at the customer’s site)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hosted</strong>—Hosted in your company’s data center (such as a SAAS application).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unknown</strong>—Unknown distribution type.</td>
</tr>
</tbody>
</table>

| **Part of Product** | The **Yes, No, or unknown** option indicating whether the item is part of the core product or an infrastructure piece such as a build or test tool. This can affect whether third-party notices are required for this item. |

| **Linking** | The option indicating whether the libraries are statically linked (included in the materials), dynamically linked (brought in at runtime), or not linked at all. The **Unknown** value indicates that linking status is not known. |

Linking can affect license priority and obligations.
The Policy page lets you edit, copy, and create policy profiles for use by your projects. See Managing Policy Profiles for more details about policies.

The page has the following fields:

Table 8-31 • Policy page

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy list</strong></td>
<td>The list of current policy profiles in a grid format. Each entry shows the profile name and its description, the user who last updated the profile, and date of the last update for the profile. Select a policy profile to edit or copy.</td>
</tr>
<tr>
<td>• <strong>Edit icon</strong> — Click to edit the selected policy profile. The Policy Details page is opened, showing the profile details.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Copy icon</strong> — Click to copy the selected policy profile. The Policy Details page is opened, showing a new instance of the selected profile. (The selected profile is always saved first.) This new instance has the name Copy of selected_policyProfile_name.</td>
<td></td>
</tr>
<tr>
<td><strong>Add Policy button</strong></td>
<td>Click the Add Policy button to create a new policy profile. The Policy Details page is opened.</td>
</tr>
</tbody>
</table>

See Also
Policy Details Page
License Details Window
Managing Policy Profiles
The **Policy Details** page lets you define or edit a policy profile that can be used to automatically review inventory items when they are published. Inventory items that meet any of the component, license, or security vulnerability criteria in the policy profile can be automatically approved or rejected (or flagged for a manual review) based on the policy definition. The following topics describe this page:

- Field Descriptions
- Impact on Policies When CVSS Version Changes on System

### Policy Fields

The page has the following fields:

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>These fields identify the policy profile you are creating or editing.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the policy profile that you are editing or copying. If you are copying a profile, the name will read Copy of <em>selected_policyProfile</em>, where <em>selected_policyProfile</em> is the name of the profile you selected to copy. To change the name of the profile, type a new name in this field.</td>
</tr>
<tr>
<td>Description</td>
<td>The policy profile description, if it exists. You can edit or add a description.</td>
</tr>
<tr>
<td>Created</td>
<td>(Edit view only) The name of the user who created the policy profile, and the date and time the profile was created. You can click the hyperlinked name to send an email to the user who created the profile.</td>
</tr>
<tr>
<td>Updated</td>
<td>(Edit view only) The name of the user who last updated the policy profile, and the date and time the profile was updated. You can click the hyperlinked name to send an email to the user who updated the profile.</td>
</tr>
</tbody>
</table>
Vulnerabilities  | The following criteria automatically approve or reject inventory items with security vulnerabilities during publication.
--- | ---
Only auto-approve inventory items if there are no associated security vulnerabilities  | Select this checkbox to have Code Insight skip any matching license-based or component policies if the inventory item has any associated security vulnerabilities.
Reject inventory items if any associated security vulnerabilities have a CVSS score above `<score>`  | Select this checkbox to have Code Insight automatically reject any inventory items with any associated security vulnerabilities that have a CVSS score above the value you enter. This policy takes precedence over any other automated approval policy.  

*Note*  | *If the FlexNet Code Insight administrator changes the CVSS version for Code Insight, the value you selected for this field might change. See Impact on Policies When CVSS Version Changes on System for details.*
Reject inventory items if any associated security vulnerabilities have a severity equal to or higher than `<severity level>`  | Select this checkbox to have Code Insight automatically reject any inventory items with any associated security vulnerabilities that have a severity equal to or higher than severity you select. (For information about vulnerability severities, see Security Vulnerabilities Associated with Inventory.) This policy takes precedence over any other automated approval policy.  

*Note*  | *If the FlexNet Code Insight administrator changes the CVSS version for Code Insight, the value you selected for this field might change. See Impact on Policies When CVSS Version Changes on System for details.*
The following fields create policies that automatically approve or reject inventory associated with a given license.

Select a License... (dropdown)  
The dropdown of available licenses on which you can create policies. Select a license, and click Add License to add it to the Licenses policy list.

Licenses (list)  
The list of license policies (in a grid format) currently used by this profile for automatically reviewing inventory items.

- **Name**—The name of the license.
- **Usage Guidance icon**—Click ![icon] to display the **Usage Guidance** dialog, in which you can add or edit text that will help reviewers in reviewing this license.
- **License Details icon**—Click ![icon] to display the **License Details** window for the selected license.
- **Action**—Select one of the following to indicate what status to automatically assign to any inventory item associated with this license:
  - **Approve**
  - **Reject**
  - **No Action** (same as the “Not Reviewed” inventory status, thus requiring a manual review)
- **Delete icon**—Click ![icon] to delete the license from the policy.

### Table 8-32 • Policy Details page (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Licenses</strong></td>
<td>The following fields create policies that automatically approve or reject inventory associated with a given license.</td>
</tr>
<tr>
<td><strong>Select a License... (dropdown)</strong></td>
<td>The dropdown of available licenses on which you can create policies. Select a license, and click <strong>Add License</strong> to add it to the <strong>Licenses</strong> policy list.</td>
</tr>
<tr>
<td><strong>Licenses (list)</strong></td>
<td>The list of license policies (in a grid format) currently used by this profile for automatically reviewing inventory items.</td>
</tr>
</tbody>
</table>

- **Name**—The name of the license.
- **Usage Guidance icon**—Click ![icon] to display the **Usage Guidance** dialog, in which you can add or edit text that will help reviewers in reviewing this license.
- **License Details icon**—Click ![icon] to display the **License Details** window for the selected license.
- **Action**—Select one of the following to indicate what status to automatically assign to any inventory item associated with this license:
  - **Approve**
  - **Reject**
  - **No Action** (same as the “Not Reviewed” inventory status, thus requiring a manual review)
- **Delete icon**—Click ![icon] to delete the license from the policy.
Components

The following fields create a policy that automatically approve or reject inventory based on the component associated with the inventory.

Add Component button

Click this button to select a component on which to create the policy, or create a new component from the Lookup Component window. (See Lookup Component Window for information about how to use this window.) Once you select a component, its entry is added to the Components policy list.

Components (list)
The list of current components and version (in a grid format) currently used by this profile for automatically reviewing inventory items.

- **Name**—The name of the component.
- **Versions**—Select a specific version or a range of versions for the given component. (The Versions from and to drop-down lists are populated with available versions for the component.) Here are some example ways to specify a version or version range:
  - To enter a specific version, select the same version in the Versions from and to fields.
  - To enter an explicit range, select a minimum version in the Versions from field and the maximum version in the to field.
  - To specify any version for the given component, select the wild card * in both Versions from and to fields.
  - To specify any version up to a specific version, enter the wild card * in the Version from field and the maximum version in the to field.
  - To specify any version after a specific version, select the specific version in the Versions from field and the wild card * in the to field.

The unknown option applies to certain components that were collected without a version value. To specifically handle unknown versions, set both Versions from and to fields to unknown.

- **Action**—Select one of the following to indicate what status to automatically assign to inventory items associated with this component-version:
  - Approve
  - Reject
  - No Action (same as the “Not Reviewed” inventory status, thus requiring a manual review)

- **Delete icon**—Click X to delete the component entry from the policy.
Impact on Policies When CVSS Version Changes on System

If the FlexNet administrator changes the CVSS version for FlexNet Code Insight, the following describes the impact on policies related to vulnerabilities.

**When CVSS v2 is switched to CVSS v3.0**

Code Insight makes the following changes:

- If the severity level for the **Reject inventory items if any associated securities vulnerabilities have a severity level equal to or higher than...** field was **Unknown** previously, it is now **None**.

- An additional severity, **Critical**, is available for this same field.

**When CVSS v3.0 is switched to CVSS v2**

Code Insight makes the following changes:

- If the severity level for the **Reject inventory items if any associated securities vulnerabilities have a severity level equal to or higher than...** field was previously **None**, it is now **Unknown**.

- If the severity level for this same field was previously **Critical**, note that this severity is no longer available. To handle the conversion, Code Insight checks to see if a score was previously entered in the **Reject inventory items if any associated security vulnerabilities have a CVSS score above...** field. If a score less than 9 was entered, that value is retained in the field (since the previous **Critical** severity started with the score 9). If a value greater than 9 or no value was entered, the value for this field is now 9.

**See Also**
- Policy Details Page
- License Details Window
- Lookup Component Window
- Managing Policy Profiles

### Custom Detection Rules Tab

The **Custom Detection Rules tab** on the **Custom Data** page lists the custom detection rules currently available for use in codebase scans in your FlexNet Code Insight system. Custom detection rules are user-defined when needed to supplement the internal detection rules used by Automated Analysis to automatically create inventory during a scan. These custom rules are saved to the FlexNet Code Insight data library for global use across projects.
From this page, you can also select to edit a rule or remove a rule from your Code Insight system.

For complete details about custom detection rules, see Managing Custom Detection Rules.

The following describes the columns and actions you can perform from the Custom Detection Rules tab.

Table 8-33 • Custom Detection Rules tab

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Component Name search string</td>
<td>To locate specific custom detection rules, enter a component-name string by which to filter the list of detection rules. The search results show only those rules whose component name contains the search string you provided. (This filter applies to only those custom rules visible in the UI; no call is made to the data library.)</td>
</tr>
<tr>
<td>Create Custom Rule</td>
<td>Click to open the Custom Detection Rule dialog to create a new custom detection rule.</td>
</tr>
</tbody>
</table>

The following columns provide details about each custom detection rule and give you access to actions you can take on the rule.

- **Component**
  - The name of the component on which the custom detection rule is based.
- **Version**
  - The component version.
- **License**
  - The license found in the FlexNet Code Insight data library and associated with the component.
- **URL**
  - The forge URL for the component.

Actions you can perform on the currently selected rule:

- Click to edit the custom detection rule. The Edit Custom Rule dialog is opened.
- Click to delete the custom detection rule from your FlexNet Code Insight system. The rule will no longer be applied during project scans.

See Also

Managing Custom Detection Rules
Custom Detection Rule Dialog
Edit Custom Rule Dialog
Custom Detection Rule Dialog

The Custom Detection Rule dialog enables you to create a custom detection rule. You can define custom rules as needed to supplement the internal detection rules used by Automated Analysis to automatically create inventory during a scan. The custom detection rules are saved to the FlexNet Code Insight data library for global use across projects. For complete details about custom detection rules, see Managing Custom Detection Rules.

This dialog is accessed from two locations:

- From the Inventory Details tab in Analysis Workbench for an inventory item of the “component” type—whether system-generated or manually created—to which codebase files have been manually associated (as described in Creating a Custom Detection Rule from Inventory of “Component” Type).

- From Custom Detection Rules tab accessed from the Custom Data tab on the FlexNet Code Insight main menu (as described in Creating a Custom Detection Rule from Scratch).

The ability to edit certain fields depends on how you accessed the dialog. To help explain these differences, the following table designates the two access locations as “Inventory Details tab” and “Custom Detection Rules tab”.

The following describes the columns and actions you can perform from the Custom Detection Rule dialog.

### Table 8-34 • Custom Detection Rule dialog

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[component selection]</td>
<td>The following fields describe the component on which the custom detection rule is based. If you have accessed this dialog from the Inventory Details tab for an inventory item in Analysis Workbench, these fields are auto-populated with component information from the inventory item and are not editable. If you have accessed this dialog from the Custom Detection Rules tab, these fields are populated once you select the component and are editable as described below.</td>
</tr>
<tr>
<td>Component</td>
<td>The name of the component on which this detection rule is based. If you accessed this dialog from the Custom Detection Rules tab, click Lookup Component to select the component and its version, license, and forge URL. The License and URL fields are populated accordingly. If you accessed this dialog from the Inventory Details tab, this field is not editable.</td>
</tr>
<tr>
<td>License</td>
<td>The license associated with the component. If you accessed this dialog from the Custom Detection Rules tab, you cannot edit the field directly once it is populated from the component selection, but you can select a different license. To do so, click to switch to another license and, optionally, change the component version. Additionally, click to view the details and text of the selected license as stored in the FlexNet Code Insight data library. If you accessed this dialog from the Inventory Details tab, this field is not editable.</td>
</tr>
</tbody>
</table>
### Table 8-34 • Custom Detection Rule dialog (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A description of the component.</td>
</tr>
<tr>
<td></td>
<td>If you accessed this dialog from the <strong>Custom Detection Rules</strong> tab, this field is editable. It is not editable if you accessed the dialog from the <strong>Inventory Details</strong> tab.</td>
</tr>
<tr>
<td>URL</td>
<td>The forge URL for the component.</td>
</tr>
<tr>
<td></td>
<td>If you accessed this dialog from the <strong>Custom Detection Rules</strong> tab, this field is editable. It is not editable if you accessed the dialog from the <strong>Inventory Details</strong> tab.</td>
</tr>
</tbody>
</table>

[license, notices, and note content] The following fields are used to provide license or notice content and any audit notes for the inventory item generated from this rule. These field are editable.

If you accessed this dialog from the **Inventory Details** tab, these fields might be pre-populated with information from the manually created inventory. However, you can edit this information as needed.

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>As-Found License Text</td>
<td>The license content you want to associate with the inventory item. If no Notices Text content is provided, the Notices report uses the information in this field as the license text for the third-party component. For more information, see Finalizing the Notices Text for the Notices Report.</td>
</tr>
<tr>
<td>Notices Text</td>
<td>The exact content to include in the Notices report. This is usually a modification of the content in <strong>As-Found License Text</strong>. (You can copy the As-Found License Text content to the Notices Text pane and edit it.) If content exists in this field, the Notices report uses it as the license text for the third-party component and ignores any information in the As-Found License Text pane. For more information, see Finalizing the Notices Text for the Notices Report.</td>
</tr>
<tr>
<td>Audit Notes</td>
<td>Any notes you want to add to the inventory item based on your findings during the analysis.</td>
</tr>
</tbody>
</table>
Table 8-34 • Custom Detection Rule dialog (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[associated</td>
<td>This pane identifies the codebase files (by file name and MD5 value) on which to base the rule. You must identify at least one file.</td>
</tr>
<tr>
<td>codebase files]</td>
<td>If you have accessed this dialog from the Inventory Details tab, the files associated with the inventory item are automatically listed and available for selection. If you have accessed this dialog from the Custom Detection Rules tab, you must manually provide file name and MD5 value for each file. Keep in mind that, if the custom detection rule is associated with multiple files, the scan uses OR logic when processing the files against the target codebase. Consequently, only one file match between codebase and the rule is required to automatically create an inventory item.</td>
</tr>
<tr>
<td>File MD5</td>
<td>If you accessed this dialog from the Inventory Details tab:</td>
</tr>
<tr>
<td></td>
<td>• To add one or more files, click the check-box next to each desired file.</td>
</tr>
<tr>
<td></td>
<td>• To remove a file from the rule, click its check-box to deselect it.</td>
</tr>
<tr>
<td></td>
<td>If you accessed this dialog from the Custom Detection Rules tab:</td>
</tr>
<tr>
<td></td>
<td>• To add a file, click Add File and enter the exact file name and MD5 value for the file.</td>
</tr>
<tr>
<td></td>
<td>• To remove a file from the rule, click X in the file entry.</td>
</tr>
</tbody>
</table>

[actions] The following are actions conclude the rule-creation session.

<table>
<thead>
<tr>
<th>Save</th>
<th>Click Save to save the new custom detection rule to the Code Insight data library. You will be asked for confirmation to proceed with the creation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cancel</td>
<td>Click Cancel to cancel the rule creation process. You will be asked for confirmation to proceed with the cancellation.</td>
</tr>
</tbody>
</table>

See Also
Managing Custom Detection Rules
Creating a Custom Detection Rule from Inventory of “Component” Type
Creating a Custom Detection Rule from Scratch
Finalizing the Notices Text for the Notices Report

Edit Custom Rule Dialog

The Edit Custom Rule dialog enables you to edit an existing custom detection rule. Custom detection rules are user-defined when needed to supplement the internal detection rules used by Automated Analysis to automatically create inventory during a scan. These custom rules are saved to the FlexNet Code Insight library for global use across projects. For complete details about custom detection rules, see Managing Custom Detection Rules.
The following table describes the fields, buttons, and icons on the **Edit Custom Rule** dialog. You can edit any of the fields, using the methods described in the table.

### Table 8-35 • Edit Custom Rule dialog

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Component selection</strong></td>
<td>The following fields describe the component on which the custom detection rule is based. These fields are editable.</td>
</tr>
<tr>
<td>Component</td>
<td>The name of the component on which this detection rule is based. You cannot edit this value directly, but you can switch to another component. To do so, click <strong>Lookup Component</strong> to select another component, along with its version, license, and forge URL.</td>
</tr>
</tbody>
</table>
| License                       | The license associated with the component. You cannot edit this value directly, but you can select a different license. Click ✋ to switch to another license and, optionally, change the component version.  

  Additionally, you can click ⚫ to view the details and text of the selected license as stored in the FlexNet Code Insight data library. |
| Description                   | A description of the component.                                                                                                             |
| URL                           | The forge URL for the component.                                                                                                            |
| **License, notices, and note content** | The following fields are used to provide license or notice content and any audit notes for the inventory item generated from this rule. These fields are editable. |
| As-Found License Text         | The license content you want to associate with the inventory item. If no **Notices Text** content is provided, the Notices report uses the information in this field as the license text for the third-party component. For more information, see [Finalizing the Notices Text for the Notices Report](#). |
| Notices Text                  | The content to include in the Notices report. This is usually a modification of the content in **As-Found License Text** pane. (You can copy the **As-Found License Text** content to the **Notices Text** pane and edit it.)  

  If content exists in this field, the Notices report uses it as the license text for the third-party component and ignores any information in the **As-Found License Text** pane. For more information, see [Finalizing the Notices Text for the Notices Report](#). |
| Audit Notes                   | Any notes you want to add to the inventory item based on your findings during the analysis.                                                  |
License Details Window

The License Details window lets you view general information and license text for a selected license. The window has the following fields:

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Information Tab</td>
<td></td>
</tr>
<tr>
<td>Id</td>
<td>The identification number of the license in the data library.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the license (for example, Academic Free License v1.1).</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority ranking of the license as determined by FlexNet Code Insight. For more information, see What Does an Analyst do?.</td>
</tr>
<tr>
<td>URL</td>
<td>The URL where the license is available on the internet.</td>
</tr>
</tbody>
</table>
The Lookup Component window lets you search for a component in the FlexNet Code Insight data library and display additional information about the component, such as vulnerabilities and license issues. The window has the following fields:

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A short description of the license.</td>
</tr>
<tr>
<td>Category</td>
<td>A license category that spans multiple license instances (for example, MIT, Public Domain, BSD-3 Clause, and others). The family designation is helpful to a legal reviewer to understand the “type” of license prior to investing the time to analyze the complete license text.</td>
</tr>
<tr>
<td>Custom License</td>
<td>A designation of whether this license is a custom license.</td>
</tr>
<tr>
<td>Commercial</td>
<td>A designation of whether the licenses is classified as commercial.</td>
</tr>
<tr>
<td>Copyleft</td>
<td>A designation of whether the licenses is considered a copyleft license.</td>
</tr>
<tr>
<td>Free Software License</td>
<td>A designation of whether the license is a free software license.</td>
</tr>
<tr>
<td>GPL V2 Compatible</td>
<td>A designation of whether a license is compatible with GPL-2.0.</td>
</tr>
<tr>
<td>License Text Tab</td>
<td>The complete text of the selected license as stored in the FlexNet Code Insight data library. This text represents the external forge license text.</td>
</tr>
</tbody>
</table>

### Lookup Component Window

The **Lookup Component** window lets you search for a component in the FlexNet Code Insight data library and display additional information about the component, such as vulnerabilities and license issues. The window has the following fields:

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search by</td>
<td>Select the type of search you want to perform or the method you want to use to create a custom component:</td>
</tr>
<tr>
<td>Keywords</td>
<td>Enter the name or title keyword by which to search components or to create a custom component.</td>
</tr>
<tr>
<td>URL</td>
<td>Enter the project or forge URL by which to search components or to create a custom component.</td>
</tr>
</tbody>
</table>
## Add Project Dialog

The **Add Project** dialog appears when you select **Project** from the **Add New** dropdown menu. It lets you provide a name and select options for a new project. The dialog has the following fields:

### Table 8-38 • Add Project dialog

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the new project.</td>
</tr>
</tbody>
</table>
The Preferences page appears when you select Preferences from the main menu. From this page, you can change your FlexNet Code Insight user account password. In addition, you can view and add authorization tokens—that is, JSON Web Tokens known as JWTs—for use with Code Insight REST APIs. (The authorization tokens are associated with the current user account.) The page has the following fields:

**Table 8-39 • Preferences page**

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Change Password</strong></td>
<td></td>
</tr>
<tr>
<td>New Password</td>
<td>Enter a new password for the selected authorization token. The password must be a minimum of 8 characters, one of which must be numeric and one of which must be in upper case. No spaces are allowed in the password.</td>
</tr>
<tr>
<td>New Password Confirm</td>
<td>Reenter the password you entered in the New Password field.</td>
</tr>
<tr>
<td>Update Password</td>
<td>After entering the password in both fields, click Update Password to save your changes.</td>
</tr>
<tr>
<td><strong>AUTH Tokens</strong></td>
<td></td>
</tr>
</tbody>
</table>
Add Token Dialog

The Add Token dialog appears when you click the Add Token button on the Preferences page. It lets you create an authorization token (that is, a JSON Web Token known as a JWT) to be used to authenticate calls to FlexNet Code Insight REST APIs. The token is associated with the user account under which you are logged in or whose password you have changed in the Change Password fields on the Preferences page. The dialog has the following fields:

Table 8-40 • Add Token dialog

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the token you are creating.</td>
</tr>
<tr>
<td>Token Validity</td>
<td>Select one of the validity periods:</td>
</tr>
<tr>
<td></td>
<td>• Never Expires: The authorization token never expires.</td>
</tr>
<tr>
<td></td>
<td>• Expires On: The authorization token is valid until the date you pick on the Validity Calendar.</td>
</tr>
</tbody>
</table>

See Also
Add Token Dialog
Edit Token Dialog
Exporting and Importing Project Data
Performing Inventory-Only Scanning
The *Edit Token* dialog appears when you click the *Edit Token* icon on the *Preferences* page. It lets you edit an authorization token (that is, a JSON Web Token known as a JWT) used to authenticate calls to FlexNet Code Insight REST APIs. The token is associated with the user account under which you are logged in or whose password you have changed in the *Change Password* fields on the *Preferences* page.

This dialog also allows you to copy the token value to the Clipboard so that you paste it whenever needed for Code Insight REST access (for example, when configuring the Code Insight plugins, importing or exporting project data, or running REST API directly).

The dialog has the following fields:

**Table 8-41 • Edit Token dialog**

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the token you are creating.</td>
</tr>
<tr>
<td>Token</td>
<td>Displays the actual characters of the system-generated token.</td>
</tr>
<tr>
<td>Select Token Text</td>
<td>Click this button to highlight the token characters displayed in the <em>Token</em> field. To copy the token to the clipboard, press <strong>CTRL-C</strong>.</td>
</tr>
<tr>
<td>Expiration</td>
<td>A read-only field that displays the expiration date of the token, or the text “Token has no expiration date.”</td>
</tr>
<tr>
<td>Save</td>
<td>Click this button to save your edits.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Click this button to exit the <em>Edit Token</em> dialog without saving your edits.</td>
</tr>
</tbody>
</table>
Advanced Inventory Search Dialog

The Advanced Inventory Search dialog is opened when you click the Advanced Search button on the Inventory Items page. This dialog provides the following options that enable you to search your inventory in a variety of ways:

Table 8-42 • Advanced Inventory Search dialog

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Items</td>
<td>The following options enable you to filter inventory by inventory attributes.</td>
</tr>
<tr>
<td><strong>Inventory Name</strong></td>
<td>Enter the whole or partial inventory name by which to filter the inventory display. For example, if you enter <code>apache</code> in this field, FlexNet Code Insight will find all inventory items that have the <code>apache</code> string in their names.</td>
</tr>
<tr>
<td><strong>Inventory Priority</strong></td>
<td>Select one or more of checkboxes (P1, P2, P3, or P4) to search the inventory by inventory priority. For more information about inventory priority, see Inventory Priority in the “Using FlexNet Code Insight” chapter.</td>
</tr>
<tr>
<td><strong>Inventory Review Status</strong></td>
<td>Select one or more of the following checkboxes to filter the inventory display based on the review status of inventory items:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Approved</strong>—Show only inventory that has been reviewed and approved, either manually by a reviewer or automatically during the auto-publish process.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Rejected</strong>—Show only inventory that has been reviewed and rejected, either manually by a reviewer or automatically during the auto-publish process.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not Reviewed</strong>—Show only inventory that has not yet been reviewed. For more information about the review status, see Review Status of Inventory in the “Using FlexNet Code Insight” chapter.</td>
</tr>
</tbody>
</table>
Dependency Options
Select one of the following options to filter the inventory display based on dependency level:

- **All Inventory Items**—Show all inventory—that is, all top-level inventory items, along with their first-level and transitive dependencies.
- **Only Top-Level Inventory Items**—Show all top-level inventory items only. No first-level or transitive dependencies are displayed.
- **Only Dependency Inventory Items**—Show only first-level and transitive dependencies. No top-level inventory is displayed.

Inventory Age
Select one of the following to filter the inventory display by the time frame in which the inventory items were published:

- **Last 1 day**—Show inventory published in the last day. For example, if today is Feb 6th, search from Feb 5th 12 AM.
- **Last 7 days**—Show inventory published in the last week. For example, if today is Feb 6th, search from Jan 30th 12 AM.
- **Last month**—Show inventory published in the last month. For example, if today is Feb 6th, search from Jan 7th 12 AM (30 days).
- **Custom Date Range**—Show inventory published within the specified time frame. Select a beginning (From) and ending (To) date from the popup calendar.
- **Any**—Show all published inventory.

Inventory Notifications
Select one or more of the following checkboxes to filter the inventory display based on security vulnerability alerts:

- **Inventory with Open Alerts**—Show only inventory items that have open vulnerability alerts (that is, alerts for vulnerabilities that were discovered post-publication and have not been closed).
- **Inventory Rejected Due to New Non-Compliant Security Vulnerabilities**—Show inventory items that have been rejected due to new security alerts that are non-compliant with policy.

### Table 8-42 • Advanced Inventory Search dialog

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependency Options</td>
<td>Select one of the following options to filter the inventory display based on dependency level:</td>
</tr>
<tr>
<td></td>
<td>- <strong>All Inventory Items</strong>—Show all inventory—that is, all top-level inventory items, along with their first-level and transitive dependencies.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Only Top-Level Inventory Items</strong>—Show all top-level inventory items only. No first-level or transitive dependencies are displayed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Only Dependency Inventory Items</strong>—Show only first-level and transitive dependencies. No top-level inventory is displayed.</td>
</tr>
<tr>
<td>Inventory Age</td>
<td>Select one of the following to filter the inventory display by the time frame in which the inventory items were published:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Last 1 day</strong>—Show inventory published in the last day. For example, if today is Feb 6th, search from Feb 5th 12 AM.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Last 7 days</strong>—Show inventory published in the last week. For example, if today is Feb 6th, search from Jan 30th 12 AM.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Last month</strong>—Show inventory published in the last month. For example, if today is Feb 6th, search from Jan 7th 12 AM (30 days).</td>
</tr>
<tr>
<td></td>
<td>- <strong>Custom Date Range</strong>—Show inventory published within the specified time frame. Select a beginning (From) and ending (To) date from the popup calendar.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Any</strong>—Show all published inventory.</td>
</tr>
<tr>
<td>Inventory Notifications</td>
<td>Select one or more of the following checkboxes to filter the inventory display based on security vulnerability alerts:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Inventory with Open Alerts</strong>—Show only inventory items that have open vulnerability alerts (that is, alerts for vulnerabilities that were discovered post-publication and have not been closed).</td>
</tr>
<tr>
<td></td>
<td>- <strong>Inventory Rejected Due to New Non-Compliant Security Vulnerabilities</strong>—Show inventory items that have been rejected due to new security alerts that are non-compliant with policy.</td>
</tr>
</tbody>
</table>
### Table 8-42 • Advanced Inventory Search dialog

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Confidence Level</td>
<td>Select one or more Confidence levels—<strong>High</strong>, <strong>Medium</strong>, or <strong>Low</strong>—by which to filter system-generated inventory items in the inventory display. The Confidence level is the measure of the strength of the discovery technique used by Code Insight to generate an inventory item. For a description of the Confidence levels and how they are used, see <em>Inventory Confidence</em> in the “Using FlexNet Code Insight” chapter.</td>
</tr>
<tr>
<td>Inventory Tasks</td>
<td>The following options filter inventory to show only those inventory items that have tasks. Refine the search using one or more task attributes—for example, task status, type, age, or owner.</td>
</tr>
<tr>
<td>Task Status</td>
<td>Select one of the following to filter the inventory display by the current status of the tasks associated with inventory:</td>
</tr>
<tr>
<td>Open Tasks</td>
<td>Show inventory associated with at least open task.</td>
</tr>
<tr>
<td>Closed Tasks</td>
<td>Show inventory associated with at least one closed task.</td>
</tr>
<tr>
<td>All Tasks</td>
<td>Show all inventory associated with tasks, open or closed.</td>
</tr>
<tr>
<td>Tasks Type</td>
<td>Select one of the following to filter the inventory display by the type of task associated with inventory:</td>
</tr>
<tr>
<td>Manual inventory review</td>
<td>Show inventory associated with at least one task requesting that a manual legal or security review be performed. (This review is needed to flag the inventory as accepted or rejected.)</td>
</tr>
<tr>
<td>Remediate Inventory</td>
<td>Show inventory (currently or previously rejected) associated with at least one task requesting that software development take some action to make rejected inventory acceptable.</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Show inventory associated with at least one task requesting that additional attention of some sort be given to the inventory.</td>
</tr>
<tr>
<td>Any</td>
<td>Show all inventory associated with tasks of any type.</td>
</tr>
</tbody>
</table>
## Table 8-42 • Advanced Inventory Search dialog

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inventory Tasks Age</strong></td>
<td>Select one of the following to filter the inventory display by the time frame in which tasks associated with inventory items have been created:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Last day</strong>—Show inventory associated with at least one task created within the last day. For example, if today is Feb 6th, search from Feb 5th 12 AM.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Last 7 days</strong>—Show inventory associated with at least one task created within the last week. If today is Feb 6th, search from Jan 30th 12 AM.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Last month</strong>—Show inventory associated with at least one task created within the last month. If today is Feb 6th, search from Jan 7th 12 AM (30 days).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Custom Date Range</strong>—Show inventory associated with at least one task created in the specified time frame. Select a beginning (<strong>From</strong>) and ending (<strong>To</strong>) date from the popup calendar.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Any</strong>—Show all inventory associated with tasks, no matter when the tasks were created.</td>
</tr>
<tr>
<td><strong>Inventory Task Owner</strong></td>
<td>Select one of the following to filter the inventory display by the user who is assigned to tasks associated with inventory items:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Only Mine</strong>—Show inventory associated with at least one task assigned to you (the current user).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Specific User</strong>—Show inventory associated with at least one task assigned to the specified user. (A <strong>Select user</strong> pop-up enables you to select the user.)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Any</strong>—Show all inventory associated with tasks, no matter to whom the tasks are assigned.</td>
</tr>
<tr>
<td><strong>Security Vulnerabilities</strong></td>
<td>The following options enable you to filter inventory by the attributes of the security vulnerabilities associated with inventory items.</td>
</tr>
<tr>
<td><strong>Security Vulnerability ID</strong></td>
<td>Enter the complete valid ID for the security vulnerability by which to filter the inventory display to show only those inventory items associated with the specified vulnerability.</td>
</tr>
</tbody>
</table>
Chapter 8  Pages and Panels
Advanced Inventory Search Dialog

Table 8-42 • Advanced Inventory Search dialog

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Security Vulnerability Severity | Select one or more vulnerability severity levels by which to filter the inventory display to show only those inventory items associated with at least one vulnerability that has one of the selected severities. The severity-level options differ depending on the CVSS version used by FlexNet Code Insight. If CVSS v3.0 is used, the following severity options are available:  
  - Critical (9.0 - 10.0)  
  - High (CVSS 7.0 - 8.9)  
  - Medium (CVSS 4.0 - 6.9)  
  - Low (CVSS 0.1 - 3.9)  
  - None (CVSS = 0)  
If CVSS v2 is used, these severity options are available:  
  - High (CVSS 7.0 - 10.0)  
  - Medium (CVSS 4.0 - 6.9)  
  - Low (CVSS 0.1 - 3.9)  
  - Unknown (N/A)  
For more information about vulnerability severities, see Security Vulnerabilities Associated with Inventory in the “Using FlexNet Code Insight” chapter. |
Select one of the following options to filter the inventory display by the time frame in which security vulnerabilities associated with inventory items were detected.

**Note** • The detection date is either the inventory creation date (if a vulnerability was reported when the inventory was created) or the date that a new vulnerability applicable to this inventory was delivered by the update service.

- **Last day**—Show inventory associated with at least one vulnerability detected within the last day. For example, if today is Feb 6th, search from Feb 5th 12 AM.

- **Last 7 days**—Show inventory associated with at least one vulnerability detected within the last week. For example, if today is Feb 6th, search from Jan 30th 12 AM.

- **Last 30 days**—Show inventory associated with at least one vulnerability detected within the last month. For example, if today is Feb 6th, search from Jan 7th 12 AM.

- **Custom Date Range**—Show inventory associated with at least one vulnerability detected within a specific time frame. Select a beginning (From) and ending (To) date from the popup calendar.

- **Any**—Show all inventory associated with security vulnerabilities, no matter when the vulnerabilities were detected.

### License Versions

The following options enable you to filter inventory by attributes of the selected license for inventory items.

<table>
<thead>
<tr>
<th>License Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Name</td>
<td>Enter the full or partial license name by which to filter the inventory display. For example, if you enter bsd in this field, FlexNet Code Insight will find all inventory items whose <strong>Selected License</strong> value has the bsd string in its name.</td>
</tr>
</tbody>
</table>
The `Import Project Data` dialog is displayed when you select `Import Project Data` from the `Manage Project` dropdown menu on the `Summary` tab. This dialog enables you to configure and start a project import process, which imports project data from a properly formatted and archived JSON file into a target project.

An additional setting to determine whether the import should delete inventory that has no associated files is defined separately on the `Edit Project: General Tab`. Ensure that this setting is properly configured for the import.
For complete details on performing a project import, see the chapter, Exporting and Importing Project Data

**Table 8-43 • Import Project Data dialog**

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Choose File to Import</strong></td>
<td>Click <strong>Browse</strong> next to the <strong>Choose File to Import</strong> field to search for and select the <code>.zip</code> file containing the JSON data file you are importing.</td>
</tr>
</tbody>
</table>
| **Only add files to inventory with matching MD5** | This option determines whether MD5 checks, in addition to a file-path checks, are required to associate a file to target inventory during the import process.  
  - **Unselected**—Disables the MD5 checks when associating files with inventory. To be associated with inventory in the target project, files need only to have file paths that match in both the import data file and the target project codebase.  
  - **Selected**—Enables the MD5 checks (in addition to file-path checks) when marking files as reviewed. To be associated with inventory in the target project, files must have both MD5 values and file paths that match in both the import data file and the target project codebase.  
  This option is unselected by default.  
  For complete details, see Option to Require MD5 Checks When Associating Files to Target Inventory. |
| **Only mark files as reviewed with matching MD5** | This option determines whether MD5 checks, in addition to a file-path checks, are required to mark a codebase files as reviewed in the target project during the import process.  
  - **Unselected**—Disables MD5 checks for marking target inventory as reviewed. Files flagged as “reviewed” in the import data file need only to have file paths that match in both the data file and the target project to be eligible for the “reviewed” flag.  
  - **Selected**—Enables MD5 checks (in addition to file-path checks). Files flagged as “reviewed” in the import data file are eligible for the “reviewed” flag in the scanned target project codebase only if their file path and MD5 value match in both the data file and the target project.  
  This option is unselected by default.  
  For complete details, see Option to Require MD5 Checks When Marking Target Codebase Files as Reviewed. |
Inventory Notes Handling

Choose one of the options in this section to determine how the import process handles notes between an identical source and target inventory item. The options apply to the following inventory notes:

- Notices Text
- Audit Notes
- Usage Guidance
- Remediation Notes

A source and a target inventory item are considered identical if they are associated with the same Code Insight data library item (based on the unique combination of component-version-license, or CVL).

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overwrite existing notes with imported notes</strong></td>
<td>Select this option to overwrite all notes in the target inventory item with notes from the source inventory item. However, empty data for a given field in the source target inventory will not overwrite existing content for that same field in the target inventory item (that is, the existing target content is retained). By default, this option is selected.</td>
</tr>
</tbody>
</table>
| **Append imported notes to existing notes** | Select this option to append notes from the source inventory item to the end of existing notes in the identical target inventory item. For a given note field, the appended content is separated from the existing content with a line break and the following heading:

  Copied during import from `<ProjectName>::<InventoryName>` (TimeStamp)

  However, if note content for a given field is the same in both the source and the target inventory items, no content is appended. |
| **OK**                        | Click to start the import process. |
FlexNet Code Insight User Roles and Permissions

This appendix serves as a reference to the various user roles and permissions that Code Insight offers as a means to control user access to its functionality at your site:

- System Roles and Permissions
- Project Roles and Permissions
- Roles and Permissions to Manage Project Task Flow

System Roles and Permissions

The following table lists the system roles and associated permissions used to manage the FlexNet Code Insight system. The initial FlexNet Code Administrator (and any subsequent administrators) assigns these roles to other FlexNet Code Insight users by using the Manage Permissions dialog accessed from the Administration Users/Permissions tab. (For details, see “Managing User Permissions for System Activities” in the “Configuring FlexNet Code Insight” chapter in the FlexNet Code Insight Installation and Configuration Guide.)

One user can be assigned multiple roles.

For Information on creating and managing FlexNet Code Insight users in general, see “Managing Users” in the “Configuring FlexNet Code Insight” chapter in the FlexNet Code Insight Installation and Configuration Guide.
### Table A-1 • System Roles and Permissions

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Roles</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Administer Code Insight:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Set system settings</td>
<td><strong>✓</strong></td>
<td></td>
</tr>
<tr>
<td>• Manage users and permissions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Schedule or run Electronic Updates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Configure an email server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Configure LDAP users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Configure Application Lifecycle (ALM) instances</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Configure a Scan Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Configure scan profiles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Define global project defaults</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Manage policies:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Create and edit policy profiles</td>
<td><strong>✓</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Create projects:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Create projects (and thereby automatically become Project Owner for each)</td>
<td><strong>✓</strong></td>
<td></td>
</tr>
<tr>
<td>• Create project folders (in Projects list)</td>
<td><strong>✓</strong></td>
<td></td>
</tr>
</tbody>
</table>

The Project Creation role is controlled by the **Allow All Users to Create Projects** option on the Manage Permissions dialog. If **Yes** (default), any user has this role. If **No**, only users assigned this role can create projects. (For details, see “Managing User Permissions for System Activities” in the “Configuring FlexNet Code Insight” chapter in the FlexNet Code Insight Installation and Configuration Guide.) Users who have this role can also create project folders in the Projects list.
Project Roles and Permissions

The following table lists the various roles and associated permissions used to manage a given project in Code Insight. The Project Owner assigns the Analyst, Reviewer, and Observer roles to FlexNet Code Insight user and can reassign project ownership. For details about these roles and the procedure for assigning them, see Assigning Project Roles to Users.

Table A-2 • Project Roles and Permissions

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Project Owner</th>
<th>Analyst</th>
<th>Reviewer</th>
<th>Observer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage a project:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Reassign project ownership</td>
<td>✔</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>• Manage project users</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Rename project</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Move projects in Project Folder Tree</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Manage scan settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Manage inventory review/remediation settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Manage Source Control Management (SCM) and Application Lifecycle (ALM) instances</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invoke a scan</td>
<td>✔</td>
<td>✔</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Upload codebase</td>
<td>✔</td>
<td>✔</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Import/export project data</td>
<td>✔</td>
<td>✔</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>View project inventory</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

The project creator automatically becomes Project Owner, who can then reassign ownership to another user.

See the previous section, System Roles and Permissions, for information about the Create Project role needed to create projects.

Any user (not just one with a project role) can view the Project Inventory tab and the associated inventory details.
Table A-2 • Project Roles and Permissions (cont.)

<table>
<thead>
<tr>
<th>Roles</th>
<th>Project Owner</th>
<th>Analyst</th>
<th>Reviewer</th>
<th>Observer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit, create, and recall project inventory</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>On the <strong>Project Inventory</strong> tab, only Reviewers and the Project Owner can perform inventory review functions:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>—</td>
</tr>
<tr>
<td>• Recall inventory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Edit inventory priority, review status, and alerts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Update the <strong>Notices Text</strong> field (on the <strong>Notices Text</strong> tab) and information on the <strong>Notes &amp; Guidance</strong> tab (except <strong>Detection Notes</strong>) for inventory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Approve or reject inventory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>However, on this same tab, only Analysts and the Project Owner have access to the <strong>Add Item</strong> button to create inventory and to the <strong>Edit Item</strong> button to edit inventory definition properties (such as component, version, selected license, URL, and usage).</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Access and use Analysis Workbench</strong></td>
<td>✓</td>
<td>✓</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>• View codebase file tree</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Create, edit, and recall inventory and manage custom detection rules.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Edit the <strong>Notices Text</strong> field on the <strong>Notices Text</strong> tab</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Edit the <strong>Audit Notes</strong> field on the <strong>Notes</strong> tab</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* The Observer role is available for only projects defined as “Private”. Only Observers, the Project Owner, Analysts, and Reviewers have access to the “Private” project to which they are assigned. The Observer is considered a regular user, restricted to viewing project inventory and generating reports for the “Private Project”.

Access and use Analysis Workbench

- View codebase file tree
- Create, edit, and recall inventory and manage custom detection rules.
- Edit the **Notices Text** field on the **Notices Text** tab
- Edit the **Audit Notes** field on the **Notes** tab
Roles and Permissions to Manage Project Task Flow

The following table lists the project roles and permissions used to manage tasks to review or remediate inventory items in a project.

**Table A-3 • Project Task-Flow Roles and Permissions**

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Project Owner</th>
<th>Analyst</th>
<th>Reviewer</th>
<th>Observer</th>
<th>Task Assignee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create/edit tasks</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Reassign task</td>
<td>✓</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>Close manual review task</td>
<td>–</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Close remediation task</td>
<td>✓</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>Close miscellaneous task</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Notes: Any user assigned to a project role can create and edit tasks. Any user assigned to a project role can close a miscellaneous task.
Chapter A  FlexNet Code Insight User Roles and Permissions

Roles and Permissions to Manage Project Task Flow